PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA

ESCOLA DE FORMAÇÃO DE PROFESSORES E HUMANIDADES

PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU* EM HISTÓRIA

GEORGE MENDES MARRA

O JOGO DA MÍMESE E O USO DA CRIPTOGRAFIA

GOIÂNIA

2017

GEORGE MENDES MARRA

O JOGO DA MÍMESE E O USO DA CRIPTOGRAFIA

Dissertação apresentada à Coordenação de Pós Graduação como parte dos requisitos para obtenção do título de Mestre em História pela Pontifícia Universidade Católica de Goiás – PUC Goiás

Orientador: Professor Dr. Eduardo José Reinato

Área de Concentração: Cultura e Poder

GOIÂNIA

2017

M358 Marra, George Mendes
O jogo da mímese e o uso da criptografia[manuscrito]/
George Mendes Marra.-- 2017.
235 f.; il. 30 cm

Texto em português com resumo em inglês
Dissertação (mestrado) - Pontifícia Universidade Católica
de Goiás, Programa de Pós-Graduação Stricto Sensu
em História, Goiânia, 2017
Inclui referências f. 206-212

1. Mimeses. 2. Enigmas lógicos. 3. Criptografia. 4.
Segunda Guerra Mundial, 1939-1945. I.Reinato, Eduardo
José. II.Pontifícia Universidade Católica de Goiás.
III. Título.

CDU: 003.26(043)

O JOGO DA MÍMESE E O USO DA CRIPTOGRAFIA

Dissertação aprovada em 11 de dezembro de 2017, no curso de Mestrado em História da Pontifícia Universidade Católica de Goiás, como requisito para a obtenção do grau de Mestre em História.

BANCA EXAMINADORA

Prof. Dr. Eduardo José Reinato
PUC Goiás / Presidente

Profa. Dra. Maria Cristina Nunes Ferreira Neto
PUC Goiás / Examinadora Interna

Prof. Dr. Robson Corrêa de Camargo
UFG / Examinador Externo

Profa. Dra. Renata Cristina de Sousa Nascimento
PUC Goiás / Suplente

Prof. Dr. Roberto Abdala Junior
UFG / Suplente

AGRADECIMENTOS

Agradeço a Deus, a minha família e meu orientador pelo apoio.

RESUMO

MENDES MARRA, George. *O jogo da mímese e o uso da criptografia.* Trabalho de Conclusão (Mestrado em História) – Pontifícia Universidade Católica de Goiás (PUC-Goiás), Goiânia, 2017

Esta dissertação de Mestrado aborda o impacto no uso da criptografia nas comunicações no período de grandes guerras mundiais. Como objetivos específicos temos: Analisar o efeito da criptografia no contexto das grandes guerras mundiais; Entender o significado político/poder da criptografia no século XX; Analisar o filme: “O jogo da imitação” tomando-o como fonte histórica para o entendimento da lógica da criptografia como mecanismo de poder; Historiar o desenvolvimento da tecnologia da máquina Enigma e desvelar os elementos de poder por detrás do uso da criptografia. A problemática seria de que maneira a criptografia passa a influenciar as estruturas de poder e ações militares a partir da descoberta da cifra da máquina Enigma? Temos as seguintes hipóteses: Devido a complexidade das relações internacionais, a partir do final do século XIX e início do século XX, as comunicações entre nações aliadas passaram a ter o cuidado de não serem descobertas pela espionagem dos rivais. Daí começa o esforço para o desenvolvimento de mecanismos de cifragem e codificação que levaram ao desenvolvimento das máquinas de cifragem até o desenvolvimento da máquina Enigma; A segunda hipótese seria que as Guerras Mundiais agilizaram as práticas de construção de máquinas de cifragem como forma de defesa de segredos nacionais; A análise do filme: “O jogo da imitação” nos mostrará o papel da Matemática e a ação da Universidade no processo de criação tecnológica para desvendamento de “enigmas”.

Palavras-chave: Mimese. Criptografia. Máquina Enigma. Jogo da Imitação. Segunda Guerra Mundial

ABSTRACT

MENDES MARRA, George. The mimic game and the use of encryption. Conclusion Work (Master in History) - Pontifical Catholic University of Goiás (PUC-Goiás), Goiânia, 2017

This Master's thesis addresses the impact on the use of cryptography in communications during the period of the great world wars. As specific objectives we have: To analyze the effect of cryptography in the context of the great world wars; Understand the political significance / power of cryptography in the twentieth century; Analyze the film: "The game of imitation" taking it as a historical source for understanding the logic of cryptography as a mechanism of power; Historize the development of Enigma machine technology and unveil the power elements behind the use of encryption. The problem would be in what way the encryption starts to influence the structures of power and military actions from the discovery of the cipher of the Enigma machine? We have the following hypotheses: Due to the complexity of international relations, from the late nineteenth and early twentieth centuries, communications between allied nations began to be careful not to be discovered by the spies of rivals. From there begins the effort to develop encryption and coding mechanisms that led to the development of encryption machines until the development of the Enigma machine; The second hypothesis would be that the World Wars speeded up the practices of building cipher machines as a way of defending national secrets; The analysis of the film: "The game of imitation" will show us the role of Mathematics and the action of the University in the process of technological creation to unravel "enigmas".

Keywords: Mimesis. Encryption. Enigma machine. Imitation Game. Second World War

LISTA DE ILUSTRAÇÕES

LISTA DE ANEXOS

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

O filme/documentário *Citizenfour* foi lançado em 2014 com direção de Laura Poitras. Esta película aborda a trajetória de Edward Snowden que trabalhava na NSA (*National Security Agency* ou Agência de Segurança Nacional) e que revelou os verdadeiros objetivos desta entidade governamental dos Estados Unidos. A NSA espiona pessoas, governos e empresas sem autorização dos mesmos. A NSA foi fundada em 4 de novembro de 1952 e é subordinada ao Departamento de Defesa dos Estados Unidos.

Edward Joseph *Snowden* era administrador de sistemas de segurança da NSA e ficou conhecido por expor para o público como a NSA realiza a vigilância global sem o consentimentos das entidades espionadas. *Citizenfour* mostra os contatos preliminares de *Edward Snowden* e os produtores deste filme depois que ele resolveu sair da NSA e revelar as informações secretas da NSA. Em seguida ele buscou asilo político na Rússia e provavelmente vive em Moscou com sua esposa.

Entidades governamentais ou privadas que usam criptografia para ocultar informações sigilosas ou segredos de estado estão menos sujeitas de serem espionadas porque exigem um esforço maior da NSA para decifrar as mensagens.

A maioria das pessoas desconhecem ou usam configurações básicas de criptografia em seus equipamentos eletrônicos como telefones celulares e computadores pessoais. A maioria das informações que trafegam na rede mundial de computadores (Internet) não está criptografada o que facilita para as agências de espionagem de diversos países o monitoramento de seus cidadãos.

A criptografia é essencial para preservar informações sigilosas e manter comunicações seguras mantendo o anonimato e privacidade.

A tendência de utilização do filme pelo historiador se consolidou no século XX, após longo debate. Inúmeros cineastas defenderam a ideia de que os audiovisuais são formas discursivas de representação do passado. Além da escrita e da oralidade, o vídeo e o cinema são formas interessantes de refletir sobre as peculiaridades da História.

Este trabalho é um esforço nessa direção. Partindo da análise do Código Enigma como forma de representação criptográfica, passou-se a explicar a grande depressão de 1929 como vetor importante para a eclosão da Segunda Guerra

Mundial até chegar ao estudo do cinema como fonte histórica.

O primeiro capítulo analisa o filme: O jogo da imitação, 2014. Este capítulo mostra uma nova abordagem para estudar temas históricos com a utilização de filmes cinematográficos. O filme escolhido para o tema desta dissertação foi o “O jogo da imitação” dirigido pelo diretor norueguês *Morten Tyldum* em 2014. Neste filme é possível observar o contexto histórico da Segunda Guerra Mundial onde a Alemanha conquista militarmente quase toda a Europa e depois de conquistar a França, se prepara para invadir a Grã-Bretanha. O filme mostra também o esforço dos britânicos para conseguir decifrar as mensagens cifradas pela máquina Enigma dos alemães. Enquanto o código secreto dos alemães não era decifrado, os ingleses iam sofrendo pesados bombardeios em suas cidades e centenas de navios mercantes estavam sendo afundados pela aviação e marinha alemãs. Neste filme é possível ver como o domínio de certas práticas de cifragem e decifragem foram decisivas no desenrolar da Segunda Guerra Mundial. Os britânicos conseguiram centralizar todo o esforço de guerra na área de criptografia em um local secreto chamado *Bletchley Park* (disfarçado como fábrica de rádios).

Os alemães não unificaram seus serviços de decifragem dos códigos dos Aliados e estas mesmas agências competiam entre si atrasando a logística da criptoanálise. O filme ilustra com cenas da Batalha da França, Batalha do Atlântico, Batalha da Inglaterra, Batalha de Stalingrado, Batalha das Ardenas e “Dia D” (invasão da Normandia) que ocorreram durante a Segunda Guerra Mundial.

O referencial teórico aborda a pesquisa bibliográfica e análise fílmica do filme: “O Jogo da Imitação”. Existe um outro filme intitulado “Enigma” lançado em 2001 dirigido por *Michael Apted* que trata da decifragem do código da máquina de cifragem Enigma antes de um grande ataque alemão a um comboio aliado no Oceano Atlântico durante a Segunda Guerra Mundial. A máquina de cifragem Enigma aparece também no filme intitulado “U-571 – A Batalha do Atlântico” lançado no ano 2000 e dirigido por *Jonathan Mostow*. Este filme mostra as várias tentativas dos Aliados de capturar um submarino alemão com sua máquina de cifragem Enigma naval além de seu livro de cifras com o objetivo de decifrar o código secreto utilizado nas comunicações alemãs. O filme “O jogo da imitação, 2014” foi baseado em fatos reais e apresenta uma densidade maior sobre criptografia, máquina de cifragem Enigma, criptoanálise e a representação de vários personagens reais que

trabalharam em um local secreto na Inglaterra chamado *Bletchley Park* durante a Segunda Guerra Mundial.

O segundo capítulo mostra o tema criptologia e a evolução da criptografia até meados do século XX e os esforços internacionais para decodificar o complexo sistema de informação do Estado Nazista através das máquinas Enigma. O uso da criptografia nas comunicações militares utilizando uma máquina de cifragem chamada Enigma colocou a Alemanha na liderança mundial no setor de comunicações seguras. Desde os primórdios da humanidade, o homem procura meios de se comunicar de forma sigilosa para que apenas os escolhidos por ele consigam entender a mensagem. Esta seção mostra como a evolução da criptografia foi decisiva em conflitos desde a Antiguidade até as grandes guerras do século XX como por exemplo na Primeira Guerra Mundial (1914-1918), período entre guerras (1919-1938) e a Segunda Guerra Mundial (1939-1945).

O terceiro capítulo explica a evolução da máquina Enigma e diversos modelos são detalhados neste capítulo. Outras máquina de cifragem também são mostradas nesta seção como a SIGABA utilizada pelos militares estadounidenses, a TYPEX utilizada pelos militares britânicos, a PURPLE utilizada pelos militares japoneses. Geralmente estas máquinas de cifragem era usadas nas embaixadas em outros países para preservar as mensagens secretas dos embaixadores e espiões locais. No caso dos alemães, existiam modelos exclusivos das máquinas de cifragem Enigma para o exército, aviação, marinha (navios de superfície e submarinos), serviço secreto e ferrovias. Além das máquinas de cifragem, britânicos e alemães já utilizavam computadores em seus sistemas de inteligência. O computador britânico *Colossus* lançado em 1943 (usado inicialmente para criptoanálise) e os computadores alemães Z1 (1935-1938) e Z3 (1941) (usados na indústria aeronáutica alemã) demonstram que a evolução da ciência da computação foi acelerada durante a Segunda Guerra Mundial.

CAPÍTULO I. Análise fílmica: O jogo da imitação

> "Pedi e vos será dado; buscai e achareis; batei à porta e vos será aberta; pois todo o que pede recebe, o que busca acha, e ao que bate se lhe abrirá."
>
> (Mateus, cap. VII, v. 7:7)

1. Apresentação: O jogo da mímese

Este capítulo apresenta análise fílmica "O jogo da imitação, 2014". Inclui as palavras "mímese e imitação" etimologicamente por entender que o conhecimento da etimologia das palavras permite introduzir a ideia de evolução semântica, principalmente quando se trata de cultura Grego-Latina.

Mimese - do grego: *ημίμησις, mímesis* - imitação é uma figura que consiste no uso do discurso direto e principalmente na imitação do gesto, voz e palavras de outrem. Para o latim a palavra imitação - *imitatione* - é o ato ou efeito de imitar que difere de emulação, também latina, - *aemulatione* - um sentimento que nos incita a igualar ou superar outrem. A palavra enigma, do grego, *aínigma*, do latim, *aenigma,* é uma descrição obscura, ambígua de alguma coisa que seja difícil adivinhá-la ou decifrá-la (FERREIRA, 1986).

Para Menard (1991, p.11) "A mitologia primitiva é a língua poética que se serviam os povos antigos para explicar os fenômenos naturais" . Nesse sentido, aos olhos antigos, sobretudo para os gregos, era importante recorrer aos mitos. Como por exemplo, o mito da Esfinge que propusera enigma aos viajantes. Um deles é ressaltado por Menard:

> Uma esfinge nascida de *Tifão* e de *Equidna* estava em uma estrada perto de Tebas e propunha enigmas aos viajantes e matava os que não adivinhavam. Com a morte do rei *Laio*, os tebanos prometeram um casamento com a rainha e a coroa para quem se livrasse da esfinge. Édipo resolveu enfrentar a esfinge. A esfinge perguntou: "Qual é o animal que tem quatro pés de manhã, dois ao meio-dia, e três ao cair da noite?". Édipo respondeu: "É o homem, na infância, anda de gatinhas; na velhice, apoia-se a um bordão." De acordo com a decisão do oráculo, a esfinge foi obrigada a atirar-se às ondas. (MENARD, op. cit., p. 33):

1.2 O cinema como fonte de histórias

As obras cinematográficas, causaram impactos na sociedade. Mas isso não significa que todas podem ser fonte de pesquisa para o historiador. Nóvoa (2009) , relata que a utilização do filme pelo historiador, por um determinado tempo foi inconcebível; posteriormente, admitido formalmente, parece constituir doravante o objeto de uma tendência cujo sucesso é crescente, visto que, mais do que nunca, os cineastas, hoje, à medida que produzem filmes de acordo com relatos históricos, têm mais prestígio. Além do mais, sociólogos, etnólogos, filósofos e historiadores afirmam a estreita relação entre o cinema e a história. Imediatamente, por causa da correspondência que parece evidente, à primeira vista, entre a imagem animada e o real. Filmar a vida: eis o que fizeram os operadores *Lumière*, cujas primeiras tomadas de cena testemunharam a saída de trabalhadores da usina que possuíam (que pode também ser lida como ancestrais da publicidade empresarial), a refeição deles com seus filhos (modelo do filme de família) assim como manifestações públicas ou de acontecimentos jornalísticos que rapidamente nutrirão os jornais de atualidades.

Ainda no século XX , “o cinema era considerado aquele da imagem em movimento e portador de uma relação intrínseca da história e da historicidade das artes que estão ligadas e ele”. Ultrapassou a problemática tradicional, que o considera como “fonte da história”, para uma incursão no domínio de uma história que se fará sob a influência do cinema e da imagem (NÓVOA, op. cit. p.81).

Além do mais, as publicações, os colóquios e as associações como a *International Association for Audiovisual Media in History* (IAMHIST), se multiplicam para afirmar a afinidade entre cinema e história e atestam, portanto, de uma causa assumida, ao termo de um longo debate. No que concerne às afirmações de princípio, foi considerado que ao prestar testemunho sobre o passado do qual elas conservavam os vestígios, as imagens cinematográficas ascenderam com pleno direito ao estatuto de documentos históricos (NÓVOA, op. cit. p. 99)

Com relação às narrativas cinematográficas, Nóvoa (2009) destaca os nomes dos principais teóricos dessa problemática entre eles, *Anton Kaes, Barbara Abrash, Daniel Walkowits, David Herling, Janet Sternberg, K. R. M. Short, Leslie Fishbein,*

Martin Jackson, Natalie Zamon Davis, Phil Rosen, R. J. Raack, Robert Brent Toplin, Robert Rosenstone, Shawn Rosenheim, Sumiko, Higashi e Vivian Shobchack. Partindo de uma visão geral da história, enquanto discurso, a maior parte desses autores defende que os audiovisuais são também formas discursivas capazes de representar o passado. Suas pesquisas caminham em algumas direções, tais como: valorizar academicamente os discursos históricos áudios-imagéticos (incluindo o cinema, o vídeo e mais recentemente as imagens digitais); estudar as características dos discursos audiovisuais e suas semelhanças e diferenças em relação a outros tipos de discursos históricos (historiografia escrita, Literatura, mito, memória, história oral); explorar as potencialidades introduzidas pelos discursos históricos áudios-imagéticos para a escrita da história e para os historiadores acadêmicos; refletir sobre a relação existente entre as representações históricas audiovisuais e a historiografia escrita; teorizar sobre as possibilidades dos historiadores de exporem seus conhecimentos através de dispositivos audiovisuais; investigar os componentes das narrativas históricas áudio-imagético; refletir sobre a questão do referencial e sobre o estatuto da ficção nos audiovisuais históricos; ou seja, sobre os tipos de realidade histórica representados em um audiovisual; analisar filmes ou conjunto de filmes como discursos históricos autônomos em relação à historiografia escrita e questionar os critérios de avaliação dos discursos históricos áudio-imagéticos. Esses autores defendem geralmente a ideia de que o cinema e o vídeo constituem-se (assim como a escrita e a oralidade) formas válidas e necessárias para representar o passado, mas buscando, ao mesmo tempo, refletir sobre suas peculiaridades (NÓVOA, 2009, p. 141).

O filme “O jogo da imitação, 2014” foi escolhido para análise no presente trabalho porque ajuda explicar o contexto da Segunda Guerra Mundial em relação à decifração do código alemão das máquinas Enigma. Nele, é possível perceber por meio da biografia de *Alan Turing*, o gigantesco esforço dos países Aliados para decifrar as mensagens secretas da Alemanha Nazista. *Turing* foi um dos grandes cientistas que ajudou a desvendar os segredos do sistema Enigma que possibilitou a vitória dos Aliados, capitaneados pela Inglaterra, Estados Unidos e União Soviética como se verá a seguir.

1.3 Análise fílmica: O Jogo da Imitação (2014)

O título do filme (em português) é: “O Jogo da Imitação”, cujo original “*The Imitation Game*”, lançado em 2014. Foi produzido por profissionais do Reino Unido e Estados Unidos. Quanto ao gênero, obteve classificação Biografia/Drama com duração de 114 min. A classificação etária é para maiores de 12 anos. Dirigido pelo norueguês *Morten Tyldum*, cuja produção contou com: *Nora Grossman*, *Ido Ostrowsky* e *Teddy Schwarzman*. O roteiro foi feito por *Graham Moore*. O elenco principal foi composto por: *Benedict Cumberbatch* (interpretando *Alan Turing*), *Keira Knightley* (interpretando *Joan Clarke*), *Matthew Goode* (interpretando *Hugh Alexander*), *Mark Strong* (interpretando o general *Stewart Menzies*), *Charles Dance* (interpretando o comandante *Alastair Denninston*), *Allen Leech* (interpretando *John Cairncross*), *Matthew Bard* (interpretando *Peter Hilton*), *Rory Kinnear* (interpretando o detetive *Nock*), *Alex Lawther* (interpretando o jovem *Alan Turing*) e *Jack Bannon* (interpretando *Cristopher Morcom*). A música, composta por *Alexandre Desplat*. *Óscar Faura* foi o responsável pela cinematografia e a edição foi feita por *William Goldenberg*.

No enredo, o filme mostra uma parte da trajetória do cientista e matemático inglês *Alan Turing* na infância, em 1927, no Colégio Interno até sua participação durante a Segunda Guerra Mundial (1939-1945), para trabalhar com um grupo de criptologistas em um local secreto chamado *Bletchley Park*, também conhecido como *Station X*, e decodificar as mensagens criptografadas pelas máquinas Enigma alemãs. Este filme demonstra como o domínio da informação pelos Ingleses foi crucial durante a Segunda Guerra Mundial. Os alemães que detinham a rede de comunicação mais segura do mundo no início do conflito. O cientista e matemático Inglês *Alan Turing* foi designado pelo governo Britânico junto com a equipe de cientistas para decifrar o código da máquina Enigma dos alemães. De posse de um modelo de uma máquina Enigma capturada pelos poloneses em Berlim, os cientistas Ingleses começaram o trabalho para decifrar o código da máquina Enigma. Os cientistas Ingleses conseguiram decifrar algumas palavras pela análise de frequência da distribuição das cartas, mas o volume de informações diárias tornava a tarefa quase impossível. As mensagens alemãs sempre começavam com cinco letras aleatórias; entretanto, alguns operadores alemães colocavam nomes próprios

no início das mensagens, com isso, as tornavam decifráveis pela posição das letras e era possível gerar a chave criptográfica do dia. Sob o nome código “Ultra”, um dos maiores serviços de inteligência da história, os Ingleses puderam decifrar diversas mensagens criptografadas pela máquina Enigma alemã. Outra questão em jogo seria escolher alguns ataques contra os alemães para eles não desconfiarem que o código da máquina Enigma tinha sido decifrado.

Segundo o filme “O jogo da imitação, 2014”, *Alan Turing* descobriu quem era o espião soviético na equipe de *Bletchley Park* e este agente sabia que *Alan Turing* era homossexual. Stewart Menzies já sabia que o John Cairncross era o traidor e espião soviético. Menzies permitia que Cairncross levasse algumas informações secretas para os soviéticos porque sabia que o Primeiro Ministro Winston Churchill não permitiria este tipo de ação. Cairncross ameaçou contar para o Comandante Deninnston que Turing era homossexual se ele contasse sobre a espionagem soviética.

Como o homossexualismo era proibido na Grã-Bretanha na época da Segunda Guerra Mundial, *Alan Turing* foi obrigado a fazer um tratamento hormonal e suicidou-se em 07 de Junho de 1954 com 41 anos. Entre 1855 e 1967, aproximadamente 49 mil homens homossexuais foram condenados por atentado ao pudor segundo a lei Britânica. Em 2013, a Rainha *Elizabeth II* concedeu a *Turing* um perdão real póstumo (Anexo A) pelos seus préstimos e conquistas sem precedentes. Segundo alguns Historiadores, com a decifração do código da máquina Enigma, foram salvas 14 milhões de pessoas e encurtou a Segunda Guerra Mundial em dois anos. *Alan Turing* desenvolveu um conceito de uma máquina universal chamada “máquina de Turing” e estes conceitos apresentados em 1936 foram usados na criação das bombas de criptografia presentes no filme capazes de decifrar qualquer cifragem da máquina Enigma. O filme O Jogo da Imitação foi baseado no livro intitulado “*Alan Turing*: The Enigma” de *Andrew Hodges”*.

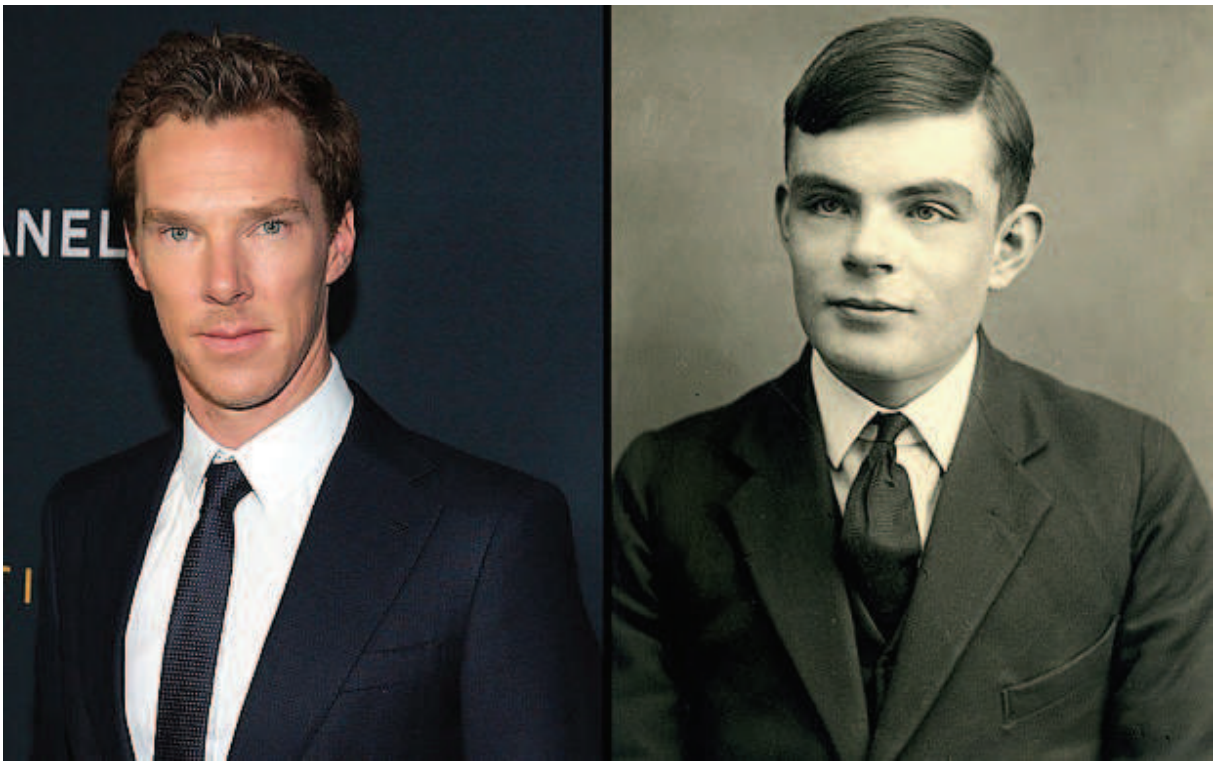
O filme “O jogo da imitação, 2014” recebeu 8 indicações ao “Oscar” incluindo melhor filme, melhor diretor, melhor ator, melhor atriz coadjuvante, melhor roteiro adaptado. Foi vencedor do “Oscar” de melhor roteiro adaptado.

Nesta pesquisa, citado anteriormente, o objetivo principal é análise fílmica do Jogo da Imitação. Algumas imagens foram selecionadas para explicar o processo de criptografia da máquina Enigma utilizado por Turing e, na sequência, as que contextualizaram o cenário da Segunda Guerra Mundial.

1.3.1 Os Personagens

Nas figuras seguintes, descrever-se-á os principais personagens do filme por sequência, a começar pelo protagonista *Alan Turing*.

Figura 1 – Ator Benedict Cumberbatch (esquerda) interpretando Alan Turing (direita) no filme “O jogo da imitação, 2014”



Fonte: http://i.telegraph.co.uk/multimedia/archive/03102/CELEB-RELATIVES-1_3102821b.jpg

Alan Turing (1912-1954), protagonista no filme, foi um matemático e criptoanalista inglês que trabalhou para o Governo Britânico em *Bletchley Park* com

intuito de decifrar os códigos secretos que os alemães utilizavam em uma máquina de cifragem chamada Enigma, durante a Segunda Guerra Mundial.

Turing aperfeiçoou uma máquina polonesa chamada “bomba” e apelidou-a, inicialmente, de “Cristopher”- amigo de colégio - que decifrava os códigos da máquina Enigma usada pelos alemães. Os historiadores acreditam que seu trabalho pode ter encurtado a guerra em dois anos.

É considerado o pai da ciência da computação, além de várias contribuições em outras áreas do conhecimento, tais como a inteligência artificial, formalização do conceito de algoritmo, a máquina universal de Turing e publicou artigos na área da química. Segundo Tyldum (2014) “O verdadeiro Enigma era o homem que ‘quebrou’ o código.” (TELEGRAPH, 2016, Trad. nossa)

Outro personagem importante, no enredo, é Comandante *Alastair Denniston*, conforme (fig. 2).

Figura 2 – Comandante Alastair Denniston (esquerda) sendo interpretado pelo ator Charles Dance (direita) no filme “O jogo da imitação, 2014”

Fonte: http://i.telegraph.co.uk/multimedia/archive/03119/PX11371353wa_bletc_3119528b.jpg

O Comandante *Alastair Denniston* da Marinha Real Britânica, foi criptólogo durante a Primeira Guerra Mundial (1914-1918) além de dominar o idioma alemão. Continuou o trabalho com criptografia na Escola de Cifras e Código do Governo que foi a precursora do GCHQ (*Government Communications Headquarters*) depois e mudou sua equipe para *Bletchley Park* no início da Segunda Guerra Mundial. Lá, foi responsável por contratar os matemáticos que quebrariam o código Enigma, incluindo *Alan Turing*. Morreu em 1961. (TELEGRAPH, 2016, Trad. nossa)

Conforme (fig. 3), apresenta-se o personagem *Conel Hugh O'Donel Alexander* destaque na equipe do Comandante *Alastair Denniston*.

Figura 3 – Campeão mundial de xadrez Conel Hugh O'Donel Alexander (esquerda) sendo interpretado pelo ator Matthew Goode (direita) no filme “O jogo da imitação, 2014”

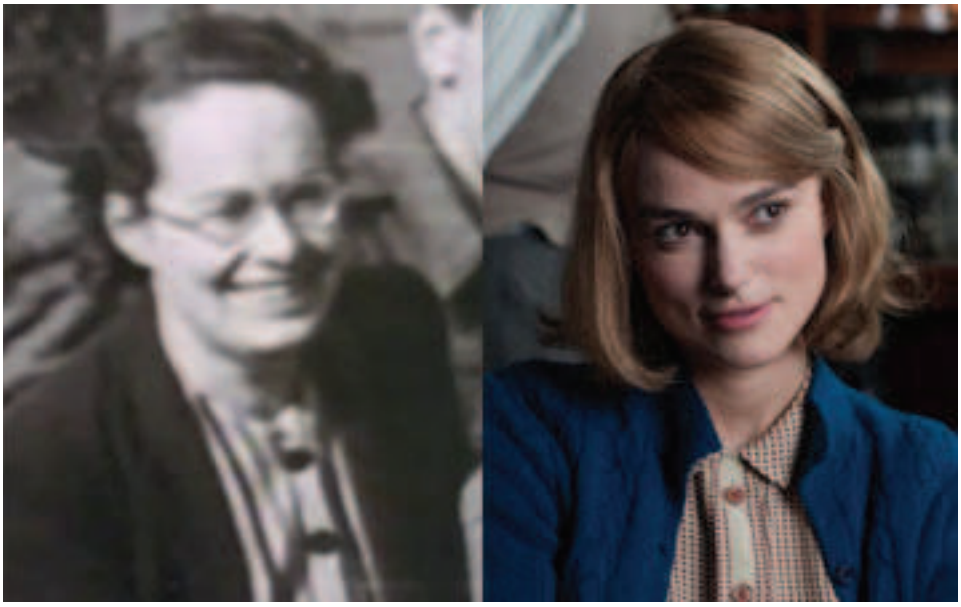
Fonte:http://www.telegraph.co.uk/content/dam/films/2016/07/29/hughalexander__3106146c-large_trans_NvBQzQNjv4Bq6f7LZ7seCW96zliyTYX6ViIMpBIiS72GQ3QPBtusw-s.jpg

Como muitos decifradores de código (*codebreakers*), *Hugh Alexander* ficou em primeiro lugar em matemática em *Cambridge*. Foi campeão britânico de xadrez duas vezes e campeão em um torneio internacional. Fez importantes contribuições para duas estratégias clássicas de xadrez: "*the Dutch defence* ou a defesa holandesa" e a "*Petroff defence* ou defesa Petroff".

Ele era conhecido na imprensa em *Bletchley Park* como C.H.O'D e seu nome completo era *Conel Hugh O'Donel Alexander*. Em 1941, ele foi transferido para *Hut* 8 (cabana 8) e tornou-se vice de *Turing*. (TELEGRAPH, 2016, Trad. nossa)

Na sequência, apresenta-se a personagem *Joan Elisabeth Lowther Clarke Murray*, assim como *Alexander*, ficou em primeiro lugar em matemática em *Cambridge*; ao contrário dele, quando foi recrutada para *Bletchley Park* foi lhe dito que o seu trabalho não exigiria realmente matemática.

Figura 4 – Criptoanalista Joan Clarke (esquerda) sendo interpretada pela atriz Keira Knightley (direita) no filme “O jogo da imitação, 2014”



Fonte: http://pic.pimg.tw/ethanwang55/1425041049-2216132466.jpg

Seus dons matemáticos levaram-na a se tornar a única mulher na equipe de nove bamburistas. E de acordo com seu chefe, *Alexander*, ela era "uma das

melhores bamburistas na seção". *Alan Turing* teve um rápido romance com Joan Clarke mas o relacionamento não progrediu. (TELEGRAPH, 2016, Trad. nossa)

Outras mulheres também trabalharam com criptoanálise em *Bletchley Park* como *Margaret Rock* e *Mavis Lilian Batey* que ajudaram na decifragem do código da máquina Enigma do serviço secreto alemão (Abwehr).

Outro personagem foi *Stewart Menzies*, (fig. 5) marcado pela introdução do sistema “Ultra” (Sistema de Inteligência dos Aliados).

Figura 5 – Stewart Menzies (esquerda) sendo interpretado pelo ator Mark Strong (direita) no filme “O jogo da imitação, 2014”

Fonte:http://www.telegraph.co.uk/content/dam/films/2016/07/29/menzies_3106163c-large_trans_NvBQzQNjv4Bq6f7LZ7seCW96zliyTYX6VilMpBIiS72GQ3QPBtusw-s.jpg

No início da guerra ele se tornou "C", o chefe do MI6. Embora não fosse um *codebreaker*, era *Menzies* que comandava *Bletchley Park*, e foi ele que introduziu o que foi chamado Ultra. Se muitas das interceptações de *Bletchley Park* fossem

cumpridas, os alemães suspeitariam que os códigos Enigma haviam sido decifrados. *Menzies*, portanto, introduziu um sistema que significava apenas uma certa percentagem da inteligência recolhida a partir de decodificação seria passada para o Exército Britânico, Marinha Real e RAF (*Royal Air Force* ou Força Aérea Real). (TELEGRAPH, 2016, Trad. nossa)

John Cairncross (Fig. 6), falava o idioma alemão, estudou linguística, amante de música; fato incomum para os decifradores de códigos. Era espião soviético.

Figura 6 – John Cairncross (esquerda) sendo interpretado pelo ator Allen Leech (direita) no filme “O jogo da imitação, 2014”

Fonte:http://www.telegraph.co.uk/content/dam/films/2016/07/29/johncairncross_3106107c-large_trans_NvBQzQNjv4Bq6f7LZ7seCW96zliyTYX6VilMpBIiS72GQ3QPBtusw-s.jpg

No filme, *Menzies* sabia exatamente o que o espião *John Cairncross* estava fazendo na Estação X. Ele admitiu espionar em 1951 quando *Guy Burgess* fugiu para Moscou e MI5 encontrou uma nota manuscrita dele no apartamento de *Burgess*. *Cairncross* chegou em *Bletchley Park* em 1942 e foi trabalhar em *Hut* 3

(cabana 3) em comunicações de grupo de exército da Alemanha. Incomum para um *codebreaker*, ele estudou línguas em *Cambridge*, ao invés de matemática.

Durante toda Segunda Guerra Mundial, *Cairncross* passou documentos através de canais secretos para agentes da KGB (Comité de Segurança do Estado), que lhe deram o nome de código *Liszt*, por causa de seu amor pela música. Ele contrabandeou mensagens decifradas em suas calças, transferindo as para sua bolsa na estação ferroviária. Mas a verdade é provavelmente mais ambígua do que este resumo de sua traição permite. Os Aliados queriam que os soviéticos conhecessem certos planos de batalha alemães, mas não de onde veio a inteligência. Afinal, eram nossos aliados em tempo de guerra. Dada a forte segurança em *Bletchley Park*, há especulações de que *Menzies* organizou determinados documentos para que *Cairncross* enviasse para os soviéticos. (TELEGRAPH, 2016, Trad. nossa).

Em seguida (Fig. 7), Peter Hilton, personagem que estudou em *Oxford* e *Cambridge*.

Figura 7 – Peter Hilton (esquerda) sendo interpretado pelo ator Matthew Beard (direita) no filme “O jogo da imitação, 2014”

Fonte:http://www.telegraph.co.uk/content/dam/films/2016/07/29/peterhilton_3106100c-large_trans_NvBQzQNjv4Bq6f7LZ7seCW96zliyTYX6ViIMpBIiS72GQ3QPBtusw-s.jpg

Aluno notável, foi recrutado em 1942 com a tenra idade de 18 anos, porque ele também sabia alemão (uma língua aprendida em um ano, na universidade). Trabalhou ao lado de *Alan Turing* em *Hut* 8, na Enigma Naval e, graças a seu extraordinário poder de visualização, foi capaz de comparar dois fluxos de caracteres de dois *telex*[1] ao mesmo tempo. Essa característica de *Hilton* se revelou vital quando os alemães introduziram um novo sistema de cifra de *telex* produzido por uma máquina muito maior e mais complexa do que a máquina Enigma. Muitos anos após a guerra, este segredo fora revelado.

A outra máquina de cifragem dos alemães era a *Lorenz* SZ40, mas, naquele tempo, o pessoal em *Bletchley Park* o chamou "*Tunny*". A máquina *Lorenz* SZ40 não foi mostrada no filme “O jogo da imitação, 2014”. Apenas a máquina Enigma Naval foi retratada. (TELEGRAPH, 2016, Trad. nossa)

O próximo personagem (Fig. 8) é *Jack Good*, matemático de *Cambridge* que trabalhava com *Alan Turing* no *Hut* 8. Isso foi muito bem porque ele decifrou um código vital em seu sono, com a solução vindo a ele em um sonho. Nele se perguntava se as letras que os telegrafistas alemães deviam acrescentar às suas mensagens para transmiti-las eram aleatórias ou se havia uma tendência para as letras particulares. Depois de inspecionar algumas mensagens que tinham sido quebradas, ele descobriu que havia uma tendência para usar algumas letras mais do que outros. Assim sendo, todos os decifradores de código (*codebreakers*) tinham que fazer era trabalhar os indicadores fornecidos no início de cada mensagem, e aplicar cada tabela bigrama por sua vez. A tabela do bigrama que produziu uma das letras populares era provavelmente a correta.

[1] Rede mundial com um plano de endereçamento numérico, com terminais únicos que poderia enviar uma mensagem escrita para qualquer outro terminal. Fonte: https://pt.wikipedia.org/wiki/Telex

Figura 8 – Jack Good (sentado a direita) sendo interpretado pelo ator James Northcote no filme “O jogo da imitação, 2014”

Fonte:http://www.telegraph.co.uk/content/dam/films/2016/07/29/Jack_Good_3105785c-large_trans_NvBQzQNjv4Bq6f7LZ7seCW96zliyTYX6ViIMpBIiS72GQ3QPBtusw-s.jpg

Quando *Good* (interpretado por *James Northcote* no filme) mencionou sua descoberta a *Turing*, o gênio se sentiu envergonhado e disse: "Eu poderia jurar que já tentei isso." Tornou-se rapidamente uma parte importante do procedimento Bamburismo. Depois da guerra, *Good* tornou-se professor e trabalhou como consultor de *Stanley Kubrick* no filme de 1968, 2001: *A Space Odyssey* (2001: Uma odisseia espacial). Ele nunca adivinhou a orientação sexual de *Turing* em todo o tempo em que eles trabalharam juntos, e tampouco as autoridades de *Bletchley Park*. "Caso contrário", como *Good* observou de forma natural, "*Turing* pode ter sido levado a matar-se mais cedo, e nós poderíamos ter perdido a guerra." (TELEGRAPH, 2016, Trad. nossa)

1.3.2 Alan Turing antes, durante e após a Segunda Guerra Mundial.

O filme: “O jogo da imitação” começa com o interrogatório de Alan Turing pelo detetive *Robert Nock* da polícia de *Manchester* no ano de 1951. O narrador do filme é o próprio *Alan Turing* que contará sua trajetória antes e durante a Segunda Guerra Mundial. O diálogo inicial entre *Alan Turing* e *Robert Nock* está descrito após a figura 9.

Figura 9 – Início do filme: “O jogo da imitação, 2014”. Alan Turing sendo interrogado

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (01:35).

> **Turing**: Está prestando atenção? Que bom. Se não prestar bastante atenção perderá os detalhes. Detalhes importantes. Eu não vou parar, não vou repetir e o Sr. não vai me interromper. Acha porque está onde está e porque onde eu estou, o Sr. está no controle dos acontecimentos? O Sr. está errado. Eu estou no controle porque eu sei de coisas que o Sr. não sabe. O que quero do Sr. é compromentimento. O Sr. vai prestar atenção e não vai me julgar até terminar. Se não for se dedicar a isso por favor saia daqui. Mas se escolher ficar lembre-se de que foi uma escolha sua. O que acontecer daqui para frente não é de minha responsabilidade. É sua. Preste atenção. (MORTHEN TYLDUN, 2014).

Ele foi um filho do Império e da classe média inglesa. Seu pai Julius, foi membro do Serviço Civil da Índia e foi em *Chatrapur*, perto de Madras, que *Turing* foi concebido. *Julius* e *Ethel Sara Turing* retornaram depois à Inglaterra, onde seu segundo filho nasceu, no dia 23 de junho de 1912, em um pequeno hospital em *Paddington*. Seu nome completo era *Alan Mathison Turing*. Quando tinha 6 anos, foi mandado para uma pequena escola chamada *Hazelhurst*. Depois de *Hazelhusrt* ele foi levado para *Sherborne*, uma das primeiras escolas públicas. Foi em *Sherborne* que ele primeiro começou a demonstrar a teimosa disposição para tomar tudo literalmente, e que mais tarde o colocaria em tantas dificuldades, mesmo que também levasse a alguns de seus avanços intelectuais mais surpreendentes (LEAVITT, 2007, p. 16).

De acordo com Fante (2005), o *bullying* é um fenômeno mundial tão antigo quanto a própria escola. Apesar de os educadores terem consciência da problemática existente entre agressor e vítima, poucos esforços foram despendidos para o seu estudo sistemático até o princípio da década de 1970. Foi nessa época que surgiu, primeiramente, na Suécia, um grande interesse de toda a sociedade pelos problemas desencadeados entre agressor e vítima, figurantes desse fenômeno, que logo se estendeu por todos os outros países escandinavos.

Figura 10 – Jovem *Alan Turing* sofrendo *bullying* na *Sherborne School* em 1928

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (25:49).

As características citadas podem ser percebidas na (Fig. 10), e posteriormente, confirmadas nas palavras de Turing. O próprio personagem de *Alan Turing* narra o *bullying* sofrido na *Sherborne School* durante a juventude em 1928.

> **Turing**: - Sabe por que as pessoas gostam de violência? Porque a sensação é boa. Os humanos acham a violência prazerosa. Tire essa satisfação e o ato se torna vazio.
> **Aluno veterano**: -Turing? Anda. Não seja tão chorão.
> **Outro aluno veterano**: Deixe-o apodrecer aí.
> **Turing**: - Não aprendi isso sozinho, é claro. Recebi ajuda. Christopher me ajudou.
> **Christopher**: - Alan, você está bem?
> **Turing**: -Não é culpa minha. As cenouras se misturaram com as ervilhas e... Desculpe, não deixarei que façam isto de novo.
> **Christopher**: - Estão piorando.

> **Turing**: - Só me bateram porque sou mais inteligente.
> **Christopher**: - Não, bateram em você porque é diferente.
> **Turing**: -Minha mãe diz que sou singular. Ela está certa.
> **Christopher**: Mas, às vezes, aqueles de quem menos esperamos fazem coisas que nunca imaginamos.
> (MORTHEN TYLDUN, 2014)

Ainda na figura 10, o ator *Alex Lawther* interpretou *Alan Turing* durante a juventude. Alguns alunos veteranos colocaram *Alan Turing* embaixo das tábuas de uma sala de aula e pregaram as tábuas deixando-o aterrorizado em um primeiro momento. Enquanto *Turing* pedia por socorro, os alunos veteranos se vangloriavam com o sofrimento dele. De repente Turing cessa os pedidos de ajuda e fica em silêncio deixando os alunos veteranos perplexos. Em seguida os alunos veteranos foram embora e o amigo e colega de classe *Christopher Morcom* conseguiu libertar *Turing*.

O *bullying* é uma realidade mais comum do que podemos imaginar. O mesmo sempre existiu, mas não era estudado, e quando acontecia, a vítima sofria calada ou mudava de escola (CALHAU, 2011). A esse respeito, Nogueira (2005) diz que no momento em que os filhos começam a frequentar a escola pode surgir o *bullying,* como um fenômeno cruel e silencioso, comprometedor do pleno desenvolvimento do indivíduo por suas consequências psicológicas, emocionais, sociais e cognitivas que se estendem para além do período acadêmico e, por isso, considerado epidêmico. Na figura 11, *Turing* tem o primeiro contato com o livro de Criptografia lido por *Chistopher Morcon*, seu amigo que no momento tivera a percepção que ele seria muito bom no assunto.

> **Turing:** - O que está lendo?
>
> **Christopher**: - É sobre criptografia.
>
> **Turing**: - Tipo mensagens secretas?
>
> **Christopher**: - Não secretas. Essa é a beleza. Mensagens que todos veem, mas ninguém entende a menos que tenha a senha.
>
> **Turing**: - Qual a diferença de falar?
>
> **Christopher**: - Falar?
>
> **Turing: -** Quando as pessoas conversam nunca falam o que querem. Dizem outra coisa e esperam que você entenda o que querem dizer. Mas eu nunca entendo. Então, qual é a diferença...
>
> **Christopher:** - Alan, algo me diz que você será muito bom nisso. (MORTHEN TYLDUN, 2014)

Figura 11 – *Christopher Morcom* apresentando o tema criptografia a Alan Turing

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (32:41).

Durante a Segunda Guerra Mundial, *Turing* se matriculou na infantaria da *home guard* para que pudesse aprender a atirar. O melhor amigo de *Turing* em *Sherborne* foi *Christopher Morcom*, como ele, um adolescente prodigiosamente dotado para as ciências, e que ele conheceu em 1928.

Christopher Morcon provavelmente não era homossexual. Se a relação tivesse continuado além de *Sherborne* e até *Cambridge*, onde *Morcom* tinha conseguido uma vaga no *Trinity College* que *Turing* cobiçava, ela poderia ter chegado ao mesmo final de muitas de suas amizades, com o avanço físico sendo gentilmente, mas firmemente, repelido. Mas então, em 1930, antes que pudesse começar a estudar em *Trinity*, *Christopher Morcom* morreu de tuberculose (LEAVITT, 2007, p.23).

No outono de 1931, *Turing* matriculou-se no *King's College*, em Cambridge, onde lhe foi dado um aposento em *Bodley's Court*. À primeira vista, o *King's College* parecia o lugar ideal para um jovem matemático homossexual.

O clima para homens e mulheres homossexuais na Inglaterra nos anos de 1930 estava longe de ser tolerante.

Entre os temas mais constantes, além das interrogações sobre a natureza e estatuto do corpo, encontra-se o questionamento sobre seus limites, sobre as antigas, apaziguadoras e hoje duvidosas fronteiras entre o individual e social, masculino e feminino, vida e morte, natureza e cultura, natural e artificial, presença e ausência, atualidade e virtualidade. Espraiado e multiplicado em experiências divergentes e até mesmo incompatíveis e incongruentes, o corpo revela que nunca foi, na realidade, puramente natural ou estável, colocando a nu a pretensa ilusão de sua unificação, ao intercambiar e confundir de modo surpreendente as dicotomias entre interioridade e exterioridade, eu e outro, passado e futuro (SANTAELLA, 2004, p. 28).

A partir da figura 12 vamos mostrar o início da Segunda Guerra Mundial e suas consequências. Na figura 13 observamos um local chamado "*Bletchley Radio Manufacturing*" onde foi reunido grande número de cientistas, matemáticos, linguistas, engenheiros com o objetivo de decifrar o código secreto da máquina de cifragem alemã Enigma.

Figura 12 – 1939 - Início da Segunda Guerra Mundial – Evacuação das crianças de Londres

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (05:48).

Ao perceber que a Inglaterra seria suscetível a ataques aéreos em tempos de guerra, o governo britânico desenvolveu um complexo esquema para evacuar crianças de cidades vulneráveis para o interior. Algumas evacuações levaram crianças para lugares tão distantes quanto o Canadá (JORDAN et al, 2008, p. 39).

Turing se juntou ao *Anti-War Council* (Conselho anti guerra), cujo objetivo era organizar os trabalhadores da indústria química e de munição a fazer greve se a guerra fosse declarada, e fez uma palestra sobre “Matemática e Lógica” em frente ao *Cambridge University Moral Sciences Club* (Clube da Ciências Moral da Universidade de Cambridge). Alan Turing era agnóstico a violência e política e poderemos ver estas características sendo mostradas na entrevista entre o Comandante Denninston e Alan Turing em Bletchley Park na figura 18.

Figura 13 – A placa diz: “Fábrica de rádios Bletchley”

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (07:53).

> Era vital conseguir descifrar esos mensajes (máquina Enigma). De este trabajo se encargaría la Escuela de Códigos del Gobierno, radicada en una mansión victoriana llamada Bletchley Park, situada a 70 kilómetros de Londres y a 100 kilómetros de la playa de invasión más próxima, para que pudiera seguir operando aunque los alemanes hubieran desembarcado ya en las islãs britânicas. En unos barracones construídos al lado de la casa principal se encontraba un

> grupo de expertos cuya única misión era lograr la clave de funcionamiento de aquella misteriosa máquina. El heterógeno equipo estaba formado por matemáticos, linguistas, maestros de ajedrez e incluso expertos en crucigramas de las universidades de Oxford y Cambridge. Trabajaron durante meses, pero la Enigma seguía haciendo honor a su nombre; era virtualmente imposible descubrir la clave (HERNÁNDEZ, 2016, p. 29).

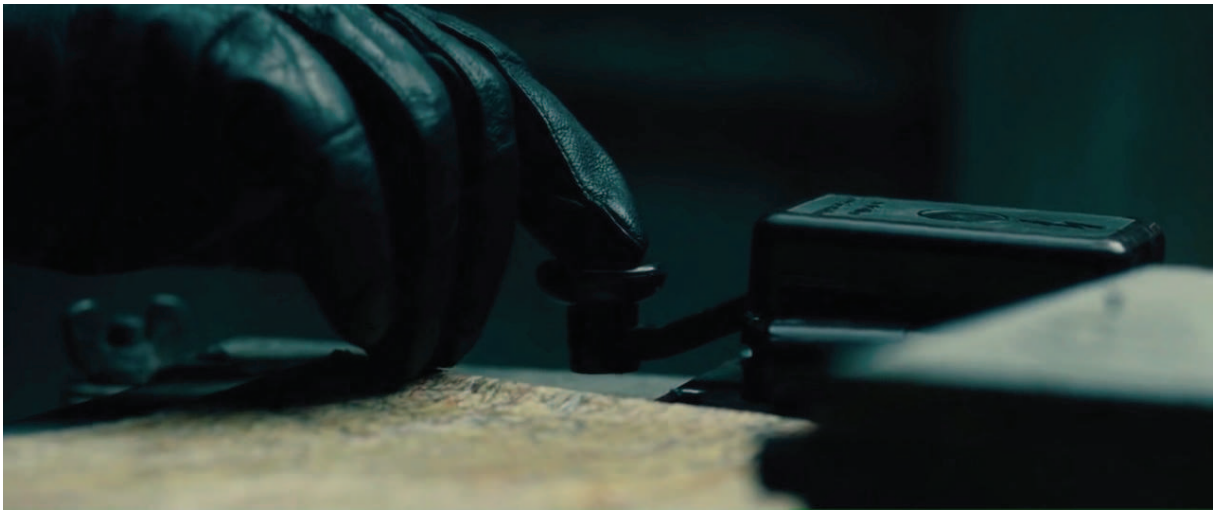
O proprietário de Bletchley Park morreu em 1937 e a propriedade foi comprada pelo financista Sir Hernert Leon. Um ano depois foi adquirida por outra pessoa que parecia ser um cavalheiro do exército ou marinha acompanhado por um grupo chamado “equipe de tiro do capitão Ridley”. Quem comprou Bletchley Park por 7.500 libras foi o almirante Sir Hugh Sinclair, chefe do MI6 e da Government Code and Cipher School (Escola de Cifras e Código do Governo). O local seria conhecido pelo misterioso nome de Station X. O “X” representava em algarismos romanos o número 10 que indicava o décimo local que o MI6 estava operando. Sua missão era quebrar os códigos secretos do inimigo, ler suas transmissões e passar seus planos para o Governo Britânico. Os cavalheiros misteriosos ocupariam o lugar por quase dez anos e uma população aumentando para mais de 10 mil homens e mulheres, civis e militares. Outro desafio era encontrar e mobilizar as melhores mentes disponíveis na Grã-Bretanha e entre os aliados além de criar condições físicas para uma melhor eficiência no trabalho de decifragem (PATERSON, 2009, p. 57).

Figura 14 – Avião de reconhecimento alemão

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (15:07).

Bombardeiro médio Dornier Do 17 (alemão) equipado com a máquina de cifragem Enigma e equipamento de rádio patrulhando as águas do Oceano Atlântico. De acordo com a figura 15, um observador alemão utiliza um binóculo para localizar formações de comboios Aliados que estavam chegando na Grã-Bretanha pelo Oceano Atlântico. O observador alemão marca no mapa a localização do comboio. Em seguida escreve a mensagem no idioma alemão. O próximo passo é digitar esta mensagem na máquina de cifragem Enigma a bordo do avião. O código cifrado é codificado em código Morse e transmitido para o submarino alemão (*U-Boot*) mais próximo utilizando um rádio transmissor.

Figura 15 – Operador de rádio utilizando código morse para enviar e receber mensagens



Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (15:19).

"O código Morse é um código padronizado, reconhecido internacionalmente. É composto por conjuntos de traços (sons longos) e pontos (sons curtos) que correspondem às letras do alfabeto latino, aos dígitos e alguns sinais gráficos. Para outros alfabetos, diferentes do alfabeto ocidental, também existem códigos específicos" (TKOTZ, 2005, p.324).

Equipamento de código Morse era usado para enviar mensagens encriptadas pela máquina de cifragem Enigma entre as forças militares alemãs. Inúmeros países

utilizavam código Morse em suas comunicações e geralmente não utilizavam criptografia. As mensagens eram compostas de palavras do próprio idioma do país. No caso dos alemães, as mensagens eram encriptadas pela máquina de cifragem Enigma e depois transmitidas usando código Morse o que tornava as mensagens ininteligíveis para quem interceptasse as mensagens. Ter apenas a máquina Enigma não adiantava pois era necessário ter o livro de códigos e as configurações iniciais que o operador da máquina Enigma escolhia antes de enviar cada mensagem.

Figura 16 – Máquina Enigma sendo utilizada em um submarino alemão

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (15:30).

Máquina de cifragem Enigma Naval com 4 rotores sendo usada dentro de um submarino alemão durante a Segunda Guerra Mundial.

> Gracias a este aparato (máquina Enigma), los submarinos alemanes destinados en el Atlántico podían comunicarse entre ellos y con su país, logrando una coordinacíon que estaba costando el hundimiento de muchos barcos a los aliados. La existencia de esta máquina era fundamental para la táctica empleada por los submarinos alemanes, conocida como la “jauría de lobos”. Consistía en la presencia continua de unos quince submarinos en alta mar, colocados estrategicamente

> en las rutas que solían seguir los convoyes aliados. Estos submarinos estaban separados entre sí por largas distancias, con lo que conseguían cobrir zonas muy amplias (HERNÁNDEZ, 2016, p. 28).

Quando um dos submarinos alemães avistava uma presa que poderia ser um comboio ou um navio isolado, comunicava a sua base a rota que o inimigo estava seguindo. A base alemã avisava os submarinos disponíveis para que convergissem sobre o objetivo em um ponto do oceano, normalmente a noite. Quando chegava o momento, todos os submarinos reunidos para a ocasião, começavam a disparar seus torpedos (HERNÁNDEZ, 2016, p. 28). Se não se conseguia afundar o barco inimigo, seguiam-no a uma distância prudente e quando chegava a noite, recomeçavam a lançar seus torpedos até conseguirem afundá-lo.

> Esta táctica era tremendamente eficaz. Con esos pocos efectivos distribuídos por el inmenso océano se mantenía en jaque a toda la flota aliada, que se veía incapaz para proteger a todos los barcos que cruzaban el Atlántico. Para que esa técnica de "jauría de lobos" pudiese llevarse a cabo era necessario contar con el factor sorpresa. Los aliados necesitaban contar con un sistema que pudiera localizar la posición de los submarinos nazis y conocer de antemano el lugar de reunión. En ese caso, los "lobos" caerían en una trampa mortal y se acabaría la amenaza. Ése era el objetivo, pero ¿como conserguirlo? Sólo había una respuesta: descubrir el significado de los mensajes enviados a través de la Enigma (HERNÁNDEZ, op.cit., p. 28).

No episódio conhecido como a Batalha do Atlântico (3 de setembro de 1939 até 8 de maio de 1945) entre os Aliados e os países do Eixo pelo domínio do Oceano Atlântico, durou praticamente toda a Segunda Guerra Mundial. Os alemães como na Primeira Guerra Mundial queriam isolar a Grã-Bretanha de receber suprimentos e forçar sua rendição. Estados Unidos, Canadá e as colônias inglesas enviavam suprimentos para a Grã-Bretanha para resistir aos ataques alemães. Quando os alemães invadiram a União Soviética em 22 de junho de 1941, os

Estados Unidos começaram a enviar suprimentos para a União Soviética através do porto de *Murmansk*.

Paterson (2009, p. 119) nos informa que no início da Segunda Guerra Mundial, os alemães conseguiram decifrar mensagens da Marinha Real Inglesa com codinome “cifradora número 3”. Estes códigos ingleses eram usados para organizar os comboios, as rotas, pontos de reunião e horários de navegação. Por muitos meses os ingleses não conseguiram decifrar mensagens da Kriegmarine (Marinha Alemã) que eram mais complexos que os dos outros serviços. A Kriegsmarine possuía 13 códigos diferentes que depois chegariam a 40 dos quais os criptoanalistas de Bletchley Park nunca conseguiram decifrar. Por exemplo: o AEGIR era o código para os navios da frota de superfície, HYDRA para os submarinos operacionais e TETIS para os que estavam em treinamento no Mar Báltico.

Segundo Masson (2015, p. 554), Bletchley Park contribuiu na Batalha do Atlântico com informações que aumentaram a segurança dos comboios e melhorou o serviço de localização de submarinos alemães. De 1940 a 1943, os ingleses souberam explorar a falha da tática das “alcatéias” com a utilização intensiva das comunicações pelo rádio. O código secreto da máquina Enigma naval foi decifrado duas vezes. De início, durante o segundo semestre de 1941. Os alemães modificaram a máquina Enigma e as cifras de condinome “Triton”. A segunda decifração ocorreu em novembro de 1942. Em março de 1943 os criptoanalistas de *Bletchley Park* não conseguiram decifrar as mensagens da marinha alemã novamente mas a captura de máquinas Enigma e seus livros de cifras a bordo de dois submarinos alemães avariados contribuiu para retomar o serviço de decifragem das mensagens.

Figura 17 – Navio Aliado sendo afundado por submarino alemão

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (39:02).

Os alemães tinham a disposição um submarino tipo VIIC que era considerado o mais avançado do mundo. Desenvolvido em 1938, tinha uma autonomia de 13.676 Km, possuía um canhão de 88 mm, 14 torpedos que podiam ser disparados da popa ou proa. A Alemanha iniciou a Segunda Guerra Mundial com 56 unidades deste submarino tipo VIIC. O navio transatlântico Athena foi afundado por um submarino alemão no dia 3 de setembro de 1939 e entre os 118 passageiros mortos, 22 eram americanos. No três primeiros meses do conflito, os alemães afundaram 114 navios mercantes (PATERSON, 2009, p. 118).

> Ao flagelo dos submarinos logo veio somar-se a ataque aéreo em águas oceânicas, feito por aviões de longo alcance. Dentre eles, o Focke-Wulf 200, conhecido como Condor, era o mais impressionante, embora a princípio, felizmente, existisse em pequeno número. Esse aviões podiam decolar de Brest ou Bordeaux, fazer um vôo contornando as Ilhas Britânicas, reabastecer na Noruega e, no dia seguinte, fazer a viagem de volta. No caminho, viam lá embaixo os enormes comboios de quarenta ou cinquenta embarcações, a que a escassez de navios de escolta nos obrigara a recorrer, deslocando-se para terra ou para alto-mar em suas viagens. Os aviões podiam

> bombardear esses comboios ou navios isolados, ou ainda indicar as posições para onde deveriam dirigir-se os submarinos que estavam à espera, para que fizessem a interceptação (CHURCHILL, 1995, p. 472).

Com o início da Segunda Guerra Mundial, o governo da Grã-Bretanha acelerou o recrutamento de matemáticos, linguistas e criptoanalistas com o objetivo principal de decifrar os códigos secretos da máquina Enigma alemã. É neste contexto que o comandante *Alastair Denniston* conhece Alan Turing.

Alan Turing depois de recusar uma oferta para trabalhar como assistente de *John von Neumann* na Universidade *Princeton* nos Estados Unidos (com um salário de 1.500 dólares por ano), ele retornou à Inglaterra no outono, onde foi convocado para um curso de criptografia e encriptação conduzido pela *Government Code and Cipher School*, em Londres. De alguma forma, seu interesse por códigos e quebras de código, sem mencionar seu talento para a matemática, tinha chegado aos ouvidos do comandante *Alastair Denniston*, o diretor da escola (LEAVITT, 2007, p. 151).

John Von Neumann (1903-1957) nascido na Hungria mas naturalizado estadunidense foi considerado um dos maiores matemáticos do século XX. Suas contribuições científicas abrangem a matemática, ciência da computação, economia, teoria dos jogos e mecânica quântica.

Apresentamos a seguir o diálogo entre o comandante *Denninston* e *Alan Turing*, de acordo com o filme, sobre proposta de trabalho para este último. A figura 18 ilustra o momento da entrevista e Alan Turing é contratado para o esforço de guerra para decifrar o código secreto da máquina de cifragem alemã Enigma.

Figura 18 – Comandante Alastair Denniston entrevista Alan Turing em Bletchley Park

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (08:50).

Denninston: - Comandante Denninston, Marinha Real. Vou lhe dar uma chance, Senhor Turing. Por que quer trabalhar para o Governo de Vossa Majestade?

Turing: - Na verdade não quero.

Denninston: - É um maldito pacifista?

Turing: - Sou agnóstico à violência.

Denninston: - Mas sabe que a 1000 quilômetros de Londres há um “baixinho emburrado” chamado Hitler que quer afundar a Europa em tirania?

Turing: - Política não é minha especialidade.

Denninston: - É mesmo? Acaba de participar da mais breve entrevista da História do Exército Britânico.

Turing: - Minha mãe diz que as vezes sou arrogante por ser o melhor Matemático do mundo.

Denninston: - Do mundo?

Turing: - Sim.

Denninston: - Sabe quantas pessoas rejeitei para este programa?

Turing: - Não.

Denninston: - Porque é ultrassecreto. Mas lhe direi porque ficamos íntimos e rejeitei um dos melhores linguistas do país semana passada. Entendia mais alemão do que Bertolt Brecht.

Turing: - Não falo alemão.

Denninston: - O quê?

Turing: - Eu não falo alemão.

Denninston: - Como irá decodificar as mensagens alemãs se não sabe falar alemão.

Turing: - Sou muito bom em palavras cruzadas.

Denninston: - Margaret.

Turing: - Os códigos alemães são uma charada. Um jogo como qualquer outro. Eu sou muito bom em jogos. Charadas. Esta é a charada mais difícil do mundo.

Denninston: - Faça boa viagem de volta a Cambridge, Professor.

Turing: - Enigma

Turing: - É o que fazem aqui. O programa secreto de Bletchley. Estão tentando decodificar a máquina alemã Enigma.

Denninston: - O que o faz pensar isso?

Turing: - É o melhor dispositivo de criptografia da História e os alemães o usam para se comunicar. Se os Aliados decodificassem a Enigma esta seria uma guerra muito breve. É claro que trabalham nisso, mas não avançaram ou não tirariam criptógrafos direto das universidades. Precisam muito mais de mim do que eu de vocês. Gosto de resolver problemas, comandante. E Enigma é o problema mais difícil do mundo.

Denninston: - Enigma não é difícil. É impossível. Os americanos, russos, franceses, alemães, todos acreditam que Enigma é indecifrável.

Turing: - Ótimo. Deixe-me tentar e teremos certeza, sim? (MORTHEN TYLDUN, 2014)

Após a entrevista, *Alan Turing* foi contratado para trabalhar em *Bletchley Park* para ajudar a desvelar o funcionamento da máquina Enigma. Na figura 19 vemos a equipe que já vinha trabalhando para decifrar o código secreto da máquina Enigma. Após a figura 19 vemos o diálogo do Comandante *Denninston* com a equipe de criptoanalistas.

Figura 19 – Comandante Denninston apresenta a máquina Enigma

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (13:30).

Denninston: - Bem-vindos à Enigma! As informações de todos os ataques surpresa, comboios secretos e submarinos do Atlântico passam por esta coisa e só captamos incoerências.

Turing: - É linda.

Denninston: - É a ceifa da Morte. Nossas oficiais interceptam milhares de mensagens de rádio ao dia e para as belas jovens da Marinha Real Feminina elas não fazem o menor sentido. Apenas quando as repassamos pela Enigma.

Cairncross: - Mas temos uma Enigma.

Denninston: - Sim! A inteligência Polonesa trouxe-a às escondidas de Berlim.

Cairncross: - Então qual é o problema? Repasse as mensagens pela máquina...

Turing: - Não é simples assim. Correto? Ter uma máquina não significa decodificar as mensagens.

Denninston: - Muito bom, Sr. Turing! Para isso, você precisa conhecer as configurações da máquina. Os alemães alteram as configurações todo dia à meia noite em ponto. Normalmente interceptamos a primeira mensagem às 06 h da manhã o que nos dá 18 h por dia para decifrar o código antes que o processo se reinicie.

Turing: - Cinco rotores. Dez cabos de conexão.

Cairncross: -Mil milhões. 1 milhão de milhão. 10 milhões, claro.

> **Turing**: - Mais de 150 trilhões de regulagens possíveis.
>
> **Denninston:** - Muito bom.
>
> **Hugh:** - 159 trilhões para ser exato. 159 e dezoito zeros atrás é o número de possibilidades a cada dia.
>
> **Denninston:** - Senhores, conheçam Hugh Alexander. Eu o escolhi para gerenciar esta unidade. O Senhor Alexander venceu o Campeonato Nacional de Xadrez.
>
> **Hugh**: - Duas vezes.
>
> **Denninston:** - Não é o único aqui que gosta de jogos, Turing.
>
> **Turing**: - Vamos trabalhar juntos? Prefiro ter minha própria sala.
>
> **Denninston:** - São uma equipe e trabalharão como tal.
>
> **Turing:** - Não tenho tempo para explicar meu raciocínio e receio que eles possam me atrasar.
>
> **Menzies**: - Se não podem jogar juntos, não haverá brincadeira alguma.
>
> **Denninston**: - Este é Stewart Menzies. Do MI6.
>
> **Kifie**: - Há apenas 5 divisões da Inteligência Militar. Não existe MI6.
>
> **Menzies**: - Exato. A ideia é essa. Senhor Turing, sabe quantos britânicos morreram em serviço por causa da Enigma?
>
> **Turing**: - Não, não sei.
>
> **Menzies:** - Três. Enquanto tivemos esta conversa. Veja, mais um. Espero que ele não tenha família. Na guerra citada pelo Comandante Denninston não estamos vencendo. Se decifrarem o código, teremos uma chance. Vamos deixar as crianças a sós com o novo brinquedo?
>
> **Hugh:** - Muito bem, senhores! Vamos jogar. (MORTHEN TYLDUN, 2014)

Quando *Alan Turing* foi apresentado à equipe de decifradores, eles ainda estavam utilizando o método de análise de frequência da distribuição de letras e as folhas de *Zygalski*. Algumas poucas mensagens alemãs foram decifradas por este processo mas era lento e, às vezes, era tarde demais para tomar uma decisão baseada no conteúdo da mensagem.

Nas palavras de Couto (2008, p. 264),

> A análise estatística é uma fonte crucial para a criptoanálise e foi aperfeiçoada durante a década de 1920. Alguns testes foram criados entre eles o teste kappa. Você tem uma caixa com as 26 letras do alfabeto. A chance de tirar uma letra da caixa é de 1/26 ou 0,0385. A cada 100 retiradas teremos a letra M umas três ou quatro vezes. A cada grupo de 100 retiradas aumentamos a chance de retirar qualquer letra (por exemplo G) em 100 vezes (0,0385 * 100 = 3,85).
>
> E se tivermos duas caixas com a letra G, qual seria a chance de tirar a mesma letra nas duas? (0,0385 * 0,0385 = 0,0015), ou seja, a cada 100 retiradas de cada caixa a mesma letra apareceria nas duas caixas apenas uma ou duas vezes. E se precisássemos tirar duas letras repetidas em específico. As chances delas saírem repetidas aumentam. A nova probabilidade seria a soma de todas as probabilidades de retirar as letras anteriores em pares. Por exemplo: AA (0,015) mais BB (0,015) e assim por diante. Matematicamente ficaria assim: 0,015 * 26 = 0,0385

A frequência das letras depende do idioma usado. No idioma Português, a letra A aparece 14 ou 15 vezes em cada 100 letras de texto, enquanto a letra B aparece apenas uma vez, a letra C entre 3 e 4 vezes.

Para (TKOTZ, 2005, p. 274).

> Se compararmos dois textos diferentes escritos em Português, ambos com o mesmo número de letras e colocados um sobre o outro, quantas colunas teriam a mesma letra? A chance de aparecer a letra A seria (15/100), a chance de encontrá-la repetida na mesma coluna é de (15/100) * (15/100) = 0,0225. Se a chance da letra B é de (1/100), a chance de repetição é de (1/100) * (1/100) = 0,0001. Se calcularmos as probabilidades de repetição para cada uma das letras e somarmos os resultados, saberemos quantas colunas com letras iguais se pode esperar. Usando as frequências das letras do Português obtém-se 0,0781, ou seja, se forem consideradas 100 colunas existe a chance de encontrar sete a oito (0,0781 * 100) = 7,81 letras repetidas. Essa probabilidade é diferente para cada idioma. No idioma francês é de 0,0778; no idioma alemão é de 0,0754; no idioma italiano é de 0,0738; no idioma espanhol é de 0,0775; no idioma inglês é de 0,0667; e no idioma russo, cujo alfabeto é de 30 caracteres é de 0,0529. Este é o teste kappa

Verifique, no anexo E, as principais características idiomáticas do espanhol, italiano, inglês, francês e alemão. O processo de decifragem da máquina enigma levou quase dois anos. Neste período, os alemães conquistaram quase toda a Europa. A (Fig 20) exemplifica uma das conquistas. Alemães marchando em Paris com o Arco do Triunfo ao fundo com uma imagem sobreposta da bomba criptológica em funcionamento.

Figura 20 - Alemães marchando em Paris em Junho de 1940

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (52:50).

A batalha da França terminou a 25 de junho de 1940 à 1h 35min da madrugada, quando entrou em vigor o armistício concedido pela Alemanha e Itália. Seis semanas depois de começar sua ofensiva no ocidente, Hitler já havia atingido a maior parte de seus objetivos. Agora só faltava fazer um acordo com os ingleses ou, se eles não concordassem, esmagá-los. Era um momento difícil para a Inglaterra, sozinha para defender a causa da democracia. Churchill declarava: “Nós defenderemos nossa ilha, que é a nossa Pátria[...]até que a maldição de Hitler seja removida da humanidade[...]” Mas como ele teria certeza do triunfo final? (HEIFERMAN et al, 1975, p. 275).

Depois da queda da França, o próximo alvo de Hitler seria a Grã-Bretanha. São utilizados os termos “A Batalha da Inglaterra” ou “A Batalha da Grã-Bretanha” nas batalhas travadas entre os alemães e britânicos principalmente pelo controle aéreo da região entre 1940 e 1941. Os alemães contavam com vários aeródromos dispostos na Alemanha, França (ocupada), Bélgica (ocupada), Holanda (ocupada), Dinamarca (ocupada) e Noruega (ocupada).

Durante a batalha contra a Inglaterra, no dia 13 de agosto de 1940 (*Adlertag* em alemão significa Dia da Águia), estavam prontos para atacar 949 bombardeiros e 336 *Stukas*, das três Frotas Aéreas Alemãs em conjunto. Estas Frotas Aéreas estavam distribuídas da França até a Noruega. 734 aviões de caça estavam em bases junto ao Canal da Mancha. 268 aviões de caça pesados estavam no interior. No lado britânico haviam mais de 700 caças disponíveis além de 471 bombardeiros que efetuavam unicamente voos noturnos realizando incursões sobre a Alemanha (BEKKER, 1968, p. 174).

Figura 21 – Bombardeiros alemães Heinkel He 111 na Batalha da Inglaterra

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (27:31).

No dia 31 de agosto de 1939, *Adolf Hitler* apresentou a “Diretiva nº 1 para a Condução da Guerra” que incluía detalhes sobre a invasão da Polônia e algumas precauções caso a França e Inglaterra atacassem a Alemanha.

> O Exército defenderá a Muralha Ocidental e fará preparativos para impedir que seja flanqueada no norte, pela violação do território belga e do holandês pelas potências Ocidentais. A Marinha realizará a campanha contra a navegação mercante, visando principalmente a Inglaterra. A Força Aérea deve, em primeiro lugar, impedir que as Forças Aéreas francesa e inglesa ataquem o Exército alemão e o *Lebensraum* alemão. Ao conduzir-se a guerra contra a Inglaterra, devem ser feitos preparativos para a utilização da Luftwaffe no despedaçamento dos suprimentos ingleses pelo mar, as indústrias de armamentos e o transporte de tropas para a França. Deve ser aproveitada uma oportunidade favorável para um ataque maciço, eficaz contra os couraçados e porta-aviões. Serão de minha decisão os ataques contra Londres. Devem ser feitos preparativos para ataques contra o território britânico, tendo em conta que êxitos parciais com forças insuficientes tem em todos os casos que ser evitados (HITLER apud SHIRER, 1967, vol. 2, p. 433).

No início de setembro de 1940 a *Luftwaffe* recebeu ordem de trocar os objetivos iniciais que seriam a destruição de portos, estações de radar, estações de comunicação, aeródromos da RAF (*Royal Air Force*), fábrica de armamentos que agora seria Londres o objetivo principal. Segundo a opinião inglesa e em particular a do Primeiro Ministro Britânico *Winston Churchill*, esta mudança de objetivo seria um dos mais graves erros alemães, visto que permitiria salvar vários grupamentos de caça que estavam sendo castigados à semanas. Por razões políticas, Hitler tinha proibido qualquer ataque aéreo em Londres durante o mês de agosto de 1940 (BEKKER, 1968, p. 202).

No dia 7 de setembro de 1940, os alemães lançaram o primeiro bombardeio maciço sobre Londres, usando 625 bombardeiros protegidos por 648 caças. Até aquele dia foi o mais devastador ataque aéreo contra uma cidade. Ao anoitecer, toda a área das docas era uma imensa massa de chamas, toda a linha férrea para o sul, tão vital para a defesa contra a invasão, estava bloqueada. Muitas pessoas, incluindo o governo britânico, acreditavam que esse bombardeio era o prelúdio de desembarques alemães. Esse ataque assinalou um momento decisivo na Batalha da Grã-Bretanha que ainda não tinha chegado ao seu clímax (SHIRER, 1963, vol. 3, p. 222). O bombardeio noturno alemão às cidades inglesas, conhecido como “Blitz” ,começou em setembro de 1940 e prosseguiu sem pausa até maio de 1941. Nas palavras de Jordan (2008, p.39)

> A maioria dos ataques era focada em Londres. Para localizar os alvos, os alemães usavam ondas de rádio *X-Gerat*, emanando de diferentes pontos

> da França, elas cruzavam acima do alvo desejado, indicando ao piloto para lançar a bomba. Esse método foi usado para destruir boa parte da cidade de *Coventry,* um ataque maciço, em novembro de 1940. Os alemães expandiram os ataques para outras cidades da Inglaterra quando cerca de 400 aviões bombardeiros foram para cima da cidade de Coventry. Jogando bombas altamente explosivas e incendiárias, os alemães mataram por volta de 500 pessoas e destruíram quase todo o centro da cidade (JORDAN et al, 2008, p. 39).

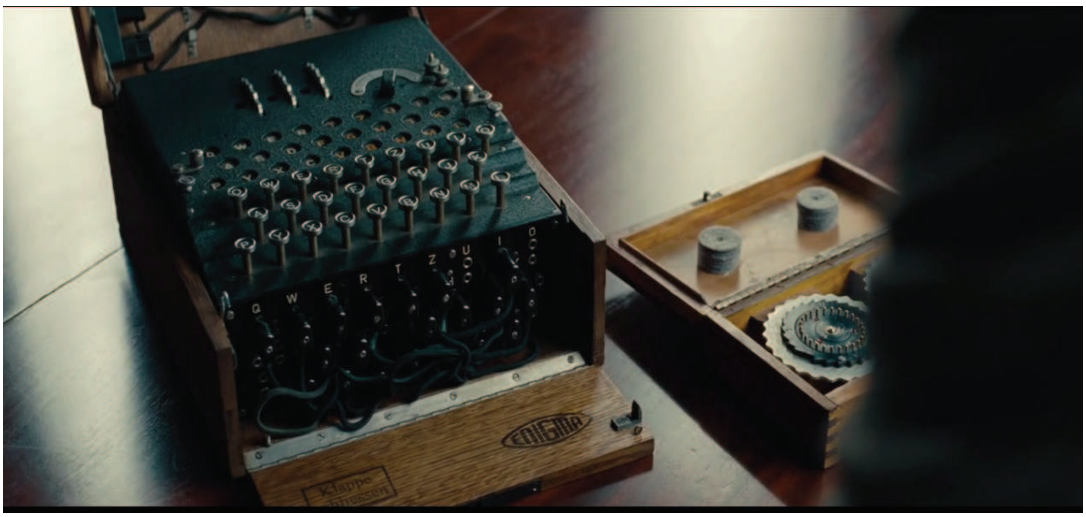
No dia 14 de novembro de 1940, Coventry foi bombardeada e tornou-se um braseiro visível num raio de 150 quilômetros. O centro, precioso testemunho do passado inglês, foi pulverizado, inclusive a maciça catedral do século XIV. As línguas inglesas e alemã enriqueceram-se com uma nova palavra, *coventrizar*, para significar o aniquilamento de uma cidade em um só bombardeio (CARTIER, 1977, p. 172). A *Luftwaffe* (Força Aérea Alemã) usava um código básico quando referenciava os nomes das cidades que seriam bombardeadas. *Birmingham*, por exemplo, era “Bild”, ou seja, a primeira letra do nome em código e o nome da cidade eram o mesmo. Em novembro de 1940, quando havia indícios de que ocorreria um grande ataque, cujo nome código era “Sonata ao Luar”, nenhum alvo havia sido identificado. O nome código da cidade era “Korn”. O ministro do ar inglês decidiu que não tinha importância. Foi decidido também que os raios eletrônicos da *Luftwaffe* que estavam concentrados na região de *Midlans* Ocidental, eram apenas um teste do sistema. Quando se percebeu que, em alemão, *Coventry* tem o som de K, era tarde demais. Coventry recebeu um dos piores ataques da Segunda Guerra Mundial. Após este ataque aéreo, criou-se muita especulação sobre o Primeiro Ministro *Churchill* dizendo que ele sabia do ataque mas não o impediu. Na verdade o destino das bombas não foi descoberto a tempo (PATERSON, 2009, p. 111).

Figura 22 – Avião alemão sobrevoando a cidade de Atenas na Grécia

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (52:48).

No dia 24 de Abril de 1941, a Grécia rendeu-se às forças do Eixo. Só restou às tropas britânicas retirar-se da península, como se tinha retirado da França um ano antes. A empresa foi tenebrosa. A Grã-Bretanha não dominava os ares como em Dunquerque. Cinquenta mil homens e não apenas algumas centenas deveriam ser embarcados debaixo das nuvens de bombardeiros inimigos. Entretanto, a operação obteve sucesso, mas as perdas foram muito pesadas: 11.840 mortos (CARTIER, 1977, p. 204).

Figura 23 – Máquina de cifragem Enigma capturada

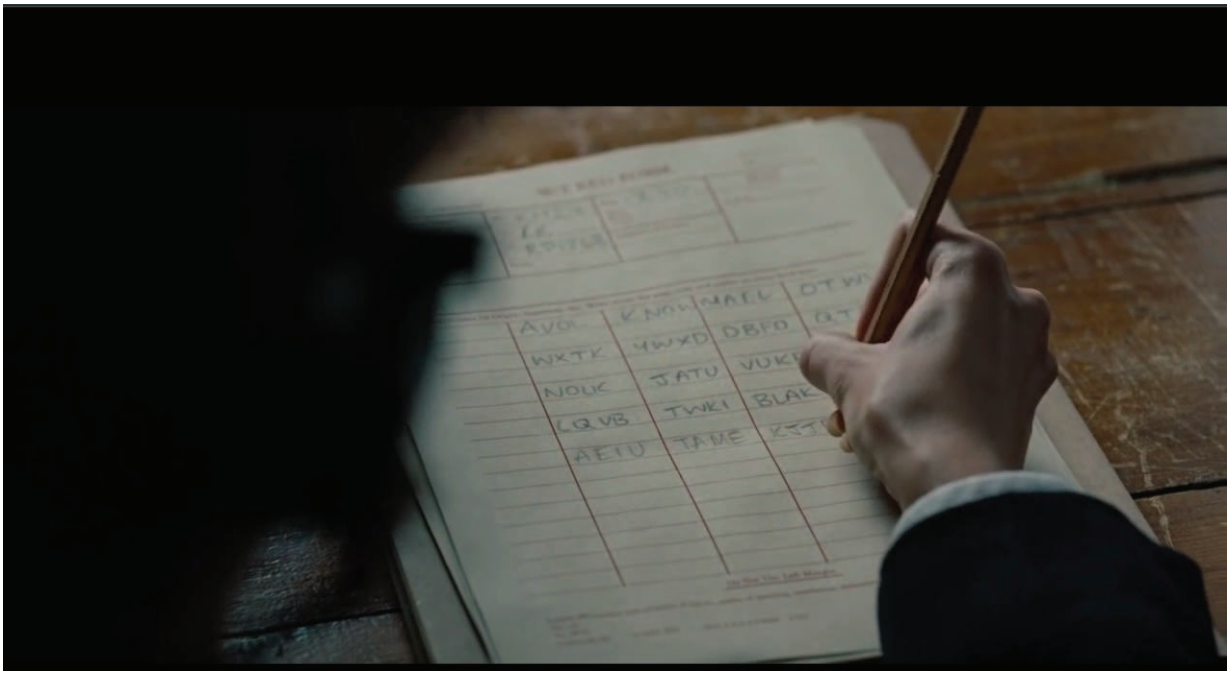


Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes,

2014. 1 DVD (114 min), NTSC, stereo, colorido. (12:04).

Na figura 23 observamos uma máquina Enigma naval com dois rotores extras (caixa menor ao lado) que foi utilizada pelos criptoanalistas de *Bletchley Park*.

Figura 24 – Mensagens alemãs criptografadas sendo interceptadas pelos ingleses



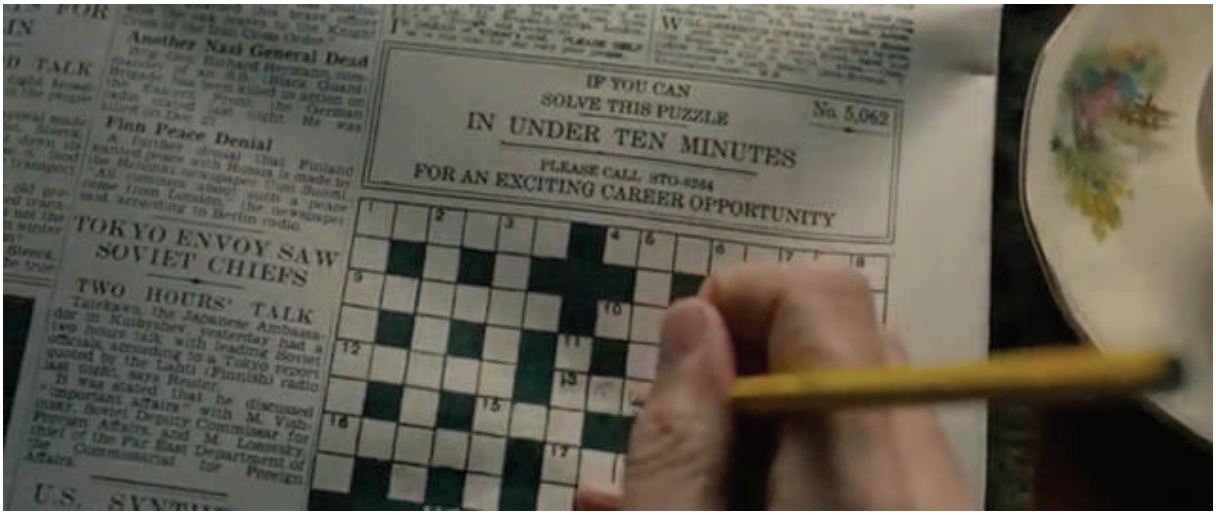
Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (15:48).

Os ingleses capturavam grandes quantidades de tráfego de informações dos alemães para serem analisados em *Bletchley Park*. As monitoras interceptam mensagens de uma torre de rádio específica. Elas tem um informante do outro lado que traduz a mensagem. As mensagens são registradas em folhas padronizadas e entregues aos criptoanalistas.

Durante a Primeira Guerra Mundial, a Alemanha transmitia dois milhões de palavras por mês, mas previa-se que a maior disponibilidade de rádios na Segunda Guerra Mundial resultaria na transmissão de dois milhões de palavras por dia (SINGH, 2011, p. 182).

O filme “O jogo da imitação, 2014” mostra a captura de informações somente dos alemães. Com a invasão do Japão em algumas colônias inglesas na Ásia, o tráfego de informações japonês também eram interceptados e analisados em Bletchley Park.

Figura 25 – Criptograma nº 5,062 publicado no Jornal Daily Telegraph no dia 13 de janeiro de 1942



Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (26:50).

Na figura 25 no retângulo que fica acima do quebra-cabeça está escrito “*If you can solve this puzzle in under ten minutes, please call STO-8264, for an exciting carrer opportunity*” que significa: “Se você resolver este quebra-cabeça em menos de 10 minutos, por favor ligue para STO-8264 para uma excitante oportunidade de carreira.

Para procurar jogadores de xadrez e aqueles que se distraíam resolvendo palavras cruzadas, o jornal *Daily Telegraph* tinham uma legião de devotos e no dia 15 de janeiro de 1942 foi simulada uma competição para resolver um quebra-cabeça em 12 minutos. Aqueles que se saíram bem foram convidados para uma entrevista. Foi resolvendo este quebra-cabeça que a carreira de *I. J. Good* começou em Bletchley Park (PATERSON, 2009, p. 64).

Figura 26 – Criptograma original publicado no Jornal Daily Telegraph em 13 de janeiro de 1942

TELEGRAPH CROSSWORD 5,062
13 JANUARY 1942

Across

1 A stage company (6)
4 The direct route preferred by the Roundheads (5,3)
9 One of the ever-greens (6)
10 Scented (8)
12 Course with an apt finish (5)
13 Much that could be got from a timber merchant (5,4)
15 We have nothing and are in debt (3)
16 Pretend (5)
17 Is this town ready for a flood? (6)
22 The little fellow has some beer; it makes me lose colour, I say (6)
24 Fashion of a famous French family (5)
27 Tree (3)
28 One might of course use this tool to core an apple (6,3)
31 Once used for unofficial currency (5)
32 Those well brought up help these over stiles (4,4)
33 A sport in a hurry (6)
34 Is the workshop that turns out this part of a motor a hush-hush affair? (8)
35 An illumination functioning (6)

Down

1 Official instruction not to forget the servants (8)
2 Said to be a remedy for a burn (5,3)
3 Kind of alias (9)
5 A disagreeable company (5)
6 Debtors may have to this money for their debts unless of course their creditors do it to the debts (5)
7 Boat that should be able to suit anyone (6)
8 Gear (6)
11 Business with the end in sight (6)
14 The right sort of woman to start a dame school (3)
18 "The war" (anag.) (6)
19 When hammering take care not to hit this (5,4)
20 Making sound as a bell (8)
21 Half a fortnight of old (8)
23 Bird, dish or coin (3)
25 This sign of the Zodiac has no connection with the Fishes (6)
26 A preservative of teeth (6)
29 Famous sculptor (5)
30 This part of the locomotive engine would sound familiar to the golfer (5)

Fonte: http://i.telegraph.co.uk/multimedia/archive/03068/crossword-puzzle_3068166c.jpg

O criptograma da figura 25 mostrado no filme foi fiel ao criptograma original mostrado na figura 26 tendo como fonte justamente o sítio Internet do jornal britânico *Daily Telegraph*. Todos os criptogramas publicados pelo jornal *Daily Telegraph* durante a Segunda Guerra Mundial serviam para identificar pessoas com raciocínio lógico e rapidez para resolver problemas complexos.

Resposta do criptograma da figura 26. Horizontal: 1 Troupe, 4 Short cut, 9 Privet, 10 Aromatic, 12 Trend, 13 Great deal, 15 Owe, 16 Feign, 17 Newark, 22 Impale, 24 Guise, 27 Ash, 28 Centre bit, 31 Token, 32 Lame dogs, 33 Racing, 34 Silencer, 35 Alight. Vertical: 1 Tipstaff, 2 Olive oil, 3 Pseudonym, 5 Horde, 6 Remit, 7 Cutter, 8 Tackle, 11 Agenda, 14 Ada, 18 Wreath, 19 Right nail, 20 Tinkling, 21 Sennight, 23 Pie, 25 Scales, 26 Enamel, 29 Rodin, 30 Bogie. (TELEGRAPH, 2016, Trad. nossa)

No filme “O jogo da imitação, 2014” apenas homens preenchiam as palavras cruzadas que eram publicadas no jornal *Daily Telegraph*. Joan Clarke foi uma exceção e encontrou resistência para poder participar do processo seletivo de *Alan Turing.* A figura 27 mostra o conflito entre Joan Clarke e o porteiro da sala onde são aplicados testes para candidatos que responderam criptogramas como o da figura 25 em menos de 10 minutos.

Figura 27 – Conflito entre Joan Clarke e o porteiro

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (29:41).

Porteiro: - O secretariado fica lá em cima. Esta é a sala dos candidatos.

Turing: - Posso prosseguir? Por favor?

Joan Clarke: - Sou uma candidata.

Porteiro: - A qual vaga?

Joan Clarke: - A carta não dizia.

Porteiro: - Secretárias ficam no outro andar.

Joan Clarke: - Só dizia ser ultrassecreto.

Turing: - O que está havendo?

Joan Clarke: - Resolvi a “cruzadinha” do jornal e recebi uma carta para me candidatar a um emprego misterioso.

Joan Clarke: - Meu nome é Joan Clarke.

Porteiro: - Senhorita, resolveu a “cruzadinha” sozinha?

> **Joan Clarke**: - Por que duvidaria? Sou muito boa em...
>
> **Porteiro**: - Senhorita, preciso...
>
> **Turing:** - Senhorita Clarke, seu atraso é inaceitável. Sente-se para que possamos prosseguir.
>
> **Joan Clarke**: - Obrigada.
>
> **Turing**: - Como eu dizia, terão 6 minutos para solucionar o problema à sua frente. Senhoras e Senhores...comecem.
>
> **Menzies**: - 6 minutos. É possível?
>
> **Turing**: - Não, eu levei 8 minutos. Não se trata do quebra-cabeça mas da postura de tentar solucionar um problema impossível. Se resolverá tudo ou se dividirá.
>
> **Turing**: - Terminou?
>
> **Joan Clarke**: - Sim.
>
> **Turing**: - 5 minutos e 34 segundos.
>
> **Joan Clarke**: - Você mandou fazer em menos de 6 minutos. (MORTHEN TYLDUN, 2014)

No diálogo entre Joan Clarke e o porteiro ficou claro que as mulheres da década de 1940 do século XX deveriam seguir vários padrões como por exemplo: não poder trabalhar fora de casa e ter profissões “adequadas” somente para mulheres como por exemplo: secretária. Teoricamente as mulheres desta época só saíam de casa quando se casavam e deveriam ser donas de casa e cuidar dos filhos.

De acordo com o porteiro as mulheres eram inferiores aos homens porque ele não acreditou que a Joan Clarke resolveu sozinha uma simples “palavra-cruzada”. Outra discriminação do porteiro seria que as mulheres já tinham os cargos específicos e aquela sala de provas não deveria ter mulheres.

No período entre guerras (1919-1939), o Governo Britânico selecionava cientistas, matemáticos, jogadores de xadrez e linguistas que dominavam o idioma alemão ou qualquer pessoa que resolvesse problemas complexos em um curto espaço de tempo. Depois que Alan *Turing* começou a trabalhar em *Bletchley Park*, ele mesmo selecionava criptoanalistas para sua equipe.

Figura 28 – Alan Turing faz um pedido ao Comandante Denninston

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (22:25).

Na figura 28, Alan Turing solicita £ 100.000 (cem mil libras) ao *Hugh Alexander* (chefe imediato de Turing) para construir uma máquina para decifrar qualquer mensagem da máquina Enigma. Como o pedido foi negado, *Alan Turing* refez a solicitação ao Comandante *Denninston* que também recusa o pedido. *Alan Turing* segue o conselho do Comandante *Denninston* para enviar esta solicitação ao Primeiro Ministro Britânico *Winston Churchill* no endereço: rua Downing, n° 10, Londres, SW1. *Turing* e sua equipe conseguem a quantia pedida e *Winston Churchill* ainda coloca *Alan Turing* como chefe da equipe no lugar de *Hugh Alexander*. Assim foi possível comprar as peças necessárias para a construção da bomba criptológica britânica. Acompanhe o diálogo entre o comandante *Denninston* e *Alan Turing* de acordo com a figura 28.

Denninston: Se quiser discutir a queixa marque um horário.

Turing: Alexander. Queixa, não. Hugh Alexander recusou meu pedido de peças para a construção da máquina que criei.

Denninston: Seus colegas se recusam a trabalhar com você e formalizaram uma queixa.

Turing: Me baseei em uma antiga codificadora polonesa só que infinitamente melhor.

> **Denninston**: Se não responder a queixa, irá para o Ministério de Interior. Deixe estes papéis em minha mesa.
>
> **Turing:** Minha resposta é que são burros. Demita-os e use a verba para construir minha máquina. Só preciso de 100.000 Libras.
>
> **Denninston**: 100.000 Libras? Por que está construindo uma máquina?
>
> **Turing**: É altamente técnico. Você não entenderia.
>
> **Denninston**: Sugiro que faça esse esforço.
>
> **Turing**: Enigma é uma máquina muito bem projetada. O problema é que usamos homens para decifrá-la. E se apenas uma máquina puder derrotar a outra?
>
> **Denninston**: Isto não é muito técnico. Alexander é o encarregado. Se disse: "não", a resposta é não.
>
> **Turing**: Não tenho tempo para isso.
>
> **Denninston**: Já venceu uma guerra, Turing? Eu já. Sabe como fazemos isso? Com ordem. Disciplina. Cadeia de comando. Não está mais na universidade. É apenas uma formiga em um amplo sistema e fará o que seus superiores mandarem.
>
> **Turing**: E quem é o seu superior?
>
> **Denninston:** Winston Churchill. Rua Downing, 10. Londres. Se não concorda com a minha decisão, fale com ele. (MORTHEN TYLDUN, 2014)

Segundo Sigh (2011, p. 197), depois de obter as cem mil libras, foi possível transformar a ideia de *Turing* em engenhos funcionais, que receberam o nome de bombas porque sua abordagem mecânica lembrava a bomba que os poloneses construíram antes de começar a Segunda Guerra Mundial. *Turing* finalizou o projeto no início de 1940 e a construção ficou sob a responsabilidade da fábrica *British Tabulating Machinery*, em *Letchworth*.

Figura 29 – Alan Turing citando o conto ou enigma do urso

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (48:32).

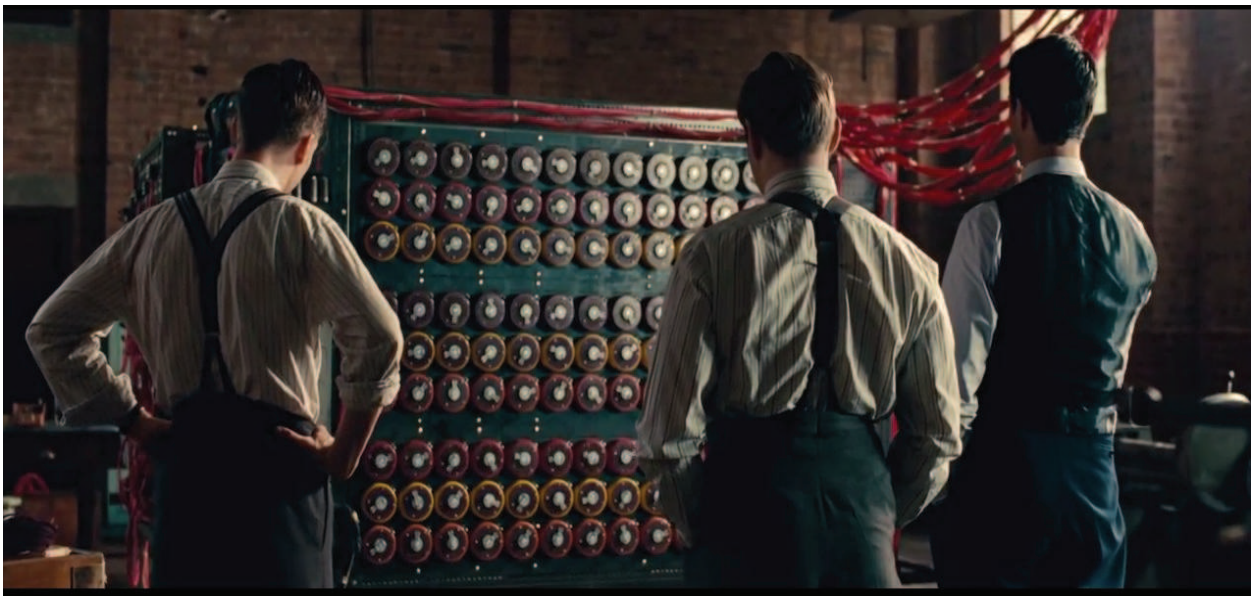
> **Hugh**: O que é isso?
>
> **Turing**: Maças. A Senhorita Clark disse que seria bom se eu trouxesse umas maças e por isso eu...
>
> **Turing:** Há duas pessoas na floresta e elas encontram um urso. A primeira pessoa se ajoelha e reza. A segunda pessoa começa a amarrar as botas. A primeira pessoa pergunta para a segunda: “Meu caro amigo, você não vai correr mais do que o urso”. A segunda pessoa responde: “Eu não preciso. Preciso correr mais do que você”. (MORTHEN TYLDUN, 2014)

De acordo com o diálogo da figura 29, Alan Turing cita o conto do urso ou enigma do urso que serviu para explicar o conflito entre a Grã-Bretanha e a Alemanha Nazista por uma linguagem metafórica. O nazismo obteve uma expansão inicial na Europa mas a Grã-Bretanha iria deté-lo.

Nas palavras de Churchill (1995), é possível fazer outra analogia com o enigma do urso. “Começou a corrida pelos despojos. Mas Mussolini não foi o único animal faminto em busca da presa. Ao Chacal veio juntar-se o Urso”. Alemanha e Rússia trabalhavam juntas, tão estreitamente quanto o permitiam suas profundas divergências de interesse. Hitler e Stalin tinham muito em comum, como governantes totalitários e seus sistemas de governo eram afins.

Neste caso o “Urso” pode ser o próprio ditador soviético Stalin ou a expansão do comunismo já que os russos ocuparam os países bálticos (Letônia, Lituânia e Estônia) e as regiões da Bessarábia e norte da província da Bukóvina na Romênia com o consentimento dos alemães. No final da Batalha da França, a Itália que era governada pelo ditador fascista Benito Mussolini declarou guerra à França para participar da divisão do espólio de guerra com a Alemanha.

Figura 30 – Bomba criptológica inglesa “*Christopher”* construída em Bletchley Park



Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (52:10).

Quando a “*bomb* ou bomba criptológica” de Bletchley Park ficou pronta, *Turing* e sua equipe ainda não sabiam como iam decifrar os códigos secretos da máquina Enigma. Devido ao grande número de combinações que a máquina Enigma oferecia, tinham que realizar os testes até a meia-noite. Exatamente à meia-noite os alemães mudavam as configurações da máquina Enigma e os criptoanalistas de Bletchey Park tinham que começar os testes a partir do zero. A primeira mensagem enviada pelos alemães era sobre o tempo exatamente às 06h da manhã.

O comandante *Denninston* queria resultados o mais rápido possível mas como não recebeu nenhuma mensagem decifrada decidiu demitir *Alan Turing*. A equipe se uniu e eles disseram que teria que demití-los também. *Hugh Alexander* pediu 6 meses para decifrar as mensagens secretas da Enigma. O comandante *Denninston* reduziu esta prazo para 1 mês. A justificativa foi de que foi feito um alto investimento em tecnologia que não estava dando resultados além do fato da Grã-Bretanha estar perdendo a Guerra para a Alemanha Nazista e seus aliados.

Nas palavras de Zochio (2016), "*bomb*" era o nome de uma máquina eletromecânica, desenvolvida durante a Segunda Guerra Mundial por *Alan Turing* e *Gordon Welchman* quando trabalhavam em *Bletchley Park* no sul da Inglaterra, como decifradores de código. A "*bomb*" inglesa era parcialmente baseada na "*bomb*" polonesa. *Turing* usou uma abordagem diferente da máquina polonesa. Sua estratégia era se basear no ataque do texto conhecido, onde se conhece ou supõe-se que um texto chamado *crib* (berço), aparece em alguns lugares no texto. *Gordon Welchman* criou a placa diagonal que reduziu consideravelmente o número de combinações para a decifração das mensagens.

Gordon Welchman não foi citado no filme o jogo da imitação, 2014. No filme o projeto da placa diagonal foi entregue por *Hugh Alexander* ao *Alan Turing*.

Figura 31 – Monitora de rádio revela um detalhe crucial para Alan Turing

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (1:13:41).

Dentro do perímetro de Bletchley Park existia um local de entretenimento para os criptoanalistas e outros colaboradores se divertirem durante as folgas. A monitora de comunicações *Helen Stewart* fez um comentário sobre um operador alemão que sempre começava as mensagens com as letras “CILLY” e ela pensou que fosse a namorada do operador alemão. Esta informação chamou a atenção de Alan Turing. Este operador alemão não estava seguindo os protocolos de segurança usando a mesma sequência de caracteres no início das mensagens. A regra seria usar de 3 a 5 letras aleatórias no começo de cada mensagem para dificultar a decifração. Acompanhe o diálogo entre Alan Turing e Helen Stewart de acordo com a figura 31.

> **Helen**: - Nós interceptamos mensagens de uma torre alemã. Temos um correspondente que envia as mensagens em Código Morse. Cada um digita diferente então conhecemos o ritmo de todos. É estranhamente íntimo. Sinto que o conheço tão bem. É uma pena que já tenha namorada, mas é por isso que discordo, Sr. Alexander porque estou apaixonada por um colega de trabalho que jamais vi.
>
> **Turing**: - Helen!
>
> **Helen**: - Sim, Alan?
>
> **Turing**: - Por que acha que seu correspondente alemão namora?
>
> **Helen**: - É uma brincadeira boba.
>
> **Turing**: - Não, me conte!
>
> **Helen**: - Todas as mensagens dele começam com as mesmas “cilly”. Acredito que “cilly” seja sua amada.
>
> **Turing**: - Impossível! Os alemães devem usar 5 letras aleatórias no início de todas as mensagens. Ele não faz isso.
>
> **Hugh**: - O amor leva o homem a fazer coisas estranhas.
>
> **Turing**: - Neste caso, o amor levou a Alemanha a perder a guerra. (MORTHEN TYLDUN, 2014)

De acordo com Singh (2011, p. 185), os britânicos já dominavam as técnicas polonesas, e melhoraram seus próprios métodos. Os criptoanalistas britânicos aproveitavam o fato de que alguns operadores alemães da Enigma ocasionalmente escolhiam chaves de mensagem óbvias. Para cada chave de mensagem deveriam ser escolhidas três letras aleatórias mas ás vezes pegavam três letras consecutivas do teclado da máquina Enigma, como QWE ou BNM. Essas chaves de mensagens

previsíveis se tornaram conhecidas como “cílios”. Outro tipo de “cílio” era o uso repetido da mesma chave de mensagem, talvez as iniciais da namorada do operador alemão, um conjunto de iniciais “CIL”, pode ter dado origem ao nome. Testar os “cílios” e seus palpites às vezes davam resultado.

Complementando sobre os operadores de rádio alemães, Davies (2009, p. 55) nos informa que um homem chamado *Walter*, estava ignorando as instruções de segurança e inicializando suas máquinas com os mesmos parâmetros todos os dias. Os criptoanalistas de *Bletchley Park* observaram que as unidades alemãs espalhadas pela Europa transmitiriam mensagens quase idênticas no dia do aniversário de *Adolf Hitler* em 20 de abril de 1940. Para completar o quadro favorável para os britânicos, eles conseguiram capturar uma máquina Enigma Naval de um navio meteorológico alemão perto da Groenlândia.

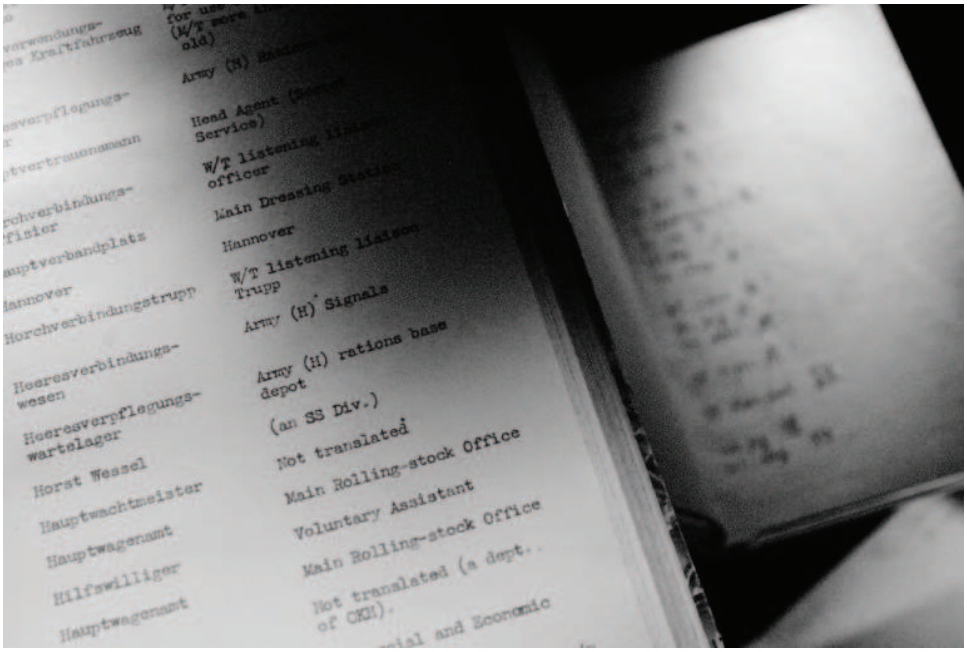
Figura 32 – Cena do filme “O jogo da imitação, 2014” em que *Alan Turing* e sua equipe decifram o código da máquina Enigma Naval pela primeira vez

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (1:17:21).

Alan Turing (sentado) manipulando uma máquina Enigma. A única mulher da imagem é a Joan Clarke. Atrás de *Alan Turing* seria o *John Cairncross*. Atrás de *Joan Clarke* seria o *Hugh Alexander*. Atrás de *Hugh Alexander* seria o *Peter Hilton*.

De acordo com a figura 32, Joan Clarke ditou as letras para *Alan Turing* que a "bomba criptológica britânica" ou "bomba de Turing" ou "Christopher" gerou depois de ser configurada com a posição das letras das palavras dos boletins de tempo alemão. A última frase das mensagens era "*Heil Hitler*", o que ajudou bastante na eliminação de configurações extras da bomba simplificando a decifração das mensagens. *Alan Turing* digitava as letras na máquina Enigma e *John Cairncross* anotava as letras do painel luminoso da máquina Enigma. A mensagem secreta era: "KMS Jaguar no ponto direcionado para 53 graus e 24 minutos norte e ao ponto um grau a oeste, *Heil Hitler*".

Figura 33 – Interpretação de mensagens alemãs decifradas



Fonte:https://i0.wp.com/www.brummiebr.com/wp/wp-content/uploads/2015/06/bletchley_park_melissa_becker03.jpg?resize=768%2C514

Não bastava apenas decifrar as mensagens da máquina Enigma, a mensagem tinha que ser traduzida neste caso (Figura 33), do alemão para o inglês, mas uma equipe de linguistas também trabalhavam na tradução de outros idiomas, como o japonês). Veja na tabela 1 alguns exemplos descritos na figura 33.

Tabela 1 – Palavras em alemão e sua significação no teatro de guerra

Palavra em alemão	Tradução para o inglês e significação
Horst Wessel	Uma Divisão da SS
Hanover	Hanover. Cidade de Hanover
Hilfswilliger	Assistente voluntário

Fonte: Elaborado pelo autor

Segundo Davies (2009, p. 55), no segundo ano da Segunda Guerra Mundial (1940), *Bletchley Park* lia todas as transmissões da máquina Enigma em um intervalo de três horas. Eles conseguiram acompanhar todas as novas versões alemãs. A “bomba criptológica britânica” ou “bomba de Turing” que era uma calculadora eletromecânica realizava as permutações e obtinha as respostas.

Figura 34 – Sala de mapas secretos em Bletchley Park

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (1:22:05).

A figura 34 mostra *Alan Turing* e sua equipe com um grande mapa indicando as rotas dos comboios entre o continente americano e a Europa. É possível ver também as posições dos navios de guerra e submarinos alemães no Oceano Atlântico. De acordo com *Peter Hilton*, seu irmão está no comboio de civis no HMS *Carlisle* e os submarinos alemães estão a 20 minutos da interceptação do comboio. A equipe quer avisar o Comandante Denniston sobre o ataque mas Alan Turing nega o pedido e é agredido pelo Hugh Alexander. A equipe segue a decisão de Turing em não avisar o comandante Denninston e deixar o ataque acontecer. A figura 34 mostra o dilema da equipe em saber de determinados ataques alemães com antecedência e não poder informar seus superiores porque se todos os ataques alemães fossem contidos, os alemães iriam desconfiar que as mensagens da máquina Enigma estariam sendo decifradas. Como consequência, os alemães poderiam mudar todos os livros de cifras além de modificar a própria máquina Enigma. Se isto acontecesse, os criptoanalistas britânicos teriam que começar todo o trabalho de decifragem novamente. Em seguida observamos o diálogo entre os personagens presentes na figura 34.

Turing: Deixe os submarinos afundarem o comboio.

John: Foi um grande dia. Deve estar mal.

Hugh: Não temos tempo para isso.

Turing: Não. (Turing arremessa o telefone na parede e leva um soco de Hugh).

Joan: Hugh, já chega.

Peter: Pare Hugh. O ataque será em alguns minutos.

Turing: Não, estou bem.

Turing: Sabe por que as pessoas gostam de violência, Hugh? Porque a sensação é boa. As vezes, não podemos fazer o que é bom. Devemos fazer o que é lógico.

John: O que é lógico?

Turing: O momento mais difícil para mentir é quando esperam que você minta.

Turing: Se alguém quer uma mentira não pode lhe oferecer uma.

Joan: Droga, Alan está certo.

Turing: O que os alemães vão pensar se destruirmos seus submarinos?

Peter: Nada, estarão mortos.

John: Não, não pode estar certo.

Turing: Se o comboio mudar de curso de repente ou um esquadrão de bombardeiros milagrosamente surgir na direção dos submarinos, o que os alemães vão pensar?

Hugh: Vão saber que decifrramos a Enigma.

Joan: Irão interromper todas as comunicações via rádio e mudarão o projeto da Enigma até o final de semana.

Turing: Eu sinto muito.

Peter: Quem você pensa que é? É o meu irmão. E você tem alguns minutos para impedir seu assassinato.

John: Ele está certo.

Peter: Alan, Joan, Hugh, John. Por favor. Os alemães não vão desconfiar se detivermos um ataque. Ninguém saberá. Estou pedindo como amigo. Por favor.

Turing: Eu sinto muito.

Peter: Você não é Deus, Alan. Não decide quem vive ou morre.

Turing: Sim, nós decidimos.

Peter: Por que?

Turing: Por que ninguém mais pode. (MORTHEN TYLDUN, 2014)

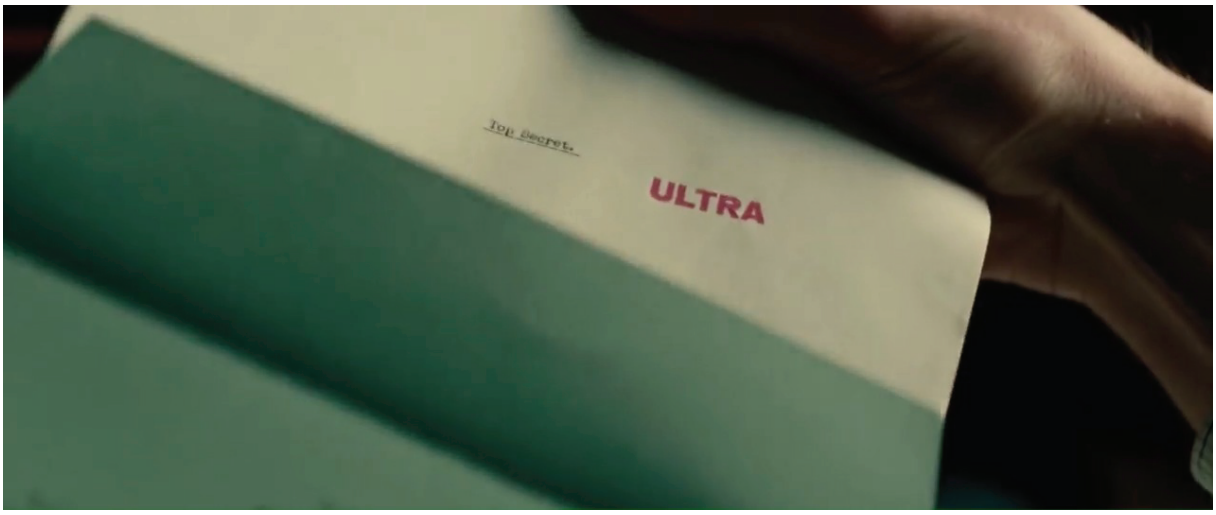
Figura 35 – Reunião entre Menzies, Clarke e Turing

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (1:24:23).

Alan Turing e *Joan Clarke* estavam desenvolvendo um sistema usando análises estatísticas que iriam determinar o quanto de inteligência usar, quais ataques parar ou continuar. Um número mínimo de ações necessárias para ganhar a Guerra mas também um número máximo de ações antes dos alemães suspeitarem. Quando Alan Turing e Joan Clarke chegam na estação de trem, Clarke nota alguns jovens soldados britânicos embarcando para lutarem na Guerra. Durante a reunião com Menzies, Clarke nota a chegada de um caminhão com soldados feridos e mutilados entrando em um hospital militar em frente à lanchonete. O objetivo principal da reunião ilustrada na figura 35 é esconder dos oficiais militares Aliados que o código secreto da máquina Enigma foi decifrado.

> **Menzies:** - Por que está me contando isso?
>
> **Turing**: - Precisamos de sua ajuda para manter isso em sigilo da Marinha, Exército e Força Aérea. Ninguém pode saber que decifrамos a Enigma. Nem *Denninston*.
>
> **Menzies**: - Que está assinando sua demissão.
>
> **Clarke**: - Você pode cuidar disso.
>
> **Turing:** - Enquanto criamos um sistema para que use bem as informações. Qual ataque deter e qual permitir. Análises estatísticas. O mínimo necessário para vencermos a guerra e o máximo permitido sem que os alemães desconfiem.
>
> **Menzies:** - E vai confiar tudo isso a estatísticas? A matemática?
>
> **Turing**: - Exato.
>
> **Clarke**: - E o MI6 pode criar as mentiras que diremos.
>
> **Turing**: - Precisarão de uma fonte alternativa confiável para a coleta das informações que usarão.
>
> **Clarke**: - Histórias falsas para justificar a informação sem relacioná-la com a Enigma e poderá “vazar” essas histórias para os alemães.
>
> **Turing**: - E para nossos militares.
>
> **Menzies**: - Manter uma conspiração no mais alto patamar do governo? Está dentro das minhas aptidões. Alan, raramente tenho a chance de dizer isso, você é exatamente o homem que eu esperava. (MORTHEN TYLDUN, 2014)

Figura 36 – Formato da mensagem secreta do sistema ULTRA



Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (1:35:32).

No final de 1941, o ULTRA estava decifrando mensagens secretas alemãs quase tão rapidamente como eram transmitidas. Em algumas ocasiões, os britânicos decifraram mensagens antes que seus destinatários as recebessem.

No verão de 1942, o General alemão *Erwin Rommel* com seu *Deutsches Afrikakorps* (ou simplesmente *Afrika Korps,* ou DAK*)* era parte do exército alemão que atuava na África. O *Afrika Korps* e várias divisões italianas conseguiram empurrar o exército britânico até a fronteira egípcia. Conquistou *Tobruk* e em fins de julho achava-se em *El Alamein* a sessenta e cinco milhas de Alexandria. Hitler enviou um bastão de marechal de campo para Rommel, mas não enviou suprimentos nem reforços (SHIRER, 1963, vol. 3, p. 435).

Ladeando continuamente as ordens de “nenhum recuo” de *Adolf Hitler* (líder alemão) e Mussolini (líder italiano), *Rommel* (Marechal de Campo do *Afrika Korps*) realizou uma magistral retirada, conservando o grosso de suas tropas restantes, retardando a perseguição do General Inglês *Montgomery*, a despeito de persistente carência de combustível e munições. Embora *Montgomery* dispusesse de recursos superiores, especialmente no ar, e informações antecipadas das intenções e planos de *Rommel* graças a interceptação de suas mensagens pela operação de espionagem ULTRA (BARNETT, 1991, p. 325).

Em 1943, o ULTRA fez a força de submarinos da Alemanha um “livro aberto”. A batalha do Atlântico foi vencida e os Aliados tiveram as maiores dificuldades para esconder o sistema ULTRA. Enquanto os alemães acreditassem que suas comunicações estavam seguras, eles não mudariam o sistema. Com o número de submarinos alemães sendo afundados crescendo, o almirante alemão *Karl Doenitz* se perguntou se as comunicações tinham sido comprometidas. Foi feita uma revisão em todo o sistema e como o número de combinações da máquina Enigma era grande, não havia razão para pensar que os Aliados estavam decifrando as mensagens. A mesma conclusão foi tirada pelos criptógrafos japoneses, que concluíram que desde que a máquina de cifragem PURPLE, usada para o tráfego diplomático de alto nível também apresentava um grande número de combinações matemáticas, nenhum possibilidade de decifração pelo inimigo foi acatada. Se os americanos tinham decifrado a PURPLE, por que então estavam tão despreparados em *Pearl Harbor* ? (VOLKMAN, 2013, p. 268)

Os canhões cessaram fogo na Europa e as bombas deixaram de cair à meia-noite de 8 para 9 de maio de 1945 com a rendição incondicional da Alemanha. Desde 1º de setembro de 1939 que não havia silêncio no continente europeu. Era o fim da guerra na Europa já que a guerra no Pacífico ainda continuava entre os Aliados contra os japoneses (SHIRER, 1975, vol. 4, p. 296).

Figura 37 – Início do discurso do Primeiro Ministro Britânico Winston Churchill

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (1:36:45).

A figura 37 apresenta um pequeno trecho do discurso da vitória do Primeiro Ministro Britânico Winston Churchill: “Essa vitória é de vocês. Vitória da liberdade em cada terra”. No discurso da vitória de Winston Churchill está presente a frase: “Vitória da liberdade”. De qual “liberdade” ele quis dizer já que homossexualismo na Grã-Bretanha era considerado crime. No regime nazista homossexualismo também era considerado crime e os homossexuais eram enforcados ou fuzilados. Na Grã-Bretanha os homossexuais tinham dois caminhos: prisão ou realizar um “tratamento” para “curar” o homossexualismo através de hormônios. Outra analogia seria comparar o regime democrático inglês (com “liberdade”) com o regime nazista totalitário (sem “liberdade”).

3.4 A morte de *Alan Turing*

Após a Segunda Guerra Mundial, *Alan Turing* retornou a *Cambridge* e a uma vida privada como um homossexual, quando isso era crime grave na Grã-Bretanha.

Detetive *Robert Nock* da polícia de Manchester interroga *Alan Turing* em uma delegacia. Inicialmente o detetive Nock suspeita que Alan Turing é um espião soviético mas ele foi monitorado e foi comprovado que ele se relacionava intimamente com homens.

Figura 38 – Alan Turing sendo interrogado pela polícia de Manchester

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (1:06:42).

A figura 38 mostra *Alan Turing* sendo interrogado pelo detetive Nock da polícia de Manchester em 1951 retomando o início do filme: “O jogo da imitação, 2014”.

Nock: Quero lhe contar um segredo.

Turing: Eu sou muito bom em segredos.

Nock: “As máquinas podem pensar?”.

Turing: Você está lendo meus trabalhos?.

Turing: Estou sendo acusado de indecência e pergunta se as máquinas podem pensar?

Nock: As máquinas poderiam pensar como os seres humanos pensam?

Turing: A maioria das pessoas diz que não.

Nock: Você não é a maioria das pessoas.

Turing: Você está fazendo uma pergunta estúpida.

Turing: É claro que as máquinas não podem pensar como as pessoas. Uma máquina é diferente de uma pessoa, portanto pensam de modo diferente. A questão interessante é, só porque alguma coisa pensa diferente de você, significa que ela não pensa? Nós concordamos que os humanos divergem uns dos outros. Você gosta de morango e eu odeio patinação no gelo. Você chora em filmes tristes, eu sou alérgico a pólen. Como explicar gostos diferentes, preferências diferentes senão dizer que nossas mentes, trabalham de forma diferente, que pensamos de modo diferente? E se podemos dizer isso um do outro por que não podemos dizer o mesmo de mentes construídas de cobre, arame e aço?

Nock: Esse é o grande artigo que escreveu? Como o artigo se chama?

Turing: O jogo da imitação.

Nock: Qual o assunto do artigo?

Turing: “Gostaria de jogar”? É um tipo de jogo para determinar o que é uma máquina ou um humano?

Nock: Como se joga?

Turing: Neste jogo tem um juiz e um sujeito. O juiz faz perguntas, e dependendo da resposta do sujeito, determina com quem ele está falando. Sobre o que ele está falando e tudo o que tem que fazer é uma pergunta.

Nock: - O que fez durante a Guerra?

Turing: Trabalhei em uma fábrica de rádio.

Nock: O que realmente fez durante a Guerra?

Turing: Está prestando atenção?

Turing continua narrando de acordo com o filme “a Guerra se arrastara por mais dois anos solitários e a cada dia mostráramos os “suados” cálculos. Todos os dias decidira quem vivia ou morria. Todo dia nós ajudávamos os Aliados a vencerem e ninguém sabia. *Stalingrado, Ardenne*, a invasão da Normandia. As vitórias seriam impossíveis sem nossa inteligência. E o povo? O povo falava da Guerra como se fosse uma batalha épica entre Civilizações”.

As figuras 39, 40 e 41 mostram detalhes das batalhas citadas por *Alan Turing* ao detetive *Nock*.

Figura 39 – A Batalha de Stalingrado

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (1:35:43).

O episódio conhecido como a Batalha de Stalingrado foi travada entre 17 de julho de 1942 e 2 de fevereiro de 1943 entre os exércitos do Eixo liderados pelos alemães e o exército russo. O objetivo desta ofensiva dos alemães era a captura da cidade de nome Stalingrado (atual Volgograd) na União Soviética (atual Rússia) que fica as margens do rio Volga.

Os alemães não conseguiram dominar a cidade de Stalingrado totalmente mas Werth (1971, p. 13) narra a contra-ofensiva russa. De 19 de novembro a 11 de

dezembro de 1942 é o período em que os russos conseguem cercar os alemães e romenos em Stalingrado. De 12 de dezembro de 1942 a 1º de janeiro de 1943, período em que corresponde a tentativa do Marechal alemão *Erich von Manstein* de romper o cerco russo sem sucesso para tentar salvar o 6º Exército Alemão além da derrota completa dos italianos no rio Don. Entre 10 de janeiro de 1943 e 2 de fevereiro de 1943 ocorre a liquidação definitiva das forças alemãs e romenas dentro do “Caldeirão” de Stalingrado.

Figura 40 – A Batalha das Ardenas

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (1:35:45).

O episódio conhecido como a Batalha das Ardenas ou Batalha do “Bolsão” foi travada entre dezembro de 1944 e janeiro de 1945 na floresta das Ardenas entre os Aliados e os alemães sendo o local da batalha situado na fronteira entre França e Alemanha. Foi a última ofensiva alemã da Segunda Guerra Mundial e o objetivo era chegar ao porto de Antuérpia e separar o Exército inglês do Exército americano.

Segundo Baldwin (1978, p. 379), o grande ataque nazista nas Ardenas constituiu uma supresa arrasadora; todos imaginavam que a Alemanha estivesse praticamente liquidada. “Raramente a guerra se desenrola de acordo com os planos, quem lesse Clausewitz haveria de encontrar a advertência:”

> Quando a desproporção de forças for tão grande, que nem a limitação do nosso objetivo nos possa livrar da catástrofe, ou quando a duração provável do perigo for tal que nem a maior economia de forças nos permita alcançar o objetivo, só restará o recurso de concentrar as forças disponíveis em um golpe temerário. Aquele que estiver sob maior pressão encarará a maior ousadia com sendo a atitude conveniente, valendo-se talvez, da ajuda de um estratagema sutil (CLAUSEWITZ apud BALDWIN, 1978, p. 382).

No dia 03 de janeiro de 1945, Adolf Hitler “abandonou oficialmente os objetivos da ofensiva das Ardenas”; no dia 08 de janeiro de 1945, permitiu o retraimento do 6º Exército Panzer SS para formar uma reserva. Toda a Frente Ocidental ficara desconjuntada. Mesmo com a fracasso da ofensiva alemã, foi evitado as ataques contra a cidadela germânica. Com a retomada da ofensiva russa na Frente Oriental no dia 12 de janeiro de 1945, os Aliados estavam se recuperando do desgaste da Batalha das Ardenas. A concentração do poderio alemão no oeste e o revés dos Aliados Ocidentais, facilitou o avanço russo e este contexto deu força às alegações comunistas que o Exército russo salvara o ocidente e ajudou os soviéticos a conquistar Berlim.

Figura 41 – A invasão da Normandia ou Dia D

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (1:35:51).

Segundo Gilbert (2014, p. 663), na madrugada do dia 6 de junho de 1944 inicio-se o episódio conhecido por “Dia D” pelos Aliados. Cerca de dezoito mil paraquedistas britânicos e americanos saltavam sobre a Normandia (norte da França), ocupando pontes importantes e destruindo linhas de comunicação alemã. Às 06h30 desembarcaram as primeiras tropas compostas por forças americanas que desceram na prais de Utah com seus tanques anfíbios. As praias de desembarque receberam nomes diferentes dos originais para não comprometer a operação. Menos de uma hora depois, às 07h25, os primeiros soldados britânicos chegavam às praias Gold e Sword, seguidos, na praia Juno, por 2.400 canadenses apoiados por 76 tanques anfíbios. No dia 7 de junho de 1944, os criptoanalistas de Bletchley Park decifraram uma mensagem da máquina Enigma enviada pela Força Aérea Alemã para a força de paraquedistas estacionada em Nancy, aludindo à falta de combustível. Outra contribuição de Bletchley Park foi que através de mensagens decifradas foi descoberta a localização do quartel general das forças Panzer no Ocidente em La Caine. O local foi bombardeado e muitos oficiais alemães foram mortos.

Esta ofensiva dos Aliados abria mais uma frente de batalha para os alemães que já lutavam contra os russos na frente oriental e os Aliados ocidentais na Itália.

Abaixo vemos a continuação do diálogo do narrador *Alan Turing* no filme: “O jogo da imitação, 2014”.

> **Turing: -** Liberdade contra tirania, Democracia contra Nazismo. Exército de milhões sangrando no chão. Frotas de navios afundando no oceano. Aviões lançando bombas do céu até que destruíssem o sol. A Guerra não era assim para nós. Éramos só meia dúzia de entusiastas numa vila ao sul da Inglaterra.
>
> **Turing**: - Eu era Deus? Não! Deus não ganhou a Guerra. E nós ganhamos.
>
> **Nock**: - Inacreditável.
>
> **Turing**: - Agora, detetive, você faz o julgamento. Então me diga, o que eu sou? Sou uma máquina ou ser humano? Um herói de guerra? Ou criminoso?
>
> **Nock:** - Não posso te julgar.
>
> **Turing:** - Então, você não me serve em nada. (MORTHEN TYLDUN, 2014)

Identificou-se com esse diálogo entre *Alan Turing* e o detetive *Nock*, o que ficou conhecido como jogo da imitação. Mais tarde se tornaria o teste de *Turing*. No exemplo a seguir aparecem 3 participantes em outra situação do teste de *Turing*.

> O jogo como ele explica, (LEAVITT apud TURING, 2007, p. 255) é jogado por 3 pessoas: um homem (A), uma mulher (B) e um interrogador (C), que pode ser de qualquer sexo. O interrogador fica em uma sala longe dos outros dois. O objetivo do jogo para o interrogador é determinar qual dos outros dois jogadores é o homem e qual é a mulher. Ele os identifica pelas etiquetas X e Y e, ao final do jogo, ele diz: “X é A e Y é B” ou “X é B e Y é A”. O interrogador pode fazer perguntas a A e a B assim: C: X pode me dizer o comprimento de seu cabelo? Agora vamos supor que X é realmente A. Então A deve responder. O objetivo de A no jogo é tentar provocar C a fazer a identificação errada. Sua resposta, portanto poderia ser: “Meu cabelo é cortado rente, e os fios mais compridos têm cerca de 20 centímetros”. A fim de que o timbre de voz não ajude o interrogador, as respostas devem ser escritas, ou melhor ainda, datilografadas”.

Figura 42 – *Alan Turing* acusado de indecência

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (1:42:00).

Uma das notícias do jornal referenciado na figura 42 diz que o Professor *Alan Turing* de *Cambridge* foi sentenciado por indecência.

O ano de 1938 viu a primeira exibição britânica da versão *Disney* de Branca de Neve e os Sete Anões, um filme que curiosamente, exerceu grande fascínio em *Alan Turing*. *Turing* assistiu Branca de Neve e sentiu um grande prazer com a cena em que a Rainha Malvada mergulha a maçã no caldo envenenado. “Mergulhe a maçã no caldo/Deixe o sono mortal impregná-la”, ela canta, e depois cacareja para seu parceiro, um corvo, enquanto o veneno forma um crânio na superfície da maçã. A cena cativou *Turing* com tal intensidade que ele passou a cantarolar os versos da rainha a todo instante (LEAVITT, 2007, p. 151) e que serviu de inspiração para o modo pelo qual ele escolheu morrer.

Em 1952, foi preso por fazer sexo com um homem de 19 anos de idade, e foi-lhe oferecida uma escolha – ou ir para a cadeia ou concordar a se submeter a tratamentos hormonais experimentais para “curar” a homossexualidade. Decidiu pelos tratamentos, o que lhe causou dor agonizante e ampliada em seus seios.

Na manhã de 7 de junho de 1954, *Turing* preparou uma mistura de cianeto em seu laboratório em casa, injetou em uma maçã e, em seguida, deu uma mordida. Morreu em poucos minutos. Apenas quatro pessoas, uma delas sua mãe, participaram do funeral. Quase quatro anos depois do dia de sua morte, a homossexualidade foi descriminalizada na Grã-Bretanha.

Turing viria a ser imortalizado, não por seu papel no “ULTRA”, mas por sua maior contribuição para a máquina que criou a Era da Informação. Cerca de 20 anos depois de sua morte, dois estudantes universitários americanos de 19 anos de idade, que trabalhavam na garagem de seus pais, montaram o primeiro computador doméstico completo. A máquina, bem como sua nova empresa, foi chamada *Apple* (VOLKMAN, 2013). Apenas algumas pessoas compreenderam o significado do logotipo da empresa; uma maçã com uma única mordida.

A Segunda Guerra Mundial tem proporcionado diversas interpretações sobre o conflito, incluindo a grande quantidade de filmes sobre o assunto.

O cinema, como fonte histórica, permite refletir sobre peculiaridades de determinado contexto. Em 1940, por exemplo, *Charles Chaplin* protagonizou o filme "O Grande Ditador" parodiando *Hitler* e o nazismo.

Autores como *David Herling*, *Leslie Fishbein*, *Aston Kaes* e outros afirmam que os audiovisuais são formas discursivas capazes de representar o passado. *Ingmar Bergman*, em 1977 fez o filme "O ovo da serpente", no qual mostrou a desumanização das pessoas na Alemanha no início da expansão do nazismo. O cineasta judeu *Steven Spielberg* concluiu o filme "A lista de *Schindler*" em 1993, sobre o massacre de judeus e outros opositores do regime em campos de concentração nazistas.

Os filmes permitem refletir sobre a relação existente entre as características dos discursos audiovisuais e suas diferenças e semelhanças em relação a outros tipos de discursos como a literatura e a historiografia escrita e oral, por exemplo. Em 2005 o filme "A queda – as últimas horas de Hitler" mostra o suicídio de *Adolf Hitler* em abrigo antiaéreo (*bunker*), no momento em que tropas soviéticas ocupam Berlim. Os filmes citados refletem uma visão dos Aliados em relação à Alemanha nazista. São obras engajadas que apontam o que houve de pior no modelo alemão da era *Hitler*.

Como os discursos históricos áudio-imagéticos (vídeo, cinema e imagens digitais) podem explorar as potencialidades da realidade para a escrita da História, optamos por escolher um filme, por sugestão do Professor orientador, para servir como estudo de caso, articulado à temática desta dissertação.

No próximo capítulo vamos mostrar o surgimento e evolução da criptografia.

CAPITULO II. Surgimento e evolução da criptografia

"O Serviço de Informações é o apanágio dos nobres; se confiado a outros, desmorona."

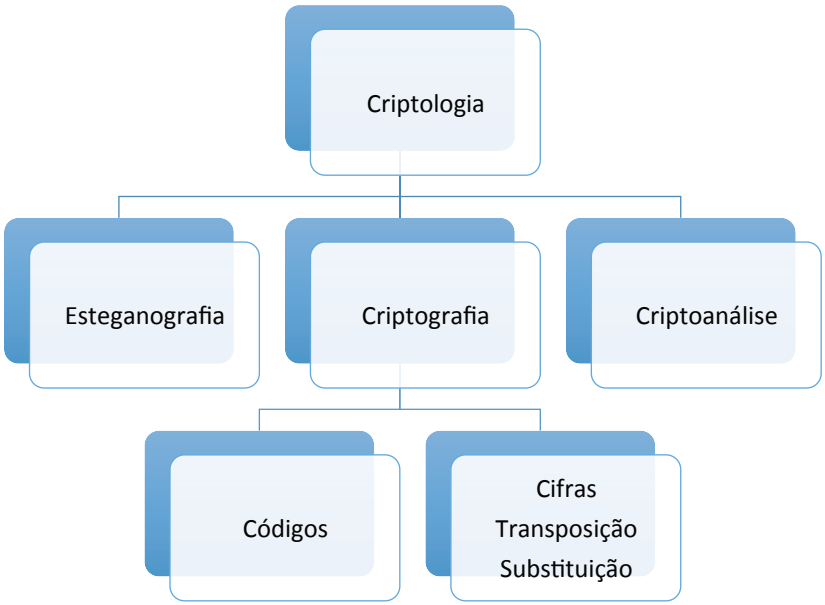
Coronel Walter Nicolai
Chefe do Serviço de Informações alemão durante a Primeira Guerra Mundial.

1. Apresentação

Este capítulo apresenta um arcabouço histórico que seja capaz de explicar, em linhas gerais, o surgimento e evolução da criptografia e a sua aplicação nos conflitos, com destaque para a Segunda Guerra Mundial.

As principais áreas da criptologia são mostradas na figura 43. Basicamente, são a esteganografia, a criptografia e a criptoanálise. Na criptografia destacam-se os códigos e as cifras. As cifras podem ser de substituição ou de transposição.

Figura 43 – Áreas da criptologia



Fonte: Elaborado pelo autor

Inicialmente, fez-se a distinção entre códigos e cifras. O Novo Dicionário Aurélio (1986) define e palavra código como “vocabulário ou sistemas de sinais convencionais ou secretos utilizados em correspondências e comunicações ”. A cifra é tida como uma “explicação ou chave duma escrita enigmática ou secreta”.

> Ao afirmar que esteganografia não é criptografia, Stallings nos informa que uma mensagem em texto claro pode estar oculta de duas maneiras. Os métodos de esteganografia escondem a existência da mensagem, enquanto os métodos de criptografia tornam a mensagem ininteligível a estranhos por meio de várias transformações do texto. Uma forma simples de esteganografia, mas que é demorada de construir, é aquela em que um arranjo de palavras e letras dentro de um texto aparentemente inofensivo soletra a mensagem real. Por exemplo, a sequência de primeiras letras de cada palavra da mensagem geral soletra a mensagem escondida. (STALLINGS, 2008, p. 34)

Ao afirmar que o texto está “criptografado”, equivale a dizer que suas informações foram tornadas inteligíveis por meio de substituições de caracteres que compõem a mensagem de uma maneira que somente aquele que possui a chave poderá tornar aquilo compreensível. A palavra cripto vem do grego *Kryptos*, que descreve algo oculto, envolto, escondido. *Graphos* também é grego e é ligada ao ato de escrever. Outras duas palavras surgem daí: logos, estudo, ciência; e *analysis*, decomposição. Criptologia, portanto, é o estudo da escrita cifrada e se ocupa com a criptografia e a criptoanálise.

Um exemplo básico de som encriptado (criptofonia) é a língua do P, usada pelas crianças para esconder uma mensagem

As palavras, caracteres ou letras da mensagem original inteligível constituem o Texto ou Mensagem Original (também conhecido como Mensagem Clara ou Texto Plano). Já as palavras, caracteres ou letras da mensagem cifrada são chamados de Texto Cifrado, Mensagem Cifrada ou Criptograma.

> Os sistemas de substituição são os mais numerosos. Nas cifras, a unidade básica da substituição é a letra e, algumas vezes, pares de letras (dígrafos ou digramas). Excepcionalmente são usados grupos

> maiores de letras, os poligramas. O conjunto de caracteres de substituição (números, letras ou sinais) forma um alfabeto substituto, chamado de alfabeto cifrante ou simplesmente de cifrante. Algumas vezes o cifrante fornece mais de um substituto. Neste caso, os substitutos adicionais são chamados de homófonos (para o mesmo som). Um alfabeto cifrante também pode conter símbolos sem significado, apenas para confundir os criptoanalistas. Esses símbolos são chamados de nulos. Quando apenas um alfabeto cifrante é usado, o sistema denomina-se monoalfabético; quando mais de um é utilizado, o sistema é dito polialfabético. (TKOTZ, apud COUTO, 2008, p. 14).

A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. O nome criptografia teve origem na palavra *cryptos* que significa secreto, oculto. A criptografia tem uma irmã gêmea na arte de decifrar códigos secretos, ou criptoanálise. Naturalmente todo código vem acompanhado de duas receitas: uma para codificar uma mensagem; outra para decodificar uma mensagem codificada. Decodificar é o que um usuário legítimo do código faz quando recebe uma mensagem codificada e deseja lê-la. Já decifrar significa ler uma mensagem codificada sem ser um usuário legítimo (COUTINHO, 2003, p. 1).

Na criptografia é necessário o uso dos chamados “números aleatórios criptograficamente fortes”. Quando se precisa gerar este tipo de número, o inimigo não pode nem desconfiar qual o número escolhido. Se o inimigo reproduzir o processo de geração do número e/ou limitar a faixa de valores, então esse número não é adequado para criptografia. Um número aleatório é aquele que foi gerado a partir de um processo totalmente aleatório como por exemplo, um dado honesto (não viciado) ou uma moeda (CARVALHO, 2000, p. 59).

Carlos (2015, p. 2) nos informa que a criptografia simétrica, é usada a mesma chave para codificar e decodificar a mensagem. Na criptografia assimétrica existe um par de chaves, sendo uma chave considerada pública que pode ser disponibilizada livremente e outra privada que deve ser mantida em posse de seu

detentor. “Essas chaves são complementares, ou seja, uma mensagem cifrada com uma chave deve ser decifrada por sua chave correspondente”.

Até recentemente, tanto a criptoanálise quanto a criptografia eram considerados uma arte. A criptologia (criptografia + criptoanálise) vem ganhando um destaque maior a aproximadamente 20 anos. A *International Association for Cryptologic Research* (IACR ou Associação Internacional para a Pesquisa Criptológica) é a organização científica internacional que coordena a pesquisa nesta área e maiores informações podem ser encontradas no sítio Internet: http://www.iacr.org. A criptologia como ciência é recente mas sua história remonta aos primórdios da humanidade (TKOTZ, 2005, p. 16).

2. Criptografia Clássica

Os hieróglifos são considerados pela maioria dos historiadores como a mais antiga forma de escrita do mundo. O hierático é uma forma simplificada de representação dos hieróglifos e ainda temos uma terceira versão chamada demótico, como utilizado na Pedra de Rosetta. Hieróglifo vem da junção de duas palavras gregas, *hieros* (sagrado) e *glyphós* (escrita) (COUTO, 2008, p. 4).

Um dos assuntos que mais chamam a atenção das pessoas são os hieróglifos do antigo Egito. Os hieróglifos foram associados aos sons das palavras que representavam pelos escribas do antigo Egito e gradativamente foram se transformando em um alfabeto fonético (TKOTZ, 2005, p. 325).

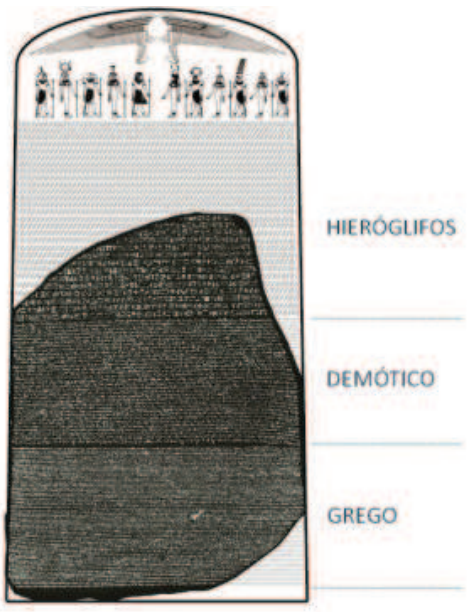
A Pedra de Rosetta foi encontrada pelo oficial francês *Bouchard* em 1799 nas imediações da cidade de Rosetta no Egito. Esta decoberta chamou a atenção no mundo inteiro porque era a primeira peça bilíngue do Egito antigo. Em 1801, os britânicos derrotaram os franceses no Egito e capturaram a Pedra Rosetta e levaram para o Museu Britânico em Londres onde permanece até hoje.

Figura 44 – Pedra de Rosetta

Fonte: https://i2.wp.com/cdn.historyextra.com/sites/default/files/imagecache/623px_wide/Rosetta.jpg

Na figura 45 é possível observar através de uma reconstituição gráfica o formato original da Pedra Rosetta com inscrições na forma de hieróglifos, demótico e grego.

Figura 45 – Representação gráfica da Pedra Rosetta



Fonte: https://ahistoriadoseculo.files.wordpress.com/2015/07/rosetta.jpg?w=293&h=364

Champollion percebeu que a contagem de frequência de caracteres também pode ser usado para decifrar inscrições antigas. Para decifrar os hieróglifos egípcios Champollion começou o processo contando caracteres nas inscrições da pedra de Rosetta. Ele descobriu que havia 486 palavras no texto grego e 1419 caracteres no texto em hieróglifos. Portanto a escrita dos antigos egípcios não podia ser ideográfica (COUTINHO, 2003, p. 2).

Na Idade Antiga, em aproximadamente 1900 A.C., é possível identificar a primeira ocorrência histórica do emprego de técnicas para ocultação de mensagens. Em uma vila egípcia perto do rio Nilo chamada *Menet Khufu, Khnumhotep II*, arquiteto do faraó *Amenemhet II*, construiu monumentos para o faraó, documentados em tabletes de argila substituindo algumas palavras ou trechos de texto com o intuito de confundir possíveis leitores não autorizados.

Aproximadamente 1500 A.C., mercadores assírios usavam *intaglios* (peças planas de pedra com símbolos entalhados) para identificação de seus produtos. Esta técnica pode ser considerada como as primeiras assinaturas registradas a conferir autenticidade. Na mesma época as culturas do Egito, China, Índia e Mesopotâmia desenvolvem a esteganografia.

O primeiro caso confirmado do uso de esteganografia foi registrado por *Heródoto* no livro “As Histórias”. O relato diz que *Hístio*, um grego do século V a.C. queria se comunicar com *Aristágoras* de Mileto e para isso escolheu um escravo fiel, raspou-lhe a cabeça, escreveu a mensagem, esperou o cabelo crescer e o enviou. Outro episódio do uso da esteganografia, foi o rei *Demaratos* que queria avisar os espartanos de um ataque eminente. Para que a mensagem não fosse interceptada e decifrada, foram utilizados tabletes usados na escrita, retirou a cera que os cobria, gravou no material que sobrou suas informações e então os cobriu novamente com cera. Dessa forma pareciam que não tinham sido usados mas a mensagem estava lá. *Gorgo* que era esposa do rei Leônidas de Esparta recebeu a mensagem e as repassou para os outros gregos que venceram os persas.

O historiador grego Enéias, o Tático revela que para enviar uma mensagem secreta ele fez pequenos furos em certas letras de um texto que não fosse composto

apenas pela mensagem. Para ler a mensagem bastava seguir a ordem dos furos pelo receptor.

Entre 600 e 500 a.C., escribas hebreus usaram uma cifra de substituição simples pelo alfabeto reverso conhecida como ATBASH no processo de escrita da obra conhecida como o livro de Jeremias. As cifras mais conhecidas da época são, além do ATBASH, o ALBAM e o ATBAH que em conjunto são as chamadas cifras hebraicas.

Já na Grécia Antiga, o bastão de Licurgo ou *scytale* espartano era um bastão que se enrolava uma tira de couro ou pergaminho. O remetente escrevia a mensagem ao longo do bastão e depois desenrolava a tira, a qual então se convertia numa sequência de letras sem sentido. O mensageiro usava a tira como cinto, com as letras voltadas para dentro. O destinatário, ao receber o ”cinto”, enrolava no seu bastão, cujo diâmetro era igual ao do bastão do remetente. Desta forma, era possível ler a mensagem (COUTO, 2008).

Ainda na Grécia Antiga, o historiador grego *Políbio,* que nasceu em Megalópolis a aproximadamente 200 a.C., descreveu a expansão do Império Romano e suas conquistas. Estes registros estão armazenados em 40 volumes da obra *Histórias* que constitue umas das primeiras obras da história universal. Em algum destes volumes existe um relato de um método de cifragem que apesar do nome “Código de Políbio” não foi criado por ele. Os verdadeiros autores deste método de cifragem são: *Cleoxeno* e *Democleto.*

Em uma grade de 5 x 5, com linhas e colunas numeradas, cada célula recebe uma letra do alfabeto e cada letra é substituída pelas coordenadas de sua posição.

TABELA 2 – Grade para o código de Políbio

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K/Q	L	M	N	O
4	P	R	S	T	U
5	V	W	X	Y	Z

Fonte: TKOTZ, 2005

O código de Políbio permite a conversão de letras em números e reduz o número de caracteres (25 caracteres são reduzidos para 5 números diferentes) e ainda existe a possibilidade de dividir uma unidade em duas partes que podem ser manipuladas isoladamente.O criptograma abaixo foi obtido de acordo com a tabela 1

“341135 21111311 3411 51241411 41451232241311 35 314515 51351315 211155 3411 41422451111411”

De acordo com os caracteres citados acima, a mensagem decifrada é: N (34) A (11) O (35) F (21) A (11) C (13) A (11) N (34) A (11) V (51) I (24) D (14) A (11) P(41) U (45) B (12) L (32) I (24) C (13) A (11) O (35) Q (31) U (45) V (51) O (35) C (13) E (15) F (21) A (11) Z (55) N (34) A (11) P (41) R (42) I (24) V (51) A (11) D (14) A (11), ou seja, “Não faça na vida pública o que você faz na privada” (TKOTZ, 2005).

Durante a Idade Média, a contribuição islâmica foi significativa, documentando estudos como a criptoanálise para a substituição monoalfabética. A denominação ”Cifra”, ”Chiffre”, ”Ziffer”, como também ”zero”, utilizado em muitas línguas, vêm da palavra árabe ”sifr”, que significa ”nulo” (COUTO, 2008).

Jean-François Champollion (1790-1832) foi linguista e egiptólogo francês e considerado o “pai” da egiptologia. Aos 16 anos já conhecia os idiomas: hebreu, árabe, persa, chinês, além de outras línguas asiáticas. Champollion era intrigado com os hieróglifos egípcios e começou a estudá-los. Com a descoberta da Pedra de

Rosetta em 1799 pelo Exército francês no Egito, *Champollion* resolveu decifrar o código. O pesquisador francês se baseou nos trabalhos do barão *Silvestre de Sacy*, *Johan David Ackerblad* e *Thomas Young*. Inicialmente *Champollion* pensava que os hieróglifos eram puramente simbólicos e que não tinham nada de fonéticos mas mudaria de ideia. Champollion se convenceu de que muitos hieróglifos possuíam um valor de efeito fonético. O sistema egípcio usava tanto sinais que representavam ideias quanto alguns que representavam sons.

Em 1824 lançou um livro chamado *Precís du Système Hièroglyphique* (Princípios do Sistema Hieróglifo), onde os princípios pesquisados por ele foram aplicados por 16 meses nas ruínas do Antigo Egito e tornou-se o decifrador das inscrições da Pedra Rosetta (COUTO, 2008, p. 8).

2.3 Cifras Clássicas

O termo “cifras clássicas” refere-se a técnicas de criptografia criadas antes da segunda metade do século XX e que se tornaram muito conhecidas através dos tempos, algumas tendo milhares de anos. Muitas das técnicas clássicas são variações da substituição simples e da transposição simples. Mesmo sendo o que havia disponível durante um período tão grande, as cifras clássicas não sobreviveriam ao uso nos dias de hoje, conforme explica Menezes: “De qualquer modo, como essas técnicas não são nem sofisticadas nem seguras contra as capacidades critoanalíticas atuais, elas não são geralmente convenientes para uso prático” (MENEZES, 1997, p. 238).

2.3.1 Cifras de substituição

Em uma cifra de substituição, cada letra ou grupo de letras é substituído por outra letra ou grupo de letras, de modo a criar um “disfarce”. Uma das cifras mais antigas é a cifra de César (*Caeser cipher*), atribuída a Júlio César. Nesse método “a”

se torna “D”, “b” se torna “E”, “c” se torna “F”, … e “z” se torna “C”. Por exemplo, “*ataque”* passaria a ser DWDTXH. Nos exemplos, o texto simples é apresentado em letras minúsculas e o texto cifrado em letras maiúsculas. Uma ligeira generalização da cifra de César permite que o alfabeto do texto cifrado seja deslocado “*k”* letras em vez de três. Nesse caso, “k” passa a ser uma chave para o método genérico dos alfabetos deslocados em forma circular. A cifra de César pode ter enganado os cartagineses, mas nunca mais enganou ninguém. O próximo aprimoramento foi fazer com que cada um dos símbolos do texto simples, digamos 26 letras, seja mapeado para alguma outra letra. Por exemplo,

TABELA 3 – Mapeamento entre texto simples e texto cifrado

texto simples	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
texto cifrado	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

Fonte: Tanenbaum, 2003, p. 774

Esse sistema geral é chamado “substituição monoalfabética”, sendo a chave o *string* de 26 letras correspondente ao alfabeto completo. Para a chave anterior, o texto simples “ataque” seria transformado no texto cifrado QZQJXT. (TANENBAUM, 2003, p. 774).

2.3.2 Cifras de transposição

As cifras de substituição preservam a ordem dos símbolos no texto simples, mas disfarçam esses símbolos. Entretanto, as cifras de transposição reordenam as letras mas não as disfarçam. A próxima figura mostra uma cifra de transposição muito comum, a transposição de colunas. A cifra se baseia em uma chave que é uma palavra ou frase que não contém letras repetidas. Nesse exemplo, MEGABUCK é a chave. O objetivo da chave é numerar as colunas de modo que a coluna 1 fique

abaixo da letra da chave mais próxima do início do alfabeto e assim por diante. O texto simples é escrito horizontalmente, em linhas. O texto cifrado é lido com colunas, a partir da coluna cuja letra da chave seja a mais baixa.

TABELA 4 – Uma cifra de transposição

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Fonte: Tanenbaum,(op. cit., p. 776)

Ao exemplificar a tabela acima , em (1) tem-se um texto simples. Em seguida, em (2), o texto cifrado.

(1) Texto simples

pleasetransferonemilliondollarstomyswissbankaccountsixtwotwo

(2) Texto cifrado

AFLLSKSOSELAWAIATOOSSCTCLNMOMANTESILYNTWRNNTSOWDPAEDOBU OERIRICXB (TANENBAUM, 2003, p. 776)

2.4 Criptografia Moderna

A Itália foi o berço do renascimento por volta do século XV e esse movimento que marcou o renascimento das artes, ciências e da educação produziram o conhecimento necessário para a criptografia. As cidades-estados italianas

independentes estavam competindo entre si nos campos políticos e militar e a criptografia para se comunicaram em segredo se tornou vital.

Giovanni Soro foi o primeiro grande criptoanalistas europeu e foi nomeado secretário de cifras de Veneza em 1506. O Vaticano que provavelmente o segundo maior centro de criptoanálise da Europa na época, enviava mensagens aparentemente indecifráveis para Soro. A corte francesa empregou criptoanalistas como *Philibert Babou* que era o criptoanalista do rei Francisco I da França. No século XVI, a França aumentou sua capacidade de decifrar mensagens com a chegada de *François Viète* que ficou famoso em decifrar mensagens dos espanhóis. Era necessário criar novas formas de cifragem já que os criptógrafos estavam dependentes da substituição monoalfabética e os criptoanalistas estavam usando a análise de frequência (SINGH, 2014).

Considerado como o “pai da criptologia ocidental”, *Leon Battista Alberti* no século 15 d.C. criou o disco de Alberti por volta de 1467. Alberti trabalhava com arquitetura, artes, ciências e direito.

Figura 46 – O disco de Alberti

Fonte: https://upload.wikimedia.org/wikipedia/commons/thumb/7/70/Alberti_cipher_disk.JPG/480px-Alberti_cipher_disk.JPG

Alberti resolveu ajudar Leonardo Dato que era secretário pontifício do Vaticano já que Dato queria enviar mensagens cifradas para todas as entidades católicas do mundo. Em 1467, Alberti fez um ensaio que daria as bases para uma nova maneira de cifrar. O ensaio incluía uma explicação de análise de frequência do idioma italiano e oferecia várias maneiras de resolver cifras. O ensaio também apresentava um sistema de encriptação que usava dois discos concêntricos de metal cujas circunferências eram divididas em 24 partes iguais. Os segmentos do disco externo continham as letras do alfabeto em ordem aleatória (menos as letras "h", "k" e "y", além das letras que não havia no alfabeto latino, como "j", "u" e "w") e números de 1 a 4.

Para enviar uma mensagem cifrada, as letras ou números de uma texto claro eram lidas no disco externo e substituídas pelas correspondentes à mesma posição no disco interno. Alberti criou um método chamado substituição polialfabética que permitia que diferentes símbolos cifrados possam representar o mesmo símbolo do texto claro (COUTO, 2008, p.76).

TABELA 5 – Alfabeto cifrante de Alberti com a letra "k" ajustada com T

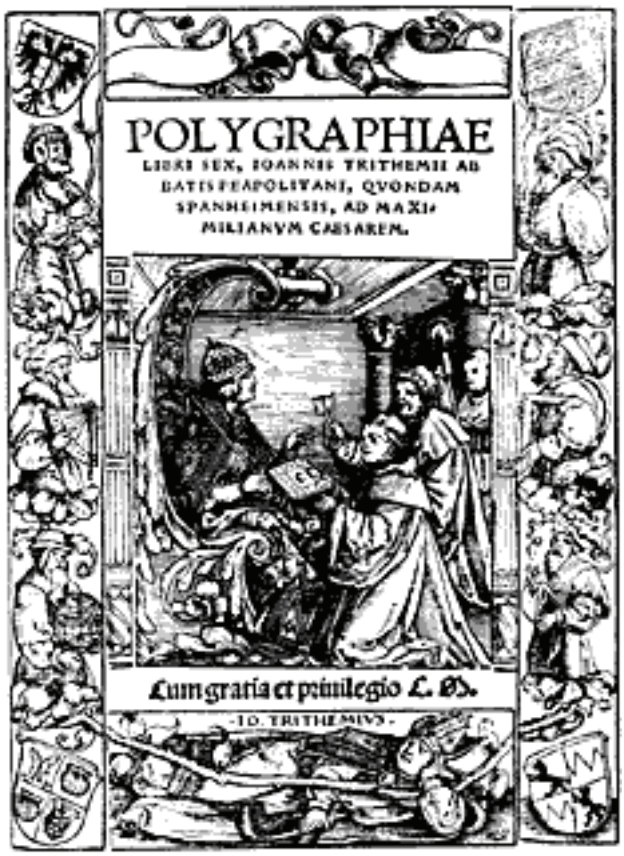
A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
c	&	b	m	d	g	p	f	z	n	x	y	v	t	o	s	k	e	r	l	h	a	i	q

Fonte: TKOTZ, 2005

A mensagem "disco de Alberti" será cifrado como T "mfsby md cz&dokf". Parece uma substituição simples mas Alberti sugere trocar o alfabeto cifrante durante o processo de cifragem, indicando os pontos de troca pelas letras maiúsculas apontadas pela letra-chave (TKOTZ, 2005, p. 195).

O abade alemão Johannes Trithemius (1462-1516) foi o primeiro a publicar um livro sobre criptografia chamado *Polygraphia* que era um tratado sobre códigos e cifras que foi publicado como uma séria de seis livros após sua morte, em 1516.

Figura 47 – Capa do livro Polygraphiae



Fonte: http://www.numaboa.com.br/images/stories/cripto_subst/polysm.gif

A técnica de encriptação apresentada por *Trithemius* é uma versão precoce e primitiva que seria empregada na máquina de cifragem Enigma alguns séculos mais tarde. A tabela de *Trithemius* é chamada de Tabela Reta (*tabula recta*), que consiste em um quadro onde cada linha substitui a anterior com um deslocamento de um caracter para a esquerda. Trithemius usava a Tabela Reta para definir uma cifra polialfabética equivalente à do Disco de Alberti. Para cifrar um texto, localize a linha com a primeira letra a ser cifrada e a coluna com a primeira letra da chave. A letra onde a linha e a coluna se cruzam é a letra cifrada (COUTO, 2008, p.78).

Figura 48 – A Tabela Reta de Trithemius

In hac tabula literarū canonica siue recta tot ex uno & usuali nostro latinarum literarum ipsarum permutationem seu transpositionē habes alphabeta, quot in ea per totum sunt monogrammata, uidelicet quater & uigesies quatuor & uiginti, quæ faciunt in numero p. lxxvi. ac per totidē multiplicata, paulo efficiunt minus q̄ quatuordecē milia.

o ñ

Fonte: http://www.numaboa.com.br/images/stories/cripto_subst/tableau.gif

Na figura 48, traduzindo do latim, lê-se:

> Sobre esta tabela ou carreiras de letras coloca-se, por permutação ou transposição, o alfabeto usual das nossas letras latinas; ou então, coloca-se nesta tabela todos os monogramas, de 24 em 24, o que totaliza um número de 576 que, multiplicado por outro tanto (24), corresponde a um pouco menos de 14.000 (TKOTZ, 2005, p. 196).

O primeiro dos seis livros da *Polygraphiae livri sex, Ioannis Trithemii abbatis Peapolitani, quondam Spanheimensis, ad Maximilianum Ceasarem* que significa Poligrafia em seis livros por João *Trithemius*, abade de *Wurzburg*, antes *Sponheim*, dedicados ao imperador Maximiliano) contém 384 colunas de palavras em latim, onde cada palavra corresponde a uma letra do alfabeto. As mensagens secretas estão disfarçadas de “orações” e “textos piedosos”.

Um dos alfabetos mostrava a seguinte correlação:

TABELA 6 - Correlação de um dos alfabetos de *Trithemius*

a	Deus
b	Creator
c	Conditor
d	Opisex
e	Dominus

Fonte: Viktoria Tkotz (2005, p.119).

Um segundo alfabeto fornecia a seguinte correlação:

TABELA 7 – Correlação do segundo alfabeto de *Trithemius*

a	clemens
b	clementissimus
c	pius
d	pijssimus
e	magnus

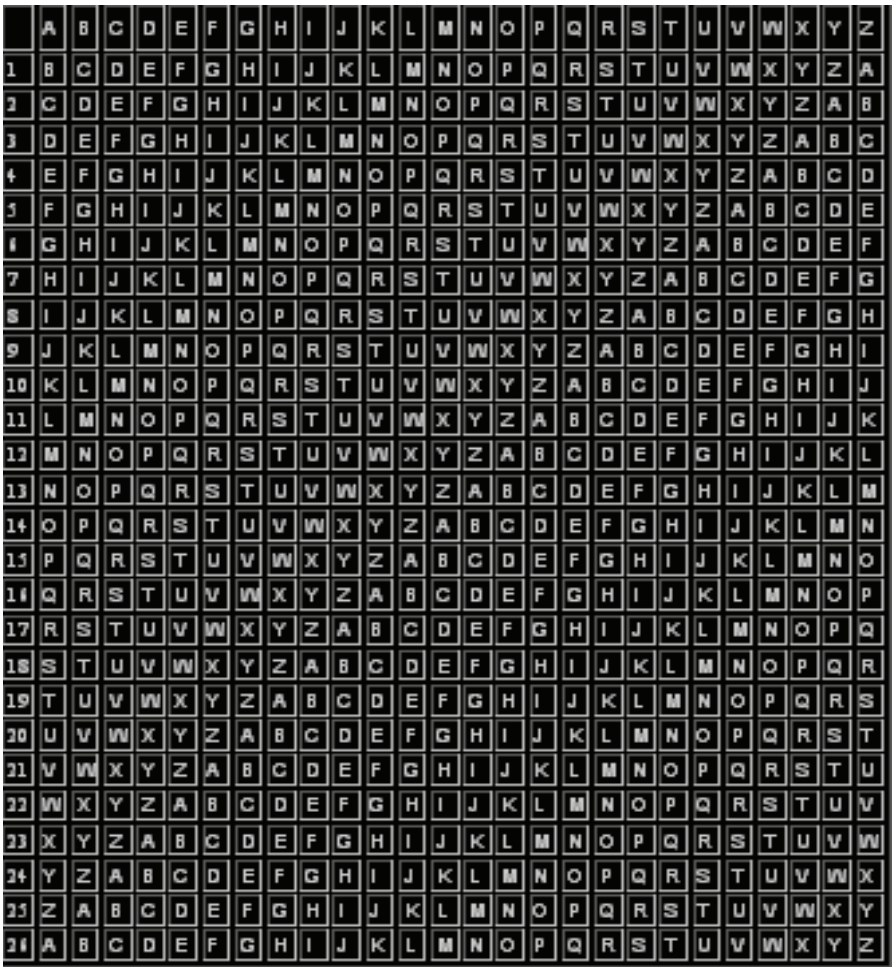
f	excelsus
g	maximus
h	optimus

Fonte: Vitoria TKOTZ (op.cit., p.119).

A palavra faca, por exemplo, pode ser cifrada como *Dominator clemens pius Deus* (TKOTZ, 2005, p.119).

A cifra de *Vigenère* usa uma tabela similiar a de *Trithemius* e é uma versão simplificada da cifra de substituição polialfabética que foi inventada por *Leone Battista Alberti*, em 1465. Apesar do nome que recebe, não foi inventada por *Blaise de Vigenère*, que teria inventado uma outra cifra conhecida como Cifra de Autochave (COUTO, 2008, p.79).

Figura 49– Tabela de *Vigenère*



Fonte: http://www.simonsingh.net/The_Black_Chamber/z_cipherimages/v_square.png

Por exemplo, ao enviar a mensagem ATACAR BASE SUL usando a cifra de Vigenère. Era escolher uma chave e repeti-la até acabar as letras da mensagem original.

TABELA 8 - Emparelhamento para cifra de Vigenère

Palavra-chave	L	I	M	A	O	L	I	M	A	O	L	I	M
Mensagem	A	T	A	C	A	R	B	A	S	E	S	U	L

Fonte: (COUTO, 2008)

A primeira letra do texto será cifrada com a alfabeto da linha L (a primeira letra da palavra-chave). Observe na tabela 8 que a linha L e procuramos a coluna correspondente a primeira letra da mensagem (A), o cruzamento das duas nos dá um “L”.

TABELA 9 – Codificação da mensagem pela cifra de Vigenère

Palavra-chave	L	I	M	A	O	L	I	M	A	O	L	I	M
Mensagem	A	T	A	C	A	R	B	A	S	E	S	U	L
Cifrado	L	B	M	C	O	C	J	M	S	S	D	C	X

Fonte: COUTO, (op.cit.)

Charles Wheatdtone (1802-1875) foi um cientista britânico apaixonado por criptologia. Wheatdtone tinha um amigo intitulado Barão de *Playfair* que tinha influência política na corte britânica. *Wheatdtone* desenvolveu uma cifra de “segurança máxima” para ser apresentada para alguns integrantes do governo inglês mas eles não aceitaram inicialmente. De alguma forma o Barão de *Playfair* conseguiu que a cifra de *Wheatdtone* fosse adotado pelo governo mas o nome da cifra acabou sendo conhecida como a cifra de *Playfair*. O diferencial desta cifra está no fato de distribuir as letras do alfabeto de forma organizada no tabuleiro de Políbio: usa-se uma palavra-chave. Observe o exemplo abaixo com a palavra-chave (Palmerston).

TABELA 10 – Exemplo de grade para a cifra de Playfair

P	A	L	M	E
R	S	T	O	N
B	C	D	F	G
H	I/J	K	Q	U
V	W	X	Y	Z

Fonte: (TKOTZ, 2005)

É necessário preparar a mensagem em texto claro para ser realizada a cifragem. Isole os digramas e se repetir alguma letra, separe com a letra “X”. Outro exemplo usando a mensagem de texto claro: “Wheatstone viu sua cifra ser chamada de Playfair” ficaria desta forma: “WH EA TS TO NE VI US UA CI FR AS ER CH AM AD AD EP LA YF AI RX”. A última letra “X” é apenas para completar o último digrama. A localização das letras dos digramas na grade só oferece três possibilidades:

1. estão na mesma linha;
2. estão na mesma coluna;
3. estão em linhas e colunas diferentes.

As letras do digrama “EA”, estão na mesma linha e serão substituídas pelas letras à sua direita. A letra “E” ocupa a última coluna, e será trocada pela letra da primeira coluna. Seria como se as colunas seguissem o sentido horário para a direita transformando “PALME” em “EPALM”. As letras EA fornecem o novo digrama PL.

Quando as letras do digrama estão na mesma coluna, como “YF”, devem ser trocadas pelas letras abaixo delas. Como a letra “Y” está na última linha, “gira-se” o conjunto “MOFQY” para baixo para obter “YMOFQ” e fazer a troca de “YF” por “MQ”.

As letras “US”, estão em linhas e colunas diferentes. Marca-se a primeira letra do digrama e a coluna da letra com a qual ela faz par. A letra correspondente ao cruzamento da linha com a coluna será substituída, ou seja, I.

TABELA 11 – Exemplo de grade para a cifra de Playfair

P	A	L	M	E
R	S	T	O	N
B	C	D	F	G
H	I/J	K	Q	U
V	W	X	Y	Z

Fonte: (TKOTZ, 2005)

Depois de aplicar as três regras de substituição da cifra Playfair, o texto claro “WH EA TS TO NE VI US UA CI FR AS ER CH AM AD AD EP LA YF AI RX” obtem-se o criptograma abaixo.

“WI PL OT ON GN WH IN IE IW BO SC PN BI LE LC LC PA ML MQ SW TV” (TKOTZ, 2005, p. 213).

A Lei de *Kerckhoffs* como ficou conhecida foi dada em homenagem a um homem importante na área de criptografia chamado *Auguste Kerckhoffs* que vivia em Melun a 40 Km de Paris no final do século XIX. *Kerckhoffs* escreveu em 1883 um livro considerado hoje como essencial na área de criptografia, *la Criptographie Militaire*. O ilustre autor determinou uma lista de seis avaliações formais que são usadas até hoje para desenvolver cifras militares.

1. O sistema deve ser indecifrável em nível substancial e matemático.
2. O sistema não deve requisitar segredo e pode ser roubado pelo inimigo sem causar problemas.
3. O sistema deve ser fácil de comunicar e lembrar as chaves sem precisar de notas escritas; deve também ser fácil de mudar ou modificar as chaves com diferentes participantes.
4. O sistema precisa ser compatível com o sistema de telégrafos.
5. O sistema deve ser portátil e seu uso não deve exigir mais que uma pessoa.
6. O sistema deve ser fácil de utilizar e não deve requerer estresse da mente ou conhecimento de uma longa série de normas.

De todas as regras acima a mais famosa é a segunda. O sistema deve ser seguro mesmo se todas as informações sobre ele, com exceção de sua chave, for de conhecimento público (COUTO, 2008, p. 143).

Não podemos nos esquecer das contribuições do criptoanalista francês *Étienne Bazeries* (1846-1931). Lutou na Guerra Franco-Prussiana (1870-1871) e foi promovido a tenente. Em 1890, já como tenente no exército francês disse que a cifra utilizada no exército podia ser decifrada sem precisar da chave. O General *Fay* enviou-lhe diversos criptogramas para *Bazeries* e todos foram decifrados. O Ministro da Guerra ordenou a criação de um novo sistema criptográfico mas antes mesmo deste sistema entrar em operação, *Bazeries* já tinha decifrado os criptogramas feitos

como teste. *Bazeries* foi transferido para o escritório de cifras (*Bureau du Chiffre*) do Ministério das relações exteriores. Bazeries decifrou os sistemas criptográficos de Francis I (rei da França de 1515 a 1547), Francis II (rei da França de 1559 a 1560), Henrique IV da França (rei de Navarra de 1572 a 1610), Mirabeau (1749-1791) e Napoleão Bonaparte (Imperador Francês de 1804 a 1815). As cifras utilizadas por Napoleão foram consideradas tão primárias por *Bazeries* que ele colocou a palavra "cifras" entre aspas no título da monografia que escreveu sobre o assunto. Quando a Primeira Guerra Mundial começou em 1914, *Bazeries* foi chamado e conseguiu decifrar muitos criptogramas militares alemães (TKOTZ, 2005, p. 264).

A máquina de cifragem Enigma usada pelos alemães antes e durante a Segunda Guerra Mundial segue todos os itens da "Lei de Kerckhoffs". O capítulo III desta dissertação de mestrado é dedicado às principais máquinas de cifragem da época e principalmente a máquina Enigma e sua evolução.

2.5 História recente da criptografia

A Primeira Guerra Mundial foi um conflito diferente de todos os anteriores devido à utilização de tecnologias como o gás de cloro, o gás mostarda, o gás fosgênio, rádio sem fio, telégrafo, código Morse, cabos submarinos interligando vários países e o uso da criptografia. Os alemães souberam utilizar a criptografia no campo de batalha mas os criptoanalistas Aliados conseguiram decifrar as mensagens alemãs e mudar o destino da Guerra.

2.5.1 Primeira Guerra Mundial

A Primeira Guerra Mundial (Grande Guerra ou Guerra das Guerras) teve início em 28 de julho de 1914 e durou até 11 de novembro de 1918. Basicamente os beligerantes organizaram-se em duas alianças opostas: os Aliados (com base na Tríplice Entente entre Grã-Bretanha, França e Império Russo) e os Impérios Centrais

(originalmente Tríplice Aliança entre Império Alemão, Império Austro-Húngaro e Itália) mas como a Áustria-Hungria era contra o acordo, a Itália não entrou em guerra e lutou pelos Aliados da Tríplice Entente.

O incidente que provocou a Primeira Guerra Mundial foi o assassinato do herdeiro do trono dos *Habsburgos*, o Arquiduque *Franz Ferdinand* e sua mulher, a Duquesa *Sophie*. As causas ocultas, no entanto, foram naturalmente, mais complexas e já existiam desde muito.

> Conforme escreveu *Sir Basil Liddell Hart*, “Foram gastos cinquenta anos no processo de tornar a Europa explosiva”. No dia 28 de junho de 1914, quando se deu o duplo assassinato, teve início uma crise que parecia apontar para um conflito militar. Foi uma provocação desnecessária o fato da realeza *Habsburgo* estar nesse dia em *Sarajevo*, capital da província austríaca *Bósnia-Herzegovina*, que fazia fronteira com a Sérvia independente. Era no dia 28 de junho que se comemorava a grande festa nacional de S. Vitos e também a batalha medieval de *Kosovo*. Esse mesmo dia era também o 14º aniversário de casamento do Arquiduque (HART apud SHERMER, 1975, p. 15).

Existe a explicação clássica sobre como começou a Primeira Guerra Mundial citando a assassinato do Arquiduque *Franz Ferdinand* mas as causas deste conflito não começaram no século XX.

Figura 50 – Europa antes da Primeira Guerra Mundial

Fonte: https://www.fatosdesconhecidos.com.br/wp-content/uploads/2017/04/0-49.jpg

A crise que resultou no início da Primeira Guerra Mundial ocorreu no âmbito de um sistema de relações internacionais cujas origens remontavam à Paz de Westfália (1648), ao final da Guerra dos Trinta Anos (1618-48). O grupo de países mais poderosos da Europa firmava ou rompia alianças de acordo com seus interesses. Em tempos de paz, esses países raramente se dividiam em campos armados hostis entre si. Antes de 1914, Grã-Bretanha, França e Rússia formaram a Tríplice Entente em resposta à Tríplice Aliança (1882) firmada entre Alemanha, Império Austro-Húngaro e Itália. A Tríplice Entente foi formada por três acordos separados: a convenção militar e Aliança Franco-Russa (1892-94), a Entente Cordiale Anglo-Francesa (1904) e a Entente Anglo-Russa (1907) sendo a motivação principal o temor pelo crescente poderio alemão. Uma das principais causas da Primeira Guerra Mundial foram o resultado de batalhas travadas antes de 1914 que levaram os países da Tríplice Entente e Tríplice Aliança a começarem uma guerra de grandes proporções. A Guerra Ítalo-Turca (1911-12) entre a Itália e o Império Otomano foi favorável aos Italianos. A Guerra dos Bálcãs (1912-13) foi um conflito

entre a Liga Balcânica (Bulgária, Sérvia, Montenegro e Grécia) e o Império Otomano. Os turcos dependiam da proteção britânica e francesa contra a Rússia mas o alinhamento destas potências na Tríplice Entente empurrou o Império Otomano na direção da Alemanha (SONDHAUS, 2013, p. 19).

Nos anos anteriores à guerra, a maior parte das grandes potências reduziu o tempo de serviço militar para imitar o modelo alemão de dois anos de serviço ativo, ao mesmo tempo em que seguiam o exemplo britânico de aumentar o contingente das formações de reserva. Devido ao aumento do número de alemães servindo na ativa por dois anos sem dispensa fez com que a França aumentasse de dois para três anos seu tempo de serviço militar. Assim como a corrida naval entre ingleses a alemães, essa competição franco-germânica para incrementar a capacidade dos dois exércitos serviu para exacerbar as tensões e contribuiu para a sensação de que a guerra era inevitável (SONDHAUS, 2013, p. 49).

A seguir vamos acompanhar alguns acontecimentos durante a Primeira Guerra Mundial em que o uso da criptografia influenciou algumas decisões no campo de batalha.

Em setembro de 1914, um cruzador ligeiro alemão, o *Magdeburg*, naufragou no mar Báltico. O corpo de um marinheiro alemão afogado foi recuperado pelos russos: grudados ao peito por braços rígidos pelo *rigor mortis*, estavam os livros de cifras e sinais da Marinha Alemã. A 6 de setembro, o adido militar russo procurou *Winston Churchill*, então Primeiro Lorde do Almirantado. O funcionário recebera uma mensagem de Petrogrado contando-lhe o que acontecera, e que o Almirantado russo, com a ajuda dos livros de cifras e sinais, conseguira decodificar partes de alguns códigos navais alemães. Os livros acabaram entregues a decodificadores britânicos na Sala 40 de *Whitehall*, onde foram usados para decodificar rotineiramente comunicações secretas alemãs. Quando os alemães vieram a escrever sua história da Primeira Guerra Mundial, registraram que "o comando da frota alemã, cujas mensagens de rádio foram interceptadas e decifradas pela Inglaterra, jogou por assim dizer com cartas à mostra contra o comando britânico" (CORNWELL, 2003, p. 248).

Verifique os principais acontecimentos da Primeira Guerra Mundial no anexo H deste trabalho.

2.5.2 Cifra ADFGVX

A cifra ADFGVX inclui ao mesmo tempo a substituição e a transposição. Ela foi criada pelo coronel *Fritz Nebel*, sendo usada pelo exército alemão para criptografar mensagens de seu alto comando no fim da Primeira Guerra Mundial. As mensagens cifradas com ADFGVX foram interceptadas pelos franceses, que contaram com o tenente *Georges Painvain*, especialista em criptoanálise militar, para desvendar a cifra. *Painvain* utilizou técnicas de análise de frequência estatística nas 17 mensagens interceptadas todos os dias, aproveitando-se do fato de que o início das mensagens seguia os rígidos protocolos militares do Exército alemão.

Painvain conseguiu, no início de junho de 1918, decifrar a primeira mensagem: um pedido urgente de munições para uma dada localização. Com esta informação, os franceses descobriram os planos dos alemães e conseguiram conter a investida militar. Embora a cifra ADVFGX tenha sido quebrada parcialmente, sua solução total só foi encontrada em 1933. A quebra da cifra ADFGVX foi mais um exemplo da necessidade de criação de novas cifras e de novos métodos de cifragem no início do século XX. Explica Singh:

> A quebra da ADFGVX foi um exemplo típico da criptografia durante a Primeira Guerra Mundial. Embora houvesse um fluxo de novas cifras, estas eram todas variações ou combinações das cifras do século XIX que já tinham sido quebradas. Embora algumas delas oferecessem uma segurança inicial, não demorava muito para que os criptoanalistas levassem a melhor sobre elas. O maior problema para os criptoanalistas era então o volume de tráfego (SINGH, 2011, p. 122).

A cifra ADVFGX foi bastante utilizada pelos alemães durante a Primeira Guerra Mundial mas o início das mensagens continham geralmente as mesmas

palavras e com a análise de frequência estatística do idioma alemão, a cifra era descoberta e uma parte da mensagem ou toda a mensagem era decifrada. A análise de frequência estatística foi discutida no capítulo I deste trabalho. Outro problema dos alemães era na metodologia na transmissão das mensagens. Os Aliados sabiam quantas mensagens criptografadas eram enviadas pelos alemães e o horário era exatamente o mesmo (TKOTZ, 2005, p. 147).

Em junho de 1918, a letra V foi adicionada à cifra, que ficou conhecida como “cifra ADFGVX”. Neste caso com a adição de mais uma letra, o quadrado de Políbio foi expandido para uma tabela de seis colunas por seis linhas que permitia o uso de 36 caracteres. A tabela abaixo mostra como ficaria um quadrado de Políbio com versão original da cifra e em vez de colocarmos os números de 1 a 5, usaremos as letras “ADFGX”.

TABELA 12 – Código ADFGX

	A	D	F	G	X
A	F	N	W	C	L
D	Y	R	H	I/J	V
F	T	A	O	U	D
G	S	G	B	M	Z
X	E	X	K	P	Q

Fonte: (COUTO, 2008)

A mensagem de texto claro: “ataque programado para amanhã” ficaria cifrada da seguinte forma. A primeira letra a ser cifrada é “A” que de acordo com a tabela 12 será “FD” (sempre na ordem coluna-linha).

TABELA 13 – A cifragem pela cifra ADFGX

Texto limpo	Cifragem correspondente
A	FD
T	FA
A	FD
Q	XX
U	FG
E	XA
P	XG
R	DD
O	FF
G	GD
R	DD
A	FD
M	GG
A	FD
D	FX
O	FF
P	XG
A	FD
R	DD
A	FD
A	FD
M	GG
A	FD

N	AD
H	DF
Ã	FD

Fonte: (COUTO, 2008)

Por extenso, a mensagem cifrada: “FD FA XX FG XA XG DD FF GD DD FD GG FD FX FF XG FD DD FD FD GG FD AD DF FD” (COUTO, 2008).

Durante a Primeira Guerra Mundial, os alemães começaram a atacar navios com seus submarinos mas em 1915, um submarino alemão afundou o navio de linha Lusitânia matando 1.198 passageiros incluindo 128 norte-americanos. O presidente dos Estados Unidos, *Woodrow Wilson* manteve a neutralidade na guerra. Se acontecesse outro incidente com cidadãos americanos, os alemães corriam o risco dos Estados Unidos entrarem na guerra ao lado dos aliados. *Arthur Zimmermann* (ministro do exterior do Império Alemão) criou um plano para atrasar ou impedir o envolvimento dos Estados Unidos na guerra. A ideia era propor uma aliança com o México para retomar os territórios do Texas, Novo México e Arizona e ainda fazer uma aliança com o Japão. *Zimmermann* redigiu a proposta e enviou por telégrafo para o embaixador alemão nos Estados Unidos. Este deveria reenviar o telegrama para o embaixador alemão no México e finalmente para o presidente mexicano.

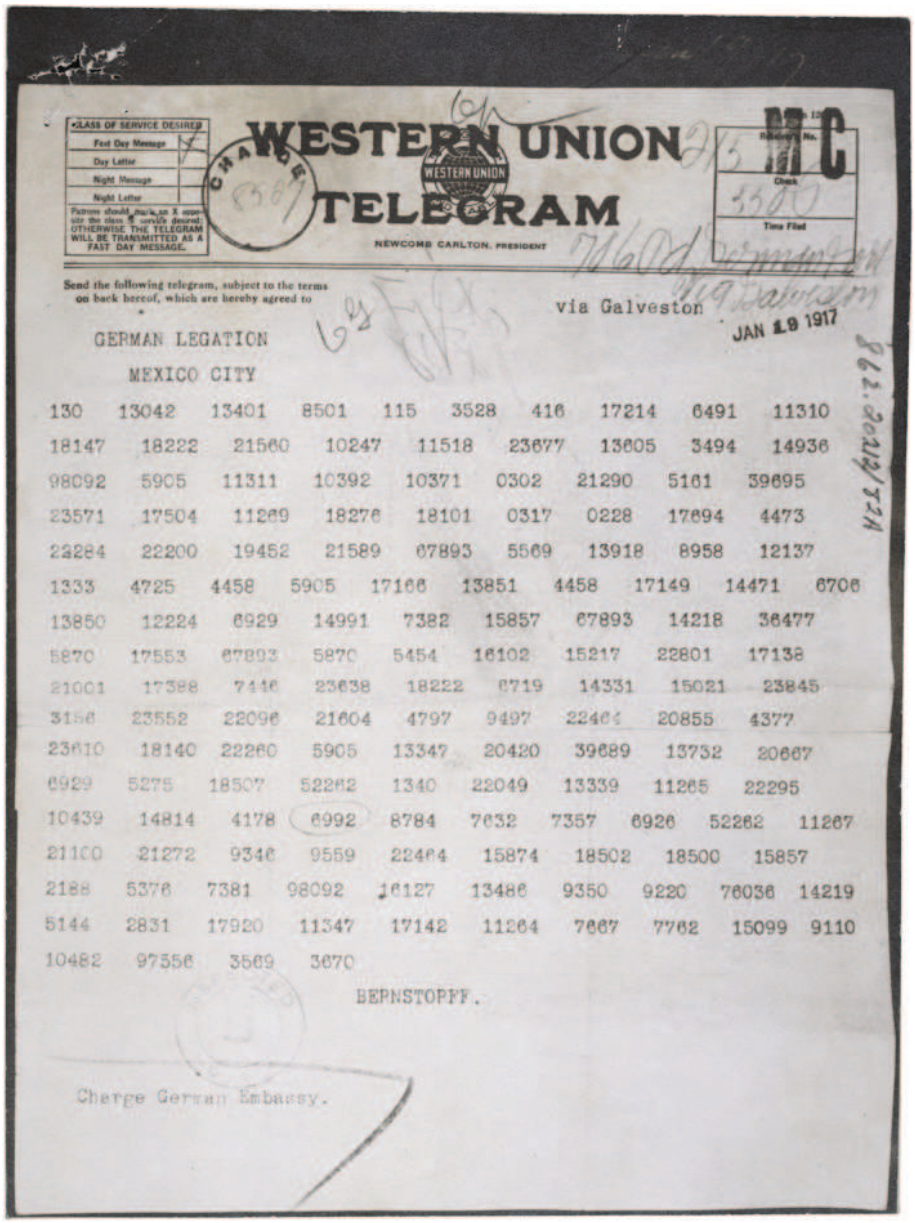
Os britânicos cortaram os cabos submarinos da Alemanha e estes foram obrigados a enviar a correspondência por meio de conexões inseguras por rádio ou utilizando cabos submarinos de outros países. *Zimmermann* codificou o texto e enviou em dois telegramas, um a partir da Suécia e o outro pelo cabo submarino norte-americano. Os ingleses interceptaram o telegrama e os criptoanalistas Reverendo *Montgomery* e *Nigel de Grey* do Serviço de Inteligência Britânico foram designados para decifrá-lo. Eles perceberam que se tratava de informação muito valiosa e que o tipo de codificação só era usado em comunicações diplomáticas de alto nível. Algumas partes do telegrama foi decifrada e entregaram ao diretor da inteligência Naval ao almirante *Sir William Hall*. Se o telegrama decifrado fosse tornado público os alemães concluiriam que seu método de codificação havia sido

“quebrado”. Por outro lado, se os ingleses não avisassem o presidente Wilson, os aliados perderiam uma oportunidade de colocar os Estados Unidos ao seu lado.

Em 1º de fevereiro de 1917, os alemães iniciaram a guerra naval irrestrita de acordo com as ordens do *Kaiser* Guilherme II. Mesmo assim o presidente Wilson anunciou ao Congresso que seu país permaneceria neutro atuando como pacificador. O almirante *Sir William Hall* viu-se obrigado a usar o telegrama *Zimmermann*. O embaixador alemão em Washington, havia retirado do telegrama as instruções que lhe cabiam e enviado o texto restante a *von Eckhardt*, embaixador alemão no México. *Eckhardt* entregou a versão alterada do telegrama em texto claro para o presidente mexicano. O almirante *Sir William Hall* entrou em contato com seu agente no México e solicitou a versão modificada. Assim que recebeu o telegrama, enviou para as autoridades americanas que apresentaram para o presidente Wilson. O serviço de inteligência norte-americano desconfiava de que pudesse ser uma artimanha dos ingleses para colocar os Estados Unidos na guerra. Em uma conferência de imprensa em Berlim, o próprio Zimmermann declarou que o plano era verdadeiro. Os Estados Unidos entraram na guerra no dia 02 de abril de 1917.

Os alemães começaram a investigar como o telegrama foi parar nas mãos dos americanos e detectaram que havia ocorrido uma traição no México. O almirante *Hall* publicou na imprensa inglesa culpando sua organização por não ter interceptado este telegrama importantíssimo. Em seguida a imprensa inglesa criticou a “ineficiência” do serviço secreto inglês e elogiaram o serviço secreto americano dando a entender que foram os americanos que interceptaram o telegrama *Zimmermann* (TKOTZ, 2005, p. 147).

Figura 51 – Telegrama *Zimmermann* cifrado



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

CLASS OF SERVICE DESIRED

Fast Day Message

Day Letter

Night Message

Night Letter

Patrons should check an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

Fonte: https://upload.wikimedia.org/wikipedia/commons/8/8d/Zimmermann_Telegram.jpeg

O texto a seguir mostra o Telegrama *Zimmermann* decifrado.

> Pretendemos iniciar a guerra submarina irrestrita no dia primeiro de fevereiro. Apesar disso devemos tentar manter a neutralidade dos Estados Unidos. No caso de não termos sucesso, faremos ao México uma proposta de aliança na seguinte base: faremos a guerra juntos e a paz juntos, apoio financeiro generoso e a compreensão, de nossa parte, de que o México deve reconquistar seus territórios perdidos no

> Texas, Novo México e Arizona. Os detalhes do acordo ficam por sua conta. Deve informar ao presidente do México do que se encontra resumido acima assim que o início da guerra contra os Estados Unidos esteja certo e acrescentar a sugestão de que ele deve, por sua própria iniciativa, convidar o Japão para se unir a nós e ao mesmo tempo servir como mediador entre nós e o Japão. Chame a atenção do presidente para o fato de que o emprego irrestrito de nossos submarinos agora oferece uma perspectiva de levar a Inglaterra a assinar a paz dentro de alguns meses. Acuse recebimento (Zimmermann apud SINGH, 2011, p. 128).

O telegrama enviado por *Zimmermann* foi codificado com o chamado Código 0075 que é composto de 10 mil palavras e frases numeradas de 0000 a 9999. O embaixador alemão no México, *von Eckhardt,* não possuía este código, o que obrigou o embaixador alemão em Washington a recodificar a mensagem com o antigo e simples código 13040. Este código havia sido distribuído para as missões alemãs nas Américas Central e Sul entre 1907 e 1909 e para Washington, Nova Iorque, Havana, Porto Príncipe e La Paz em 1912. Como *Hall* possuía as duas versões, a decodificação da primeira mensagem pode ser confirmada e completada com a ajuda da segunda mensagem.

De acordo com o Código 0075, podemos observar no telegrama *Zimmermann* alguns códigos da mensagem. 13605 para *Februar* (fevereiro), 13732 para *fest* (firme), 13850 para *finanzielle* (financeira), 17142 para *Frieden* (paz), 17214 para *ganz geheim* (totalmente em segredo), 67893 para México, 36477 para Texas e o conjunto 5454, 16102, 15217 e 22801, respectivamente, para AR, IZ, ON e A, o que permite escrever Arizona, palavra que não consta no código (TKOTZ, 2005, p. 150).

1.5.3 Cifra One Time Pad

No ano de 1917, o engenheiro estadounidense Gilbert S. Vernam recebeu a missão de investigar a segurança de transmissões por meio do telégrafo impressor. As mensagens podiam ser interceptadas se as flutuações de corrente fossem

gravadas por meio de um oscilógrafo. Mesmo quando as mensagens eram enviadas simultaneamente (multiplexação), ainda assim a segurança era precária.

Vernam sugeriu substituir o Código Morse pelo Código de Baudot. A motivação principal seria porque no Código Morse, os caracteres são representados por um número variável de sinais longos e curtos. No Código Baudot, os caracteres são substituídos por um número fixo de 5 unidades (ou pulsos). A unidade é um período de tempo-padrão, durante o qual existe corrente elétrica ou não. Quando há corrente, a unidade é chamada de marca e quando não há corrente, é chamada de espaço.

Vernam sugeriu que se perfurasse uma fita com os caracteres de uma chave e adicionar eletromecanicamente seus pulsos aos dos caracteres do texto claro. O resultado desta “soma” seria o texto cifrado. Vernam criou as seguintes regras: se os pulsos da chave e do texto claro fossem ambos marcas ou espaços, o pulso do texto cifrado seria espaço; se os pulsos da chave e do texto claro fossem diferentes, o pulso do texto cifrado, seria marca.

Tabela 14 – Cifragem de *Vernam*

Texto claro	Chave	Texto cifrado
Marca	Marca	Espaço
Marca	Espaço	Marca
Espaço	Marca	Marca
Espaço	Espaço	Espaço

Fonte: (TKOTZ, 2005).

Vernam não foi o primeiro a projetar um dispositivo de cifragem mecânica com impressão de mensagem. Por volta de 1870, os franceses Émile Vinay e Joseph Gaussin já tinham projetado uma máquina similar. Vernam acrescentou a cifragem no processo de comunicação. Este processo ficou conhecido como “cifragem on-line”.

O General estadounidense Joseph O. Mauborgne se interessou pelos dispositivos de “cifragem automática” mas nem questionou o procedimento relativo às chaves. O Código de Baudot já era de domínio público e montar uma tabela de cifrantes parecida com a de *Trithemius* ou *Vigenère* não apresentavam nenhuma dificuldade. O sistema foi aperfeiçoado e passou a usar fitas perfuradas com chaves totalmente randômicas de comprimento de mensagem que seria usada somente uma vez. Este sistema recebeu o nome “one-time” (uma única vez) e sua autoria se deve a Mauborgne e o projeto e construção das máquinas cifrantes se deve a Vernam. A Alemanha formalizou um sistema conhecido como “*one-time pad*” que pode ser traduzido como bloco de uso único. As folhas dos blocos continham sequências randômicas de dígitos que deveriam ser usados como chaves. Quando destinatário e rementente usassem a mesma folha, a mesma era descartada imediatamente (TKOTZ, 2005, p. 222).

2.6 O Tratado de Versalhes e o Período entre Guerras

Poucas épocas foram tão cheias de esperança de paz e de progresso para toda a humanidade como os meses que se seguiram ao fim da guerra. Com base nas concepções idealistas dos 14 pontos apresentados pelo presidente dos Estados Unidos *Woodrow Wilson*, e nos anseios de todos os que haviam sofrido, direta ou indiretamente, os quatro anos de guerra, esperava-se que a conferência de paz reunida em Versalhes em janeiro de 1919, pudesse encontrar uma fórmula capaz de impedir o retorno às disputas internacionais que haviam gerado o conflito, e levasse à criação de um organismo internacional capaz de resolver pacificamente as crises futuras (MAGALHÃES FILHO, 1986, p. 397).

O Tratado de Versalhes impôs uma série de ações punitivas à Alemanha como a ocupação da Renânia (importante centro industrial alemão) por tropas estrangeiras; a perda de território, como a obrigação de entregar as colônias alemãs aos países vencedores da Primeira Guerra Mundial (Grã-Bretanha, França); a proibição de forças armadas. Deveria também pagar 132 bilhões de marcos aos países aliados, os custos da Primeira Guerra Mundial. Esse montante correspondia

a 33 bilhões de dólares, o triplo da quantia sugerida pelos peritos economistas da Conferência de Versalhes.

Esse tratado significou uma paz imposta e não negociada pois nenhum alemão ou austríaco foi admitido às conferências enquanto os documentos não ficassem prontos para receber as assinaturas dos culpados. Diante da relutância dos vencidos em assinar o tratado, os aliados ameaçaram invadir a Alemanha caso o país não aceitasse o mesmo. Representantes do novo governo provisório republicano alemão (que sucedeu a monarquia) e dos aliados se reuniram no Palácio de Versalhes, na França, e o tratado foi assinado em junho de 1919.

Em consequência das disposições territoriais, a Alemanha foi despojada de dois quintos de carvão, de um sexto de suas terras aráveis e de dois terços de seu ferro. Foi forçada a entregar à Inglaterra, França e Bélgica os seus navios mercantes de algum valor, um oitavo de seu gado e grande quantidade de carvão, máquinas e materiais de construção. Teve que entregar todos os submarinos e a marinha de superfície. Foi proibida de ter aviação militar ou naval e o exército foi limitado a 100.000 homens a serem recrutados por alistamento voluntário (BURNS, 1966, p. 927).

A partir de 1922 o pagamento das reparações de guerra, a fuga de capitais para o exterior, e a impossibilidade de reconquistar os mercados externos perdidos, começaram a repercutir nas finanças alemãs. Através de um vórtice inflacionário, o escambo substituiu as operações com moeda e a vida econômica foi totalmente desorganizada. A crise financeira fortaleceu a extrema direita e seus pequenos partidos, levando a acontecimentos como o fracassado *Putsch* (golpe) da Cervejaria, em Munique, em novembro de 1923, chefiado por *Adolf Hitler* (MAGALHÃES FILHO, 1986, p. 400).

O Tratado de Versalhes desarmava virtualmente a Alemanha e, assim pelo menos durante algum tempo, constituía um obstáculo à hegemonia alemã na Europa. Não obstante, o Tratado de Versalhes, deixava a Alemanha, em grande parte, geograficamente e economicamente intacto, preservando sua unidade política e seu poderio latente como grande nação. O tratado restringia o exército a 100.000 voluntários a longo prazo, proibindo-lhe que possuísse aviões e tanques. O Estado-

Maior foi também proscrito. A Marinha foi reduzida a pouco mais do que uma força simbólica, sendo-lhe vedado construir submarinos ou barcos acima de 10.000 toneladas (SHIRER, 1967, p. 101, vol. 1).

> Quando, no ano de 1919, o tratado de paz foi imposto ao povo alemão, podia-se ter motivo de esperar que, justamente esse instrumento de opressão, deveria ter sido aproveitado para auxiliar o movimento da libertação da Alemanha. Tratados de paz cujas condições caem sobre os povos como chicotadas, não raras vezes são o primeiro toque para reunir para o ressurgimento nacional. Como era fácil a um governo enérgico fazer deste instrumento de extorsão um meio para exaltar ao máximo as paixões nacionais. Como era fácil, mediante uma inteligente propaganda das crueldades e do sadismo dos conquistadores, transformar a indiferença do povo em revolta, a revolta no ódio mais intenso (HITLER, 1983, p. 392).

Além do Tratado de Versalhes, que se aplicava à Alemanha, vários outros pactos foram redigidos para ajustar contas com os aliados dos alemães: a Áustria (Tratado de Saint Germain), a Hungria (Tratado de Trianon), a Bulgária (Tratado de Neuilly) e a Turquia (Tratados de Sévres e de Lausanne).

Ainda durante a Primeira Guerra Mundial, diversas transações clandestinas foram negociadas pelos governos da Entente, relativas à divisão dos despojos de guerra. Em abril de 1915 a Itália foi induzida a entrar na guerra ao lado dos Aliados pela promessa de lhe serem concedidos territórios austríacos e turcos. Vários outros tratados secretos foram feitos. O resultado foi que a distribuição dos territórios tomados às nações vencidas seguiu com precisão as linhas traçadas pelos acordos secretos. “Wilson permitiu até que o Japão se apoderasse das concessões alemãs na China, a despeito de terem os chineses feito a guerra ao lado dos Aliados”. (BURNS, 1966, p. 864).

De acordo com Mandel (1989), a contradição do Tratado de Versalhes foi que os vencedores quiseram enfraquecer o capitalismo alemão, sem desarmá-lo por completo. Com seu poder industrial, tornou inevitável sua reabilitação militar. A Alemanha, apesar da derrota na Primeira Guerra Mundial, não ficou eliminada da corrida pela liderança mundial.

2.6.1 Guerra Russo-Polonesa

O Estado Polonês foi recriado pelo Tratado de Versalhes o que levou a várias reconfigurações de fronteiras principalmente com a Alemanha que perdeu territórios para a Polônia.

A Guerra Russo-Polonesa foi um conflito armado entre a Polônia e a Rússia Comunista no período entre 1919 a 1921. O líder polonês Pilsudski resolveu se aproveitar das dificuldades da Rússia para lançar-se à restauração da Grande Polônia do século XVIII. Em 6 de maio de 1920, os poloneses ocuparam Kiev (capital da Ucrânia) permanecendo lá durante 5 semanas. Os poloneses foram expulsos de Kiev em 11 de junho de 1920 pelo exército vermelho da Rússia.

Os russos continuaram a avançar e entraram em território polonês com o objetivo de anexar a Polônia ao território russo. O exército vermelho russo chegou a 20 Km de Varsóvia (capital da Polônia) mas foram contra-atacados pelo exército polonês em 16 de agosto de 1920 fazendo milhares de prisioneiros. No dia 24 de agosto de 1920 os poloneses fizeram de 60.000 a 70.000 prisioneiros e estavam perto de expulsar os russos da Polônia.

Em Riga (capital da Letônia), a 12 de outubro de 1920, russos e poloneses assinaram um armistício e um tratado preliminar de paz. Durante o inverno, as condições econômicas da Polônia estavam desesperadoras e a 18 de março de 1921, foi confirmado o armistício pelo Tratado de Riga (WISKEMANN, 1974, p. 1072).

Figura 52 – Mapa da Polônia (em amarelo) em 1919

Fonte:https://upload.wikimedia.org/wikipedia/commons/thumb/d/d4/PBW_December_1919.png/1024px-PBW_December_1919.png

2.6.2 Decifradores de código poloneses

A Polônia se restabeleceu como Estado independente depois de 1918 mas preocupava-se com as ameaças pairando sobre sua nova soberania. A leste ficava a Rússia, uma nação ambiciosa, querendo espalhar seu comunismo. E a oeste ficava a Alemanha, preocupada em recuperar territórios cedidos à Polônia depois da Primeira Guerra Mundial via Tratado de Versalhes. Espremidos entre esses dois inimigos, os poloneses buscavam desesperadamente obter informações estratégicas e fundaram um novo departamento de cifras, o *Biuro Szyfrów*. Se a necessidade é a mãe da invenções, então a adversidade é a mãe da criptoanálise. O sucesso dos criptoanalistas poloneses de *Biuro Szyfrów* pode ser exemplificado pelo seu êxito durante a Guerra Russo-polonesa entre 1919 e 1921. Em Agosto de 1920, quando o exército russo se preparava para invadir Varsóvia, o *Biuro* decifrou 400 mensagens inimigas e através de informações das posições russas, o exército polonês conseguiu expulsar os russos de seu território (SINGH, 2014, p. 164).

A criptoanálise era uma tarefa tradicionalmente adequada a classicistas e linguistas. Em vista da complexidade mecânica da Enigma, o departamento de códigos polonês decidiu voltar-se para os matemáticos e entre seus primeiros recrutas, em 1929, estava Marian Rejewski, de 24 anos. Falando alemão, ele se matriculara em matemática em Gottingen, antes de passar para a universidade de Poznan, onde estudou estatística e criptologia. Descobriu sua verdadeira vocação ao tentar decifrar o código da máquina Enigma concentrando-se nos padrões da "chave da mensagem", repetida duas vezes no início de cada mensagem. Após um laborioso processo de verificação de cada uma das 105.456 "configurações de embaralhamento", que levou um ano, Rejewski finalmente começou a penetrar no mistério da cifra da Enigma (CORNWELL, 2003, p. 252).

Figura 53 – Marian Adam Rejewski

Fonte: http://www.cryptomuseum.com/people/img/rejewski.jpg

O encarregado de decifrar as mensagens alemãs era capitão *Maksymilian Ciezki*, um dedicado patriota que crescera na cidade de *Szamotuty*, centro do nacionalismo polonês. *Ciezki* tivera acesso à versão comercial da máquina Enigma, a qual lhe revelou todos os princípios de invenção de *Scherbius*. Infelizmente, o modelo comercial era bem diferente do militar no que se refere à fiação dentro de cada misturador. E sem conhecer a fiação da máquina militar, *Ciezki* não tinha

qualquer chance de decifrar as mensagens que eram enviadas pelo exército alemão. Ele ficou tão desesperado que, certa vez empregou uma vidente numa tentativa frenética de obter algum significado das mensagens interceptadas. Não é surpresa nenhuma que a vidente não tenha conseguido fazer a descoberta que o *Biuro Szyfrów* necessitava. Coube a um alemão descontente, *Hans-Thilo Schmidt*, dar o primeiro passo em direção à quebra da cifra Enigma.

Hans-Thilo Schmidt nasceu em Berlim, em 1888, filho de um professor e de sua esposa aristocrata. Ele entrou para o exército e lutou na Primeira Guerra Mundial, mas o exército alemão considerou que ele não tinha valor suficiente para permanecer em suas fileiras depois dos cortes exigidos pelo Tratado de Versalhes. *Schmidt* então tentou se tornar um homem de negócios, mas acabou obrigado a fechar sua fábrica de sabão devido à hiperinflação e à depressão do pós-guerra. Sua família mergulhou na pobreza. A humilhação dos fracassos de *Schmidt* era aumentada pelo sucesso de seu irmão mais velho. Rudolph que também lutara na Primeira Guerra Mundial, mas permanecera no exército depois dela. Durante a década de 1920 ele foi promovido e chegou a Chefe do Estado Maior do Corpo de Sinaleiros. Era o responsável em garantir comunicações seguras, e de fato foi *Rudolph* quem aprovou, oficialmente, o uso da máquina Enigma pelo exército alemão. *Rudolph* arranjou um emprego para *Schmidt* em Berlim, no *Chiffrierstelle*, escritório encarregado de administrar as comunicações cifradas da Alemanha. Era o centro de comando da Enigma, um estabelecimento altamente secreto que lidava com informações da mais alta importância (SINGH, 2014, p. 164).

Em 8 de novembro de 1931, *Hans-Thilo* encontrou-se com um agente francês, codinome *Rex*, na cidade belga de *Verviers*. Por uma alta soma de dinheiro, deixou que *Rex* fotografasse dois documentos: *Gebrauchsanweisung fur die Chiffriermaschine* Enigma (Manual de operação da máquina de cifragem Enigma) e *Schlusselanleitung fur die Chiffriermaschine* Enigma (Instruções de uso das chaves da máquina de cifragem Enigma). Apesar de não indicar precisamente a fiação de cada um dos rotores, as informações contidas nos documentos permitiam deduzir o conjunto de conexões. Graças à traição de *Hans-Thilo*, os aliados criaram uma réplica perfeita da mais temida máquina de cifragem da época. A força da Enigma não residia no mecanismo utilizado, mas sim na chave. A posição inicial dos rotores

e dos cabos do quadro de ligação, uma única combinação dentre as milhões de bilhões possíveis, era o segredo que precisava ser desvendado para que as mensagens interceptadas pudessem ser quebradas.

Os franceses, convencidos de que a cifra era indecifrável, nem se deram ao trabalho de construírem sua réplica. Como tinham um acordo de cooperação com os poloneses, estes se mostravam altamente interessados. *Rex* enviou as fotografias dos documentos da Enigma. Diferentemente dos outros serviços de inteligência, os criptólogos do *Biuro Szyfrów* perceberam que, conhecendo o modo de funcionamento da Enigma, havia uma possibilidade de quebrar a cifra (TKOTZ, 2005, p.252).

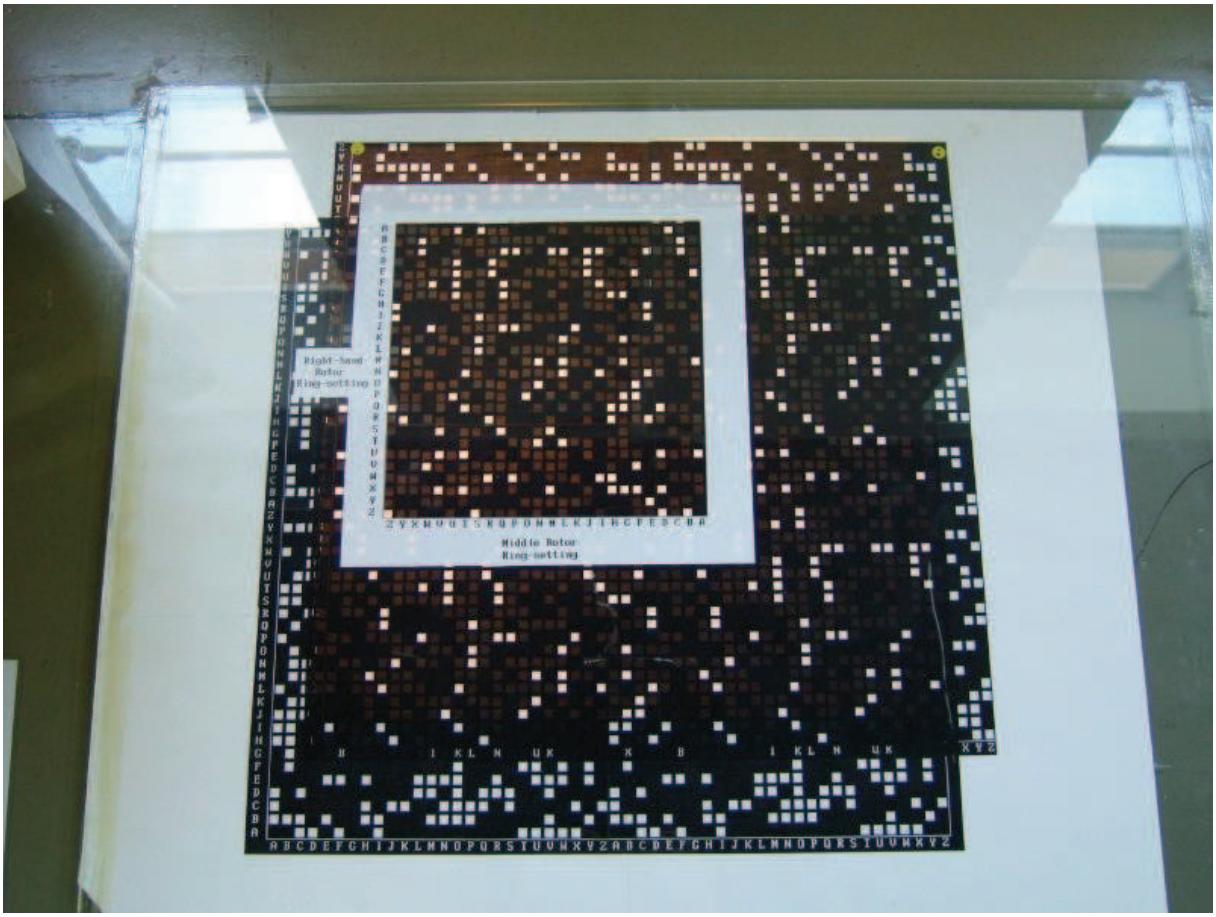
Figura 54 – *Henyk Zygalski*

Fonte: http://www.cryptomuseum.com/people/img/zygalski.jpg

Henryk Zygalski, colega de Rejewski, havia percebido que os indicadores (os grupos de seis letras que os operadores batiam duas vezes) tinham certas semelhanças. Os grupos tinham algumas letras continuamente em comum: a primeira e a quarta, a segunda e a quinta, a terceira e a sexta foram chamadas de “fêmeas”. Como não podiam ser produzidas pelos operadores alemães, cada uma representava uma configuração, e no todo, elas eram responsáveis por cerca de 40% do total que não podia ser usada e poderia por isso ser eliminada dos cálculos.

Eram feitos furos em cartões nos lugares onde deveria haver uma “fêmea”. Se, por acaso, uma série inteira de cartões fosse tratada dessa maneira, elas eram empilhadas em uma mesa de vidro iluminada por baixo. Quando um espaço aparecia através de toda a pilha, indicava a posição das rodas e a ordem das rodas para aquele dia. Elas, então eram testadas para confirmar. Essa prática eficiente mas trabalhosa e por isso muito lenta, e ficou muito demorada quando os alemães começaram a usar mais rotores (PATERSON, 2009, p. 45).

Figura 55 - Demonstração das folhas de Zygalski no museu de Bletchley Park



Fonte:https://upload.wikimedia.org/wikipedia/commons/6/67/Zygalski_sheets_%28perforated_sheets%29.jpg

Henryk Zygalski concebeu as "folhas perfuradas", de acordo com a figura 55, um dispositivo manual para encontrar as configurações de uma máquina de cifragem Enigma. Este procedimento, tal como o catálogo de cartões era independente do

número de conexões usadas no painel da máquina de cifragem Enigma.

Na figura 56, o personagem Peter (O jogo da imitação, 2014) está utilizando as “folhas perfuradas” de *Henryk* Zygalski. Como os poloneses não receberam os devidos créditos pela criação das “folhas perfuradas” tem-se a impressão que foi inventada pelos britânicos.

Figura 56 – Peter utilizando a folha de *Zygalski*

Fonte: O JOGO DA IMITAÇÃO. Direção: Morten Tyldum. Reino Unido/Estados Unidos: Paris Filmes, 2014. 1 DVD (114 min), NTSC, stereo, colorido. (17:14).

A figura 57 mostra o esboço fornecido por *Rejewski* em 1979. Como os alemães tinham uma máquina Enigma de três rotores diferentes naquele momento, haviam seis combinações de rotores possíveis para serem consideradas. Isso foi feito executando seis bombas em paralelo. Cada bomba tinha 6 conjuntos de rotor Enigma completos sendo 2 em sua parte superior, conectados em pares. Cada par foi usado para resolver uma (das três) “fêmeas”.

Embora a operação exata da bomba criptológica polonesa ainda seja desconhecida, muitos tentaram explicar seu princípio através da reconstrução de um modelo teórico e uma tentativa plausível foi feita por *David Link* (CRYPTO, 2016).

Na figura 30 é possível ver bomba criptológica inglesa que oferece um poder de processamento de dados maior do que a bomba criptológica polonesa. Na figura 28 *Alan Turing* faz referência à bomba criptológica polonesa.

Figura 57 – Bomba criptológica polonesa

Fonte: http://www.cryptomuseum.com/crypto/bombe/img/bomba_3_small.jpg

2.7 Segunda Guerra Mundial

Na Segunda Guerra Mundial foi utilizado as mesmas tecnologias usadas na Primeira Guerra Mundial como o rádio sem fio, telégrafo, código Morse, cabos submarinos interligando continentes (América e Europa), criptografia em larga escala. Com exceção dos gases tóxicos (cloro, mostarda, fosgênio) que foi proibido pela convenção de Genebra no período entre Guerras (1919-1938).

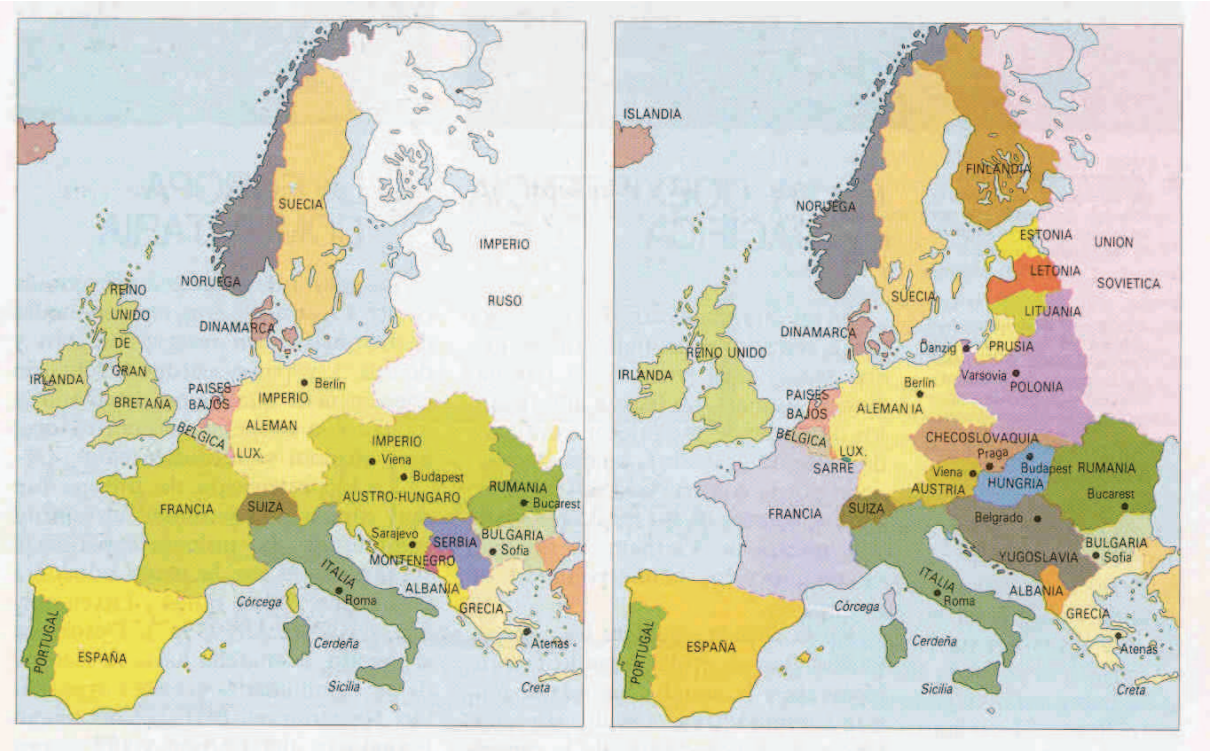
Adolf Hitler conseguiu desmantelar o Tratado de Versalhes, impôs uma política de rearmamento do *Reich*, remilitarizou a Renânia, anexou a Áustria ("*Anschluss*"), realizou anexação dos Sudetos e a decomposição da Tchecoeslováquia pelo Golpe de Praga em março de 1939. Ao longo deste período, a Europa parece fascinada, petrificada, incapaz de reagir. *Hitler* foi hábil em explorar

determinados fatores e tirar partido do estado de espírito e das opiniões dos dirigentes dos países europeus da época. Soube jogar com as ambiguidades e contradições da conferência sobre desarmamento, para reinvindicar e finalmente impor a igualdade de direitos para o restabelecimento de um *Reich* como potência militar e não se submeter a um estatuto discriminatório e permanente. A política alemã se beneficia também da omissão americana, embora Roosevelt não possa ser posto em causa. Ele toma consciência, de imediato, do enorme risco representado pelo nazismo mas nada pode fazer e opta pelo isolacionismo (MASSON, 2015, p. 14).

A Segunda Guerra Mundial teve início em 03 de setembro de 1939 e durou até 08 de maio de 1945. Basicamente os beligerantes organizaram-se em duas alianças opostas: os Aliados (Grã-Bretanha, França e União Soviética) e os países do Eixo (Alemanha, Itália e Japão). Posteriormente os Estados Unidos entraram na guerra ao lado dos Aliados.

Se desenvolveu um simulado ataque germânico à estação de rádio alemã em *Gleiwitz*, executado pelos homens da S.S. em uniformes poloneses sob o comando de *Naujocks*, que esse fato agora usado pelo Chanceler do *Reich* para justificar a sua cínica agressão contra a Polônia. Na verdade, logo nos seus primeiros comunicados o Alto Comando alemão empregava o termo “contra-ataque” ao referir-se às operações militares (SHIRER, 1967, vol. 2, p. 444).

Figura 58 – Europa antes e depois da Primeira Guerra Mundial



Fonte:http://jesussanpablo.files.wordpress.com/2011/03/europa_antes_y_despues_de_la_gran_guerra.jpg

Ao raiar do sol, no dia 1º de setembro de 1939, exatamente na data que *Adolf Hitler* fixara em 3 de Abril, os soldados alemães transpassaram a fronteira polonesa e convergiram para Varsóvia (capital da Polônia) pelo Norte, sul e oeste**.**

No céu, aviões de guerra rugiam em busca de seus objetivos. Visavam colunas do exército polonês, depósitos de munições, pontes, estradas de ferro e até cidades desprotegidas. Dentro de poucos minutos, os soldados e os civis poloneses sentiram na carne a primeira demonstração do que seria esta guerra, em que a força aérea distribuía a morte e a destruição em escala nunca dantes vista no mundo. Iniciou-se assim um terror que se tornaria habitual para centenas de milhares de homens, mulheres e crianças na Europa e na Ásia durante os seis próximos anos, e cujo espectro, após o advento da bomba atômica, iria assombrar a humanidade inteira com a ameaça de extermínio total. Grã-Bretanha e França declararam guerra à Alemanha no dia 03 de setembro de 1939 (SHIRER, 1967, vol. 2, p. 442).

A Segunda Guerra Mundial foi retratada no filme: “O jogo da imitação, 2014” (Capítulo I) onde mostra as principais batalhas ocorridas durante o conflito ao mesmo tempo em que a decifragem de alguns códigos secretos da máquina de cifragem Enigma favoreceu os Aliados em maior ou menor grau.

Verifique no anexo I os principais acontecimentos da Segunda Guerra Mundial. A seguir vamos acompanhar a guerra dos decifradores de código do Eixo e dos Aliados.

2.7.1 Decifradores de código alemães

As ambições de *Hitler*, de uma rápida guerra de agressão, e o inerente desperdício e sobreposição de rivalidades policráticas no *Reich*, iam expor muitas áreas de negligência na defesa, incluindo a inteligência de sinais. Ao contrário da extraordinária centralização da decifração de código em *Bletchley Park*, na Grã-Bretanha. Havia nada menos que sete organizações de decifração de códigos no *Reich* de *Hitler*. Entre estas estavam o Ministério do Exterior, a marinha, o exército, a *Luftwaffe* e vários departamentos de segurança. Ao todo eram cerca de 6 mil pessoas trabalhando em criptoanálise, mas espalhadas por essas diferentes organizações. Muitas vezes elas não sabiam do trabalho de seus “rivais”, e portanto não tinham ideia da sobreposição e duplicação. Em 1942, sugeriu-se a *Hitler* que se pusessem os criptoanalistas sob uma única organização, controlada pelo especialista húngaro Major *Bibo*; mas ele se recusou a sancionar a medida. A mais eficiente dessas organizações era o *B-Dienst* (*Beobachtungs-Dienst*), ou Serviço de Observação, uma unidade naval de criptoanalistas sob o controle último do Almirante *Donitz*. O *B-Dienst* na verdade dividia-se em três partes diferentes, um serviço de escuta, uma operação de decodificação e um serviço de avaliação. Mesmo antes de começar a Segunda Guerra Mundial, o *B-Dienst* decifrou o Código Administrativo da Marinha Real Britânica, ou o Código Naval, usado por recrutas marinheiros. Isso ajudou o *B-Dienst* a decifrar a Cifra Naval usada por oficiais britânicos para comunicações secretas. Esses sistemas navais, que não eram mecânicos, envolviam um livro de código com acréscimos que os alemães

reconstruíram com pouca dificuldade. Na última parte de 1940, o *B-Dienst* estava decifrando metade de todos os sinais da Marinha Real Britânica (CORNWELL, 2003, p. 253)

Enquanto a Inglaterra conservou suas organizações de segurança do período anterior à guerra e da época da guerra e continuou a desenvolvê-las de forma que em 1939 tinha montado o maior sistema de inteligência do mundo, a Alemanha teve que recomeçar do zero. Vários exércitos privados foram criados, conhecidos como *Freikorps*, para preservar a ordem no início da República de Weimar e também para evitar uma revolução comunista. A maioria eram ex-soldados alemães da Primeira Guerra Mundial e muitos se juntaram depois à SA (*Sturmabteilung*) de Hitler. Uma unidade de inteligência foi montada no interior de um desses *Freikorps* de Berlim para monitorar e analisar a ameaça comunista. Foi criado um Gabinete de Pesquisa (*Forschungsamt*) que era responsável pelas escutas telefônicas e outras pesquisas eletrônicas. *Gottfried Schapper* que durante a Primeira Guerra Mundial havia comandado a estação de rádio do quartel-general do Exército, levou seus conhecimentos de criptógrafo e sua especialização em comunicações militares para o recém criado Gabinete de Pesquisa. O *Forschungsamt* ficou ligado à *Luftwaffe* (Força Aérea Alemã).

A organização era composta por seis departamentos. Aqueles especializados em relações exteriores processavam uma grande quantidade de informações provenientes de relatórios de agentes, jornais estrangeiros e transmissões feitas por comunicações sem fio, transmissões de rádio “originais” e codificadas, que chegavam a mais de duas mil por mês quando irrompeu a guerra. O departamento Bureau IV tratava as comunicações codificadas. Este departamento se concentrou na decodificação das mensagens diplomáticas e 70% dos códigos usados pelos países vizinhos foram decodificados usando escutas nos telefones de embaixadas, diplomatas e jornalistas estrangeiros. A posição central da Alemanha na Europa facilitava a interceptação de mensagens devido a passagem de linhas de comunicação internacionais que passavam pelo país. Na crise da Tchecoeslováquia em 1938, Hitler teve um conhecimento precioso sobre os limites do apoio da França e da Inglaterra pelas mensagens interceptadas. Em 1939 foi a vez da Polônia ficar vulnerável com as exigências alemãs e apesar de uma postura mais inflexível da

França e Inglaterra, *Hitler* arriscou a invasão dando início à Segunda Guerra Mundial.

Havia também a organização governamental encarregada do serviço de espionagem e inteligência, o Serviço de Segurança do Reich (SSR), e a *Abwehr*, serviço secreto militar chefiado pelo almirante *Wilhelm Canaris*. No começo da guerra estes departamentos eram muito eficientes mas padeciam de inveja e desconfiança mútuas que impediam qualquer partilha de conhecimento e esforços coordenados. Nessas condições, apesar de haver alguns sucessos, os esforços da Alemanha estavam condenados desde o início.

O legendário decodificador austríaco *Andreas Figl* estava preso na Áustria. Com a anexação da Áustria ao III Reich alemão em 12 de março de 1938, *Hitler* o levou para Berlim e o designou para o *Schutztaffel* (SS) como instrutor de criptografia (PATERSON, 2009, p. 34).

A partir de 1942-1943 é que a *Wermacht* perde a batalha dos códigos importantes tanto no mar quanto em terra. Mesmo assim, os alemães ainda conseguiram decifrar códigos menores de ordem tática principalmente do exército britânico. Na Itália e na Normandia, os alemães conseguem importantes informações do plano operacional dos Aliados devido a negligências e diversas fontes de informação. A decifragem das mensagens da Polícia Militar americana permitiu aos alemães conhecer a ordem de batalha americana. Os alemães foram eficazes na análise de comunicações radioelétricas utilizando o aparelho *Funkabewehr*. O deslocamento da 82º divisão aerotransportada americana foi detectada às vésperas do desembarque da Normandia (MASSON, 2015, p. 273).

2.7.2 Decifradores de código estadounidenses

A equipe de criptoanalistas liderados por N. Friedman, do *Signal Intelligence Service* do exército americano consegue fabricar em 1940 uma réplica de máquina de codificar utilizada pelos diplomatas japoneses e com isso o governo americano tomou conhecimento das mensagens japonesas que utilizavam o código Violet.

Assim foi possível seguir a evolução das relações entre os governos Japonês e Soviético. Foi possível monitorar as mensagens endereçadas ao Japão pelo embaixador Oshima a serviço em Berlim. A ruptura do código Violet não provocou reviravolta da Guerra do Pacífico e mesmo com o ataque japonês a *Pearl Harbor* (7 de dezembro de 1941), os americanos ainda eram incapazes de decifrar os códigos da marinha e exército japonês.

O serviço de informações da marinha americana, o OP-20-G, ou a Fleet Radio Unit não conseguiram decifrar o código da marinha japonesa reservado às comunicações estratégicas mas em compensação a partir de março de 1942, o código JN-25 foi decifrado em uma proporção de 60% após a Batalha do Mar de Coral (4 a 8 de Maio de 1942). Os americanos conseguem na véspera da Batalha de Midway (4 a 7 de Junho de 1942) decifrar o código secreto japonês e com isso ganhar a batalha mesmo com menos navios e aviões. Os japoneses perceberam suas falhas e com a ajuda dos alemães, começaram a utilizar máquinas de cifragem Enigma (MASSON, 2015, p. 268).

Cartier (1977, p. 326) nos dá mais detalhes sobre a véspera da Batalha de Midway. “A última dúvida era a significação de um certo grupo “A.F.” que designa o objetivo dos imensos preparativos em andamento. O comandante Rochefort recorreu a um estratagema. Ordenou que fosse enviada de Midway uma mensagem clara, dizendo que o aparelho de destilação de água do mar estava avariado. No dia seguinte, o boletim de informações japonês assinalou que A.F. estava sem água doce”.

Como os estadounidenses sabiam que os japoneses iriam iniciar um grande ataque mas não sabiam onde, o estrategema do comandante Rochefort deu certo e os japoneses perderam o fator surpresa no episódio conhecido como a Batalha de Midway.

A seguir vamos analisar como a *Abwehr* (Serviço Secreto Militar Alemão) conseguiu importantes vitórias para os alemães no campo da decifragem de mensagens secretas dos Aliados. A *Abwehr* utilizava sua própria versão da máquina de cifragem Enigma G ou *Zählwerk* Enigma G31 ou *Abwehr* Enigma. Veja maiores detalhes deste modelo no item 3.2.9.1 do capítulo III.

2.7.3 *Abwehr* (Serviço Secreto Militar Alemão)

Figura 59 – Almirante *Wilhelm Canaris* chefe da *Abwehr* (Serviço Secreto Militar)

Fonte: https://upload.wikimedia.org/wikipedia/commons/c/c5/Bundesarchiv_Bild_146-1979-013-43%2C_Wilhelm_Canaris.jpg

O Almirante *Wilhelm Canaris* assumiu a chefia da *Abwehr* (Serviço Secreto Militar) em janeiro de 1935 e em seu escritório diz para seus subordinados:

> "Senhores, a Abwehr é um simples serviço do grande estado-maior. Tentaremos fazer um Serviço de Informações completo: contra-espionagem, segurança e espionagem, para que a Abwehr se torne realmente uma "Casa". Retomaremos a divisa do meu lendário predecessor, o Coronel Nicolai: "O serviço de informações é o apanágio dos nobres" (BRISSAUD apud CANARIS, 1978, p. 42).

A partir de 1935, a *Abwehr* ia expandir sua infraestrutura para tornar-se um verdadeiro Serviço Secreto, similar ao *Intelligence Service* britânico. Em 1938, *Adolf Hitler* substituiu o Ministério da Guerra por um Comando Supremo do Exército alemão, estado-maior militar do *Führer* (*Oberkommando der Wehrmacht*), abreviadamente OKW, dirigido pelo General *Keitel*. A *Abwehr* tornou-se *Amtsgruppe Auslandnachrichten und Abwehr* (abreviadamente: "A. Ausl. Abw."). Em outubro de 1939 o Serviço Secreto recebeu a denominação oficial: *Amt Ausland/Abwehr des* O.K.W. Em 1941 foi criado um Departamento Exterior (*Amtsgruppe "Ausland"*). Canaris era auxiliado pelo Tenente-Coronel *Willy Jenke*, que dirigia seu estado-maior (*Dem Amtchel*), compreendedo cinco departamentos: o Escritório Central de contra-espionagem (*Abwehrstellenleiter*), a Direção da organização de guerra (*Kriegsorganisation-Leiter ou KO-Leiter*), o comando de contra-espionagem no *front* (*Frontabwehrstellenkommandeure*), a direção dos oficiais de ligação (*Verbindungsoffiziere*) e o Comando das ligações extraordinárias para designações especiais 800 que se tornou, Comando da Divisão "*Brandenburg*" (*Kommandeur des Sonderver-bandes* z.b. V.800). A "casa Canaris" estava instalada no cais *Tirpitz*.

A Seção para o Exterior que mais tarde se tornou um departamento (*Abteilung*, depois *Amtsgruppe* "*Ausland*"), era encarregada da ligação entre a OKW e o ministério das Relações Exteriores (*Wilhelmstrasse*) de *Joachim von Ribbentrop* (ministro das Relações Exteriores da Alemanha). Era o organismo central, encarregado dos adidos militares de terra, mar e ar no exterior e era responsável pelos adidos militares estrangeiros na Alemanha.

A Seção Central (*Abwherabteilung Z*: *Zentralabteilung*) era responsável por todos os assuntos administrativos, financeiros e jurídicos, próprios da *Abwehr*, assim como designações e transferências do conjunto de seu pessoal.

A Seção I (*Abwehrabteilung* I "*Geheimer Meldedienst*") era responsável essencialmente pela espionagem. Recebia de suas agências no exterior (*Abwehrstelle*), relatórios dos "homens de confiança" (V. *Mann*: *Vertrauensmann der Abwehr*) contendo informações importantes sobre Exércitos, armamentos e a indústria de guerra dos países estrangeiros que eram repassados para a OKW.

A Seção II era responsável pelo serviço de sabotagem e trabalhava na retaguarda do inimigo em tempo de guerra.

A Seção III (*Abwehrabteilung* III "*Spionageabwehr*" era responsável pela contra-espionagem e segurança. A missão era descobrir espiões inimigos e criar medidas de segurança nos organismos garantindo a defesa do território alemão e também dos territórios ocupados pelo Exército alemão (BRISSAUD, 1978, p. 42, p. 491).

Segundo Masson (2015, p. 483) "os criptoanalistas da *Abwehr* obtiveram algumas vitórias no campo de batalha da informação quando conseguiram decifrar o código do ministério da Guerra Francês e de suas regiões militares antes da Batalha da França. *Abwehr* conseguiu decifrar também o código diplomático dos Estados Unidos entre 1942 a setembro de 1944".

Finalizando este capítulo, mostramos o surgimento e evolução da criptografia e a sua aplicação nos conflitos históricos com destaque para a Segunda Guerra Mundial.

No Egito foi possível identificar o surgimento das primeiras técnicas para ocultação de mensagens, a pelo menos 20 séculos antes de Cristo. De lá para cá os métodos de codificação e decodificação de diversificaram e se complexificaram.

A criptografia tem o auxílio da criptoanálise até então consideradas uma arte. Nos últimos 20 anos a criptologia (criptografia + criptoanálise) vem ganhando maior importância. A criação da Associação Internacional para a Pesquisa Criptológica, organização científica internacional que coordena a pesquisa na área considera a Criptologia como ciência e não apenas como arte (TKOTZ, 2005, p. 16).

Após o surgimento da criptografia, destacamos as cifras clássicas e a criptografia moderna, para chegar à história recente da criptografia, parte mais substantiva deste capítulo.

Analisamos a Primeira Guerra Mundial, com os métodos de decodificação, o Tratado de Versalhes e o período entre guerras, com ênfase na guerra Russo-Polonesa e os decifradores de código poloneses. O destaque do capítulo foi a Segunda Guerra Mundial e os decifradores de código alemães.

Explicamos como a Grã-Bretanha, vitoriosa na Primeira Guerra Mundial conservou suas organizações de segurança e continuou a desenvolvê-las, enquanto

a Alemanha derrotada, teve que recomeçar. Foram criados vários exércitos privados, os *Freikorps* para preservar a ordem no início da República de *Weimar* e também para evitar uma revolução comunista. Um Gabinete de Pesquisa foi criado no interior de um desses *Freikorps* de Berlim, na realidade uma unidade de inteligência para monitorar a ameaça comunista. A esse respeito, a título de ilustração, seria interessante ver o filme “Rosa Luxemburgo”, de *Margarette von Trotta*, de 1986, uma cinebiografia de militante e pensadora marxista que foi assassinada por militares alemães, após tentativa de insurreição socialista, fracassada em novembro de 1918.

A expansão das unidades de inteligência e a posição central da Alemanha na Europa facilitaram a interceptação de mensagens, já que muitas linhas de comunicação internacionais passavam pelo país.

De 1935 em diante a Alemanha expandiu sua infraestrutura para tornar-se um verdadeiro Serviço Secreto, similar ao britânico *Intelligence Service*.

Uma guerra é um fenômeno complexo, com muitas variáveis que se interpenetram. E no confronto das duas maiores potências mundiais de então (Alemanha e Grã-Bretanha) com seus respectivos aliados, os serviços de inteligência foram colocados à prova e, no limite, a Alemanha saiu derrotada mais uma vez.

No próximo capítulo vamos esmiuçar o desenvolvimento das máquinas de cifragem antes e durante a Segunda Guerra Mundial com ênfase para a máquina de cifragem Enigma alemã.

CAPÍTULO III. Desenvolvimento das máquinas de cifragem na Segunda Guerra Mundial

> La clave de todo el sistema de comunicación secreto alemán era un artefacto parecido a una máquina de escribir dentro de una caja de madera. Bajo su inofensivo aspecto se ocultaba un sofisticado ingenio que tenía como misión enviar mesajes mediante un mecanismo que los convertia en indescifrables para el inimigo (HERNÁNDEZ, 2016, p. 29).

Neste capítulo objetivamos analisar a partir de uma revisão bibliográfica, o desenvolvimento das máquinas de cifragem e os esforços internacionais liderados pela Inglaterra, para decodificar o complexo sistema de inteligência nazista. Detalhes técnicos foram necessários para melhor compreensão do assunto.

3.1 Apresentação

A história dos esforços da sofisticada codificação alemã na Segunda Guerra Mundial começa em 1923, quando *Winston Churchill* publicou sua história da Grande Guerra, *The World Crisis*, contando que em setembro de 1914 os britânicos conseguiram a posse dos códigos navais secretos da Alemanha. Muitos alemães ignoravam certos fatos relatados na obra de Churchill após cinco anos do fim da Primeira Guerra Mundial. O livro certamente afetou as decisões dos militares alemães sobre códigos secretos nas décadas de 1920 e 1930.

Após a revelação de *Churchill* em 1923, as autoridades militares alemãs voltaram-se para a invenção de um “rotor de cifra”, uma máquina de escrever que trabalhava com base num sistema de “substituição” mecânica. O aparelho padrão, que parecia uma máquina de escrever de cerca de 30,5 centímetros quadrados, 15,2 centímetros de altura e pesando 3,6 quilos fora desenvolvido por um engenheiro elétrico alemão, *Arthur Scherbius*, para uso no comércio, na diplomacia e potencialmente para usos militares. Deu-lhe o nome de Enigma, palavra grega. Descrevendo a máquina para a Marinha Imperial Alemã em 1918, *Scherbius*, então

com trinta e nove anos e vivendo em Berlim, gabara-se de que ela “evitaria qualquer repetição da sequência de letras ainda que a mesma letra fosse batida milhões de vezes”. A solução de um telegrama seria também impossível se uma máquina cair em mãos não autorizadas, pois exige um sistema de chaves pré-combinado.

A criação de uma cifra com uma máquina de rotor do tipo que evolui para a Enigma envolve bater as teclas de uma máquina de escrever correspondentes às letras da mensagem, ou o “texto simples”, e anotar o “texto cifrado”, as sucessivas letras que se acendem numa tela de vidro (CORNWELL, 2003, p. 248).

3.2 Máquina de cifragem Enigma

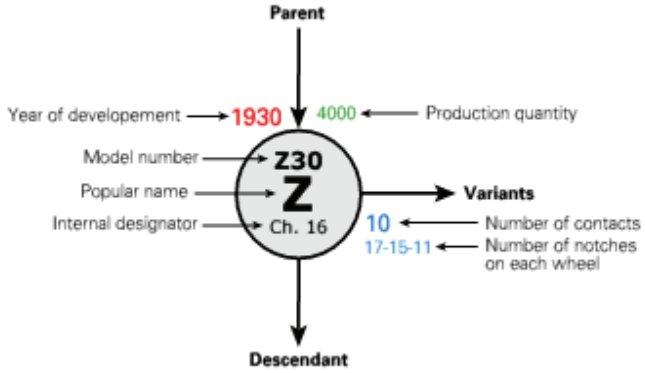
> Quando cada letra é cifrada, a corrente elétrica passa pelo contato da placa de entrada dessa letra, entra no rotor no contato oposto a este, gira pelo rotor, sai numa posição diferente na outra face, passa para a placa de saída e vai para a lâmpada embaixo da letra de texto cifrado (CORNWELL apud KAHN, 2003, p. 250).

Foram desenvolvidas e fabricadas mais de 50 modelos da máquina Enigma. Segundo Tkotz (2005, p. 247), foram fabricadas entre 100 e 200 mil máquinas desse tipo.

Figura 60 – Enigma logo

Fonte: http://cryptomuseum.com/crypto/enigma/index.htm

Figura 61 – Legenda da Árvore Enigma



Fonte: http://cryptomuseum.com/crypto/enigma/tree.htm

De acordo com a figura 61 temos as seguintes informações:

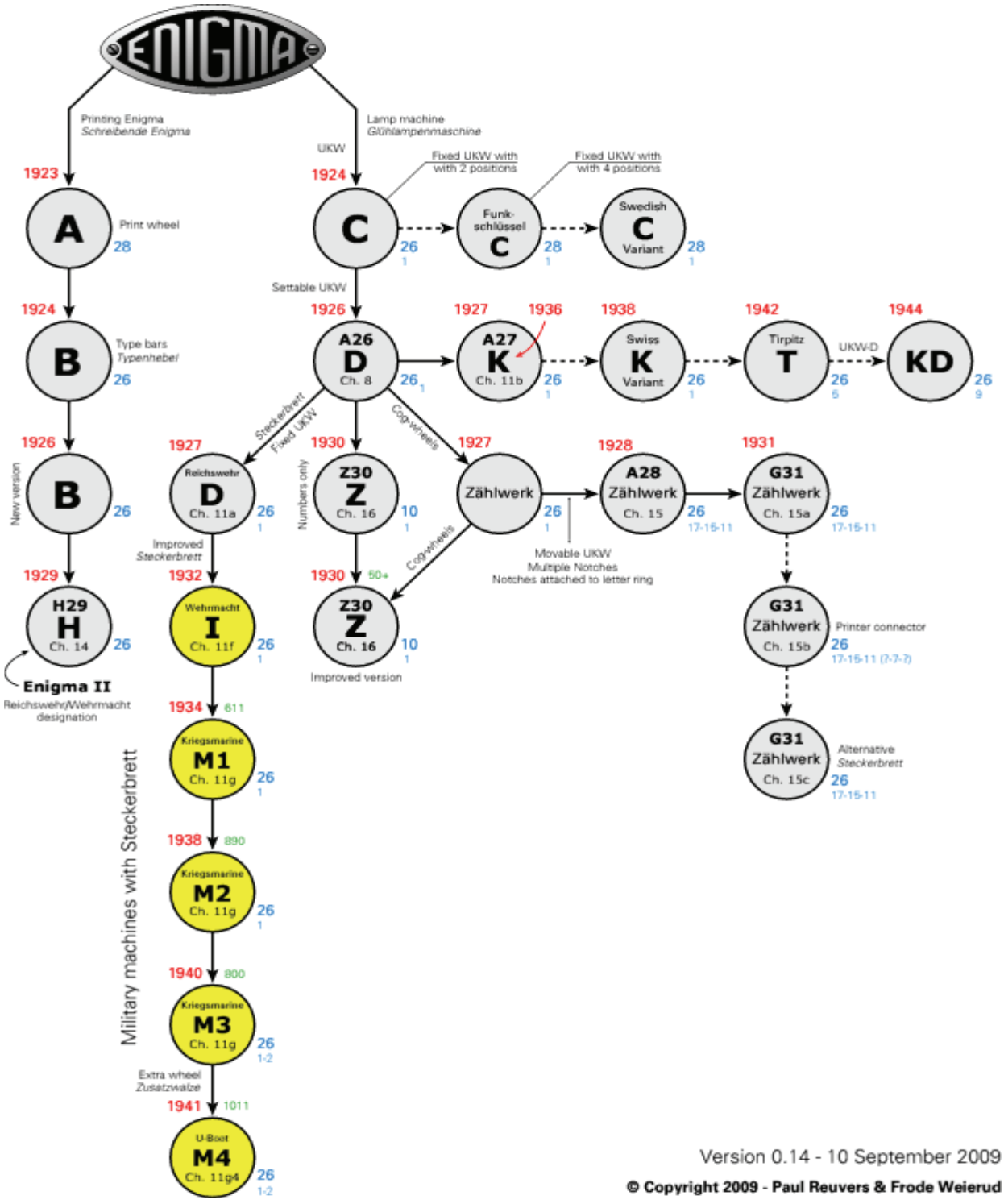
Tabela 15 – Tradução da legenda da Árvore Enigma

Itens da legenda em inglês	Tradução dos itens da legenda	Observações
Parent	Origem	O modelo Z descende que qual modelo da máquina Enigma?
Year of developement	Ano de desenvolvimento	1930
Model number	Número do modelo	Z30
Popular name	Nome popular	Z
Internal designator	Designador interno	Ch. 16
Descendant	Descendente	Modelo Z deu origem a outro modelo de máquina Enigma
Production quantity	Quantidade produzida	4000
Variants	Variantes	Variações do modelo Z
Number of contacts	Número de contatos	10
Number of notches on each wheel	Número de entalhes em cada rotor	17-15-11

Fonte: Elaborada pelo autor

A árvore de derivações de máquinas Enigma (figura 62) é um resumo dos principais modelos e suas características. A árvore da máquina Enigma foi desenvolvida por *Paul Reuvers* e *Frode Weierud*.

Figura 62 – Árvore da máquina de cifragem Enigma



Fonte: http://cryptomuseum.com/crypto/enigma/tree.htm

A tabela 16 ensina a usar a árvore da máquina enigma citada na figura 62.

TABELA 16 - Explicação da família da Máquina Enigma.

Parent (Origem)	*Year of developement* (Ano de desenvolvimento)	*Model number* (Número do modelo)	*Popular name* *(Nome popular)*	*Internal designator* (Designador interno)	*Descendant* (Descendente)	*Production quantity* (Quantidade Produzida)	*Variants* (Variações)	*Number of contacts* (Número de contatos)	*Number of notches on each wheel* (Número de entalhes em cada roda)
Enigma comercial	1923	-	A	-	B	-	-	28	-
A	1924	-	B	-	B (nova versão)	-	-	26	-
B	1926	-	B (nova versão)	-	H	-	-	26	-
B (nova versão)	1929	H29	H	Ch. 14 Enigma II (Reichswehr/Wermacht)	-	-	-	26	-
Enigma comercial	1924	-	C	-	-	-	-	26	1
-	1924	Funk-schlüssel	C	-			C	28	1
-	1924	Swedish	C	-	-	-	C Funk-schlüssel	28	1
C	1926	A26	D	Ch. 8	-	-	-	26	1

-	1927-1936	A27	K	Ch. 11b			D	26	1
-	1938	Swiss	K	-	-	-	K	26	1
-	1942	Tirpitz	T	-	-	-	K Swiss	26	5
-	1944	-	KD	-	-	-	Tirptiz	26	9
D	1927	Reichwehr	D	Ch. 11a	-	-	-	26	1
D Reichwehr	1932	Wermacht	I	Ch. 11f	-	-	-	26	1
I Wermatch	1934	Kriegsmarine	M1	Ch. 11g	-	611	-	26	1
M1	1938	Kriegsmarine	M2	Ch. 11g	-	890	-	26	1
M2	1940	Kriegsmarine	M3	Ch. 11g	-	800	-	26	1-2
M3	1941	U-Boat	M4	Ch. 11g4	-	1011	-	26	1-2
D A26	1930	Z30	Z	Ch. 16	-	-	-	10	1
Z30 Zählwerk	1930	Z30	Z	Ch. 16 Versão melhorada	-	50	-	10	1
D A26	1927	-	Zählwerk	-	-	-	-	26	1
-	1928	A28	Zählwerk	Ch. 15	-	-	Zählwerk	26	17-15-11
-	1931	G31	Zählwerk	Ch. 15a	-	-	Zählwerk A28	26	17-15-11
-	1931	G31	Zählwerk	Ch. 15b	-	-	Zählwerk G31	26	17-15-11
-	1931	G31	Zählwerk	Ch. 15c	-	-	Zählwerk G31	26	17-15-11

Fonte: Elaborada pelo autor.

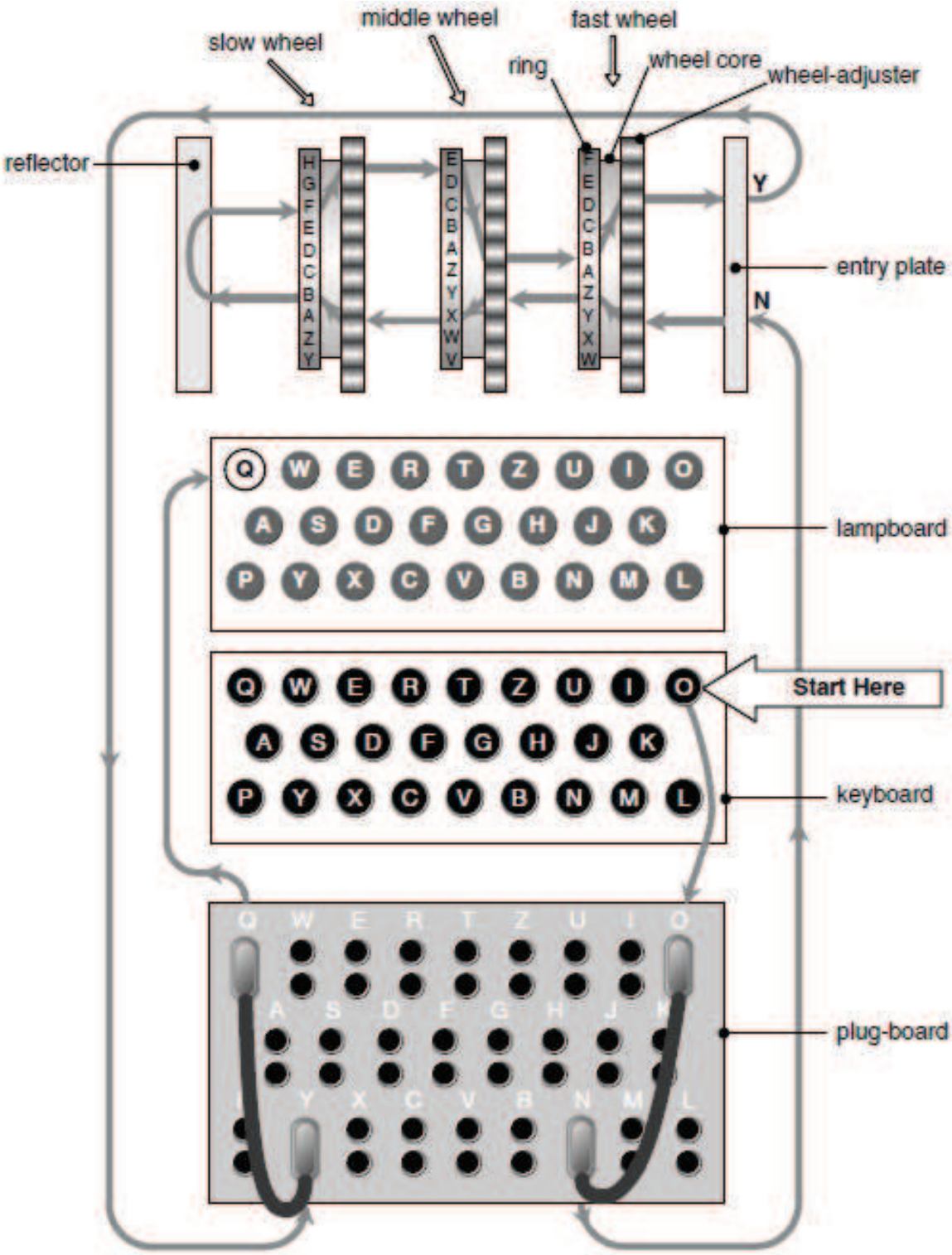
A máquina Enigma tem uma das mais fascinantes histórias dentre os diversos aparelhos mecânicos da época. Ela foi usada comercialmente durante o começo dos anos 1920 e possuía vários modelos. Foi adotada não só pelos alemães, mas também por vários outros governos. O modelo alemão, conhecido como *Wehrmacht Enigma*, é o mais discutido por ter sido o que os decifradores aliados conseguiram desvendar depois de muito estudo (COUTO, 2008).

Nos anos posteriores à Primeira Guerra Mundial, os criptoanalistas britânicos continuaram a monitorar as comunicações alemãs. Em 1926 eles começaram a interceptar mensagens que os deixaram completamente confusos. A Enigma tinha entrado em ação, e à medida que o número de máquinas aumentava, a capacidade da Sala 40 para colher informações diminuía rapidamente. Os estadounidenses e Franceses tentaram quebrar a cifra da Enigma mas não conseguiram. Os poloneses continuaram a monitorar as comunicações dos alemães com eficiência até 1926 quando eles também não conseguiram decifrar as mensagens da máquina Enigma. A Alemanha tinha agora a rede de comunicações mais segura do mundo (SINGH, 2014).

De acordo com a figura 63, podemos observar uma máquina Enigma dentro de seu compartimento de proteção feito de madeira maciça. No fundo da tampa da caixa é possível ver o símbolo Enigma e abaixo do símbolo existe algumas informações como modelo e de qual entidade militar (exército, marinha ou aeronáutica) ela pertencia. Outra observação importante é que esta máquina Enigma possuía 4 rotores em vez dos tradicionais 3 rotores. Os rotores se localizam logo acima do painel luminoso. A máquina de cifragem Enigma possui seis componentes principais: teclado (keyboard), um quadro de luzes representando um teclado luminoso (*lampboard*), um conjunto de rotores (*set of rollers*), um refletor (*reflector*), quadro de plugues (*plug-board*) e uma bateria (*battery*). O operador da máquina Enigma tinha que regular os rotores de acordo com a cifra do dia para então começar a digitar as mensagens utilizando o teclado (*keyboard*). A cada letra pressionada no teclado (keyboard), uma luz representava a letra cifrada no quadro de lâmpadas (*lampboard*). As primeiras máquinas Enigma tinham três rotores, cada um com 26 posições que podiam ser escolhidas manualmente seguindo-se um padrão pré-combinado para a formação do código inicial (chave da mensagem).

Quando foi possível trocar os rotores, eles passaram a ter uma numeração baseada em algarismos romanos (TKOTZ, 2005).

Figura 63 – Componentes básicos de uma máquina Enigma



Fonte: http://www.cryptool-online.org/images/stories/cto/enigma-grafik2.jpg

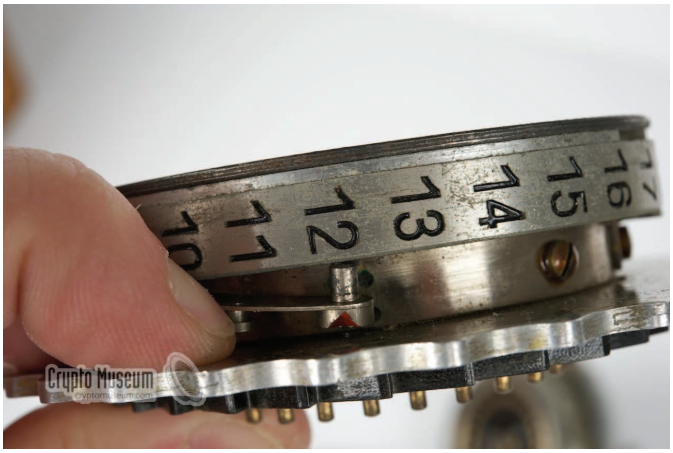
Na figura 63, o operador pressionou a tecla “O” do teclado (*keyboard*) onde uma seta com a frase (*Start Here*) “Comece aqui” está indicando. Seguindo uma linha que percorre um trajeto dentro da máquina Enigma, é demonstrado como era realizado neste caso a cifragem da letra “O” que na figura aparece a letra “Q” no quadro de lâmpadas (*lampboard*). Cada letra digitada move um rotor do lado direito uma posição e caso o operador digite a mesma tecla “O”, outra letra no quadro de lâmpadas será acesa em vez da letra “Q”.

Figura 64 – Rotor (roda ou tambor) da máquina de cifragem Enigma

Fonte: http://www.cryptomuseum.com/crypto/enigma/img/exploded.gif

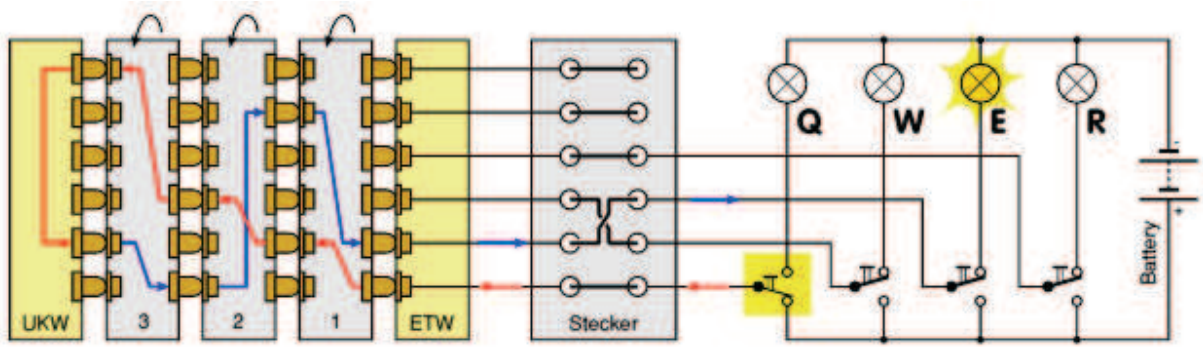
Era possível colocar letras do alfabeto no anel do rotor como na figura 64 ou colocar números (1 a 26) no anel do rotor de acordo com a figura 65.

Figura 65 – Rotor com a numeração de 1 a 26



Fonte: http://www.cryptomuseum.com/crypto/enigma/i/img/300002/056/full.jpg

Figura 66 – Diagrama simplificado do circuito de uma Enigma de Serviço ou Enigma I de 3 rotores



Fonte: http://www.cryptomuseum.com/crypto/enigma/img/sch3.gif

As letras ou números são "misturadas" por um conjunto de rotores ou rodas giratórias cada uma com 26 contatos de cada lado. Cada contato em um lado é conectado (ligado) a um contato no outro lado de maneira aleatória. Alguns modelos, como a Enigma de Serviço e a M3 têm 3 rotores ou rodas giratórias, mas o modelo M4, usado mais tarde na guerra exclusivamente para os submarinos alemães, tinham 4 rotores ou rodas. Cada vez que uma tecla é pressionada, a roda mais à direita é girada por um passo, resultando em um mapeamento diferente dos fios internos. Como resultado, cada nova letra é codificada de forma diferente. Na figura acima é possível ver o refletor da esquerda (UKW), rotores 3, 2, 1, refletor da direita (ETW), Stecker (misturador), contatos do teclado, painel de lâmpadas e conexão para a bateria (Battery). No exemplo acima a letra “Q” foi pressionada e a letra “E” no painel de lâmpadas acendeu indicando que a letra “Q” está cifrada na letra “E” naquele momento. Se a letra “Q” for pressionada outra vez, outra letra acenderá no painel de lâmpadas e não será a letra “E” (CRYPTO, 2016).

Figura 67 – Conectores do *Steckerbrett*

Fonte: http://www.cryptomuseum.com/crypto/enigma/i/img/300002/083/full.jpg

As versões militares alemãs da máquina de cifragem Enigma usavam fiação interna diferente, além de terem uma *Steckerbrett* (placa de conexões ou painel de plugues). A máquina Enigma apresentava uma aparência não muito agradável e ainda contava com buracos onde um operador poderia colocar plugues para conectar ainda mais pares de letras. Isso proporcionava mais uma camada de cifragem aumentando o número de configurações possíveis para aproximadamente 160 trilhões. Nos círculos militares e governamentais alemães se estabeleceu uma certa complacência com este nível de segurança alcançado (PATERSON, 2009, p. 43).

Figura 68 - *Steckerbrett* (placa de conexões ou painel de plugues) da Enigma A

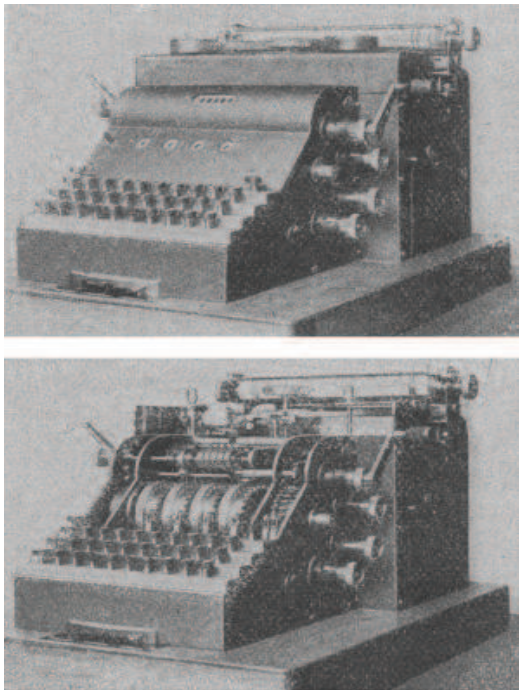
Fonte: http://www.cryptomuseum.com/crypto/enigma/i/img/300002/026/full.jpg

A partir de 1933, a Enigma estava em uso não só no exército e na marinha, como também no serviço diplomático e fazia parte do programa de armamento maciço de Hitler. Os modelos usados na inteligência eram diferentes dos modelos comerciais e suas configurações eram segredo de Estado (TKOTZ, 2005).

3.2.1 Máquina Enigma A

A Enigma A foi a primeira máquina de cifragem vendida com a marca Enigma, lançada no mercado em 1923. A máquina foi desenvolvida pela companhia berlinense *Scherbius & Ritter*, mas foi colocada em produção pela também berlinense *Gewerkschaft Securitas* (que mais tarde se tornaria *Chiffriermaschinen* AG). Ela era grande, pesada e volumosa, e sua entrada de dados era como uma máquina de escrever normal, com a saída de dados diretamente em papel. Como neste modelo a operação de cifragem não era reversível, havia três modos de uso: cifragem, decifragem e texto claro, sendo que este último fazia com que a máquina pudesse ser usada como uma máquina de escrever normal a qualquer momento. Na figura 69 observamos a máquina de cifragem Enigma A com a tampa frontal (imagem superior) e a mesma máquina Enigma A sem a tampa frontal (imagem inferior) sendo possível ver os rotores logo acima do teclado (CRYPTO, 2016).

Figura 69 – Máquina de cifragem Enigma A com a tampa frontal e sem a tampa frontal



Fonte: http://www.cryptomuseum.com/crypto/enigma/a/img/etz0t.jpg

3.2.2 Máquina Enigma B

A máquina de cifragem Enigma B ou (*Schreibende* Enigma) foi desenvolvida em 1924 sendo a sucessora da Enigma A de 1923. A Enigma B era bastante pesada e também imprimia diretamente no papel. A cabeça rotativa de impressão do modelo A foi substituída por uma série de barras de digitação, como as de máquinas de escrever. Embora fosse bem acabado, este modelo teve muitos problemas de produção. A máquina era muito cara além de ser difícil de operar de maneira confiável em velocidades mais rápidas. Em 1926, foi lançada uma versão modificada e melhorada do modelo, que foi sucedido em 1929 pelo modelo H (CRYPTO, 2016).

Figura 70 – Máquina de cifragem Enigma B

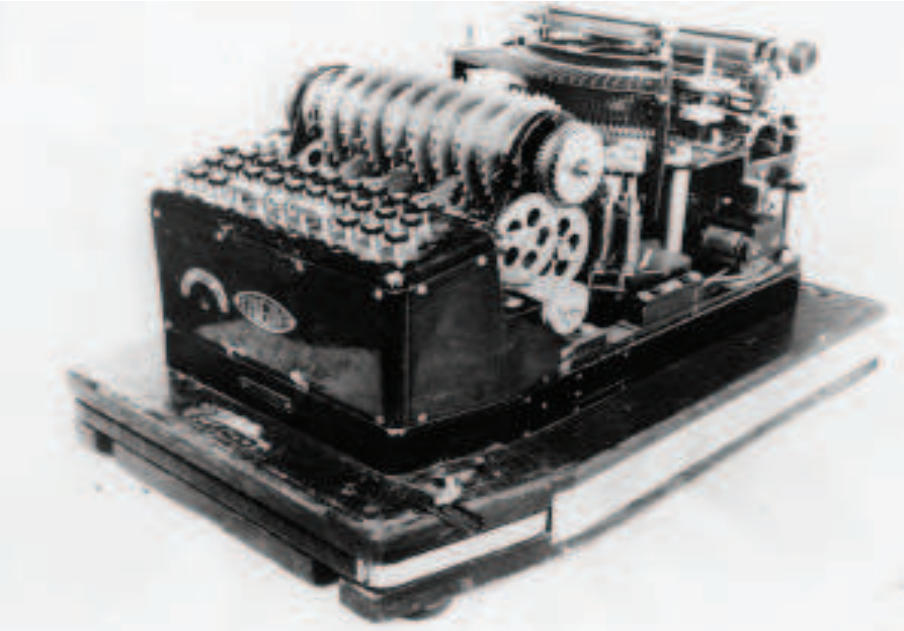
Fonte: http://www.cryptomuseum.com/crypto/enigma/b/img/b_003_small.jpg

3.2.3 Máquina de cifragem Enigma H

A máquina de cifragem Enigma H foi a última da série (*Schreibende* Enigma). Foi desenvolvida e introduzida em 1929 como sendo a sucessora da Enigma B de 1926 sendo usada principalmente pelo exército alemão (*Wehrmacht*) onde era conhecida como Enigma II. Esta máquina foi vendida também para consumidores estrangeiros como por exemplo para os húngaros (modelo H-221) que a introduziram no exército.

A máquina tinha 8 rotores de cifra, mas apenas 4 delas foram usadas para a codificação dos sinais elétricos. Cada rotor tinha 26 pontos de contato (A-Z) e a máquina era capaz de criptografar letras e números. O número oficial dessa máquina Enigma era H29 (Ch. 14). Como desvantagens tinha o peso elevado e um elevado custo de aquisição (CRYPTO, 2016).

Figura 71 – Máquina de cifragem Enigma H



Fonte: http://www.cryptomuseum.com/crypto/enigma/h/img/h_small.jpg

3.2.4 Máquina de cifragem Enigma C

A máquina de cifragem Enigma C, lançada em 1924, foi o primeiro modelo a usar um painel de lâmpadas (Alemão: *Glühlampen*) para a saída de dados. Era uma alternativa de baixo custo para os modelos baseados em máquinas de escrever além de ser muito menor que os modelos anteriores, o que a tornava portátil. O custo da Enigma C era cerca de 1/8 do custo da Enigma A.

Muitas versões da Enigma C foram construídas mas o modelo básico apresentava 26 pontos de contato no rotor de cifragem além de usar o alfabeto internacional padrão. As teclas do teclado estavam dispostas na ordem do alfabeto (ABCDEFG) e não no padrão QWERTY. Uma versão especial da Enigma C foi desenvolvida para a (*Kriegsmarine* – Marinha Alemã) chamada *Funk Schlüssel* C e possuía 28 pontos de contato em cada rotor de cifragem. No entanto, o teclado tinha 29 teclas, das quais a letra X estava conectada "diretamente". O UKW (refletor ajustável) foi fixado nesta versão (não podia ser ajustado), mas poderia ser montado em 4 orientações diferentes (CRYPTO, 2016).

Figura 72 – Máquina de cifragem Enigma C

Fonte: http://www.cryptomuseum.com/crypto/enigma/img/300699/005/small.jpg

3.2.5 Máquina de cifragem Enigma D

A máquina de cifragem Enigma D era também conhecida como Enigma comercial A26 e foi desenvolvida em 1926 como sucessora da Enigma C. O número do modelo oficial era A26 e seu designador interno era Ch. 8 de acordo com o fabricante *Chiffriermaschinen* AG. A Enigma D foi substituída um ano depois por um modelo quase idêntico chamado Enigma K (A27).

A Enigma D apresentava várias melhorias em relação ao modelo anterior Enigma C. Primeiro, a tampa superior da máquina ficou mais acessível, de modo que era mais fácil alterar as configurações básicas (tecla). Os três rotores de codificação foram montados agora em um eixo removível, de modo que a ordem das rotores poderia ser mudada também. Além disso, o refletor (UKW) tornou-se ajustável, o que significa que poderia ser ajustado para qualquer uma das 26 posições. Tudo isso aumentou o número máximo de permutações.

Olhando para a árvore genealógica Enigma (figura 52) é óbvio que por volta de 1926 o Enigma D foi o principal produto do fabricante *Chiffriermaschinen* AG. Todas as máquinas Enigma adicionais seriam baseadas (em grande parte ou em parte) no projeto Enigma D (CRYPTO, 2016).

Figura 73 – Máquina de cifragem Enigma D

Fonte: http://www.cryptomuseum.com/crypto/enigma/d/img/301443/039/small.jpg

3.2.6 Máquina de cifragem Enigma I ou Enigma *Reichswehr* D

A Enigma I ficou conhecida como Enigma de Serviço, com designador interno Ch. 11a. e foi a primeira máquina Enigma com painel de lâmpadas usada exclusivamente pelo Exército alemão antes e durante a Segunda Guerra Mundial. O Exército alemão adotou a máquina Enigma em 1927, e ela entrou em uso em 1928 com uma importante alteração: um painel de plugues. Todas as outras máquinas Enigma usadas pelo Exército alemão foram baseadas neste modelo (Enigma I). A Enigma I era baseada no chassi da Enigma D, mas tinha um refletor fixo e um único painel de plugues atrás da aba de madeira na parte frontal da máquina. Ela possuía inicialmente três rotores de códigos que podiam ser inseridas em 6 posições diferentes. Em dezembro de 1938, surgiram dois novos rotores, o que fazia com que o número de posições diferentes de configuração inicial passasse para 60 aumentando em 10 vezes a segurança da cifra. Os dois rotores que não estavam sendo usados no momento eram acondicionados em uma pequena caixa de madeira. Inicialmente foi usado pelo Exército e Força Aérea Alemãs. Posteriormente foi adotada pela Marinha Alemã se tornando conhecida como M1, M2 e finalmente M3. Cerca de 20 mil máquinas desse tipo foram construídas (CRYPTO, 2016).

Figura 74 – Máquina de cifragem Enigma I ou Enigma *Reichswehr* D

Fonte: http://cryptomuseum.com/crypto/enigma/i/img/300002/022/Small.jpg

3.2.7 Máquina de cifragem Enigma M1, M2 e M3 ou Enigma Naval de 3 rotores

As Enigmas M1, M2 e M3 eram máquinas de cifragem eletromecânicas de 3 rotores, geralmente conhecidas como M3, usadas durante a Segunda Guerra Mundial pela Marinha Alemã (Kriegsmarine). A máquina era compatível com a Enigma I usadas pelo Exército (*Wehrmacht*) e pela Força Aérea (*Luftwaffe*). Depois que o *Wehrmacht* introduziu a Enigma I em 1932, a *Kriegsmarine* seguiu em 1934 com a introdução do M1. Embora a máquina Enigma M1 seja compatível com o Enigma I, tem algumas diferenças de fabricação que são exclusivas da Marinha Alemã. As Enigmas M1, M2 e M3 são também conhecidas pelo seu designador: Ch.11g. Verifique a tabela 16 para verificar os designadores internos.

Como exemplo: os rotores de cifragem têm letras (A-Z) ao redor do aro em vez de números (01-26) e a máquina tem soquetes de 4V (Volts) ou 6V (Volts), para que ele possa ser alimentado a partir da rede elétrica do navio submarino.

No total foram construídas 611 unidades da Enigma M1. O modelo M1 foi seguido em 1938 pelo modelo M2, dos quais 890 unidades foram entregues. Finalmente, em 1940, foi substituído pelo M3, dos quais aproximadamente 800 unidades foram construídas (CRYPTO, 2016).

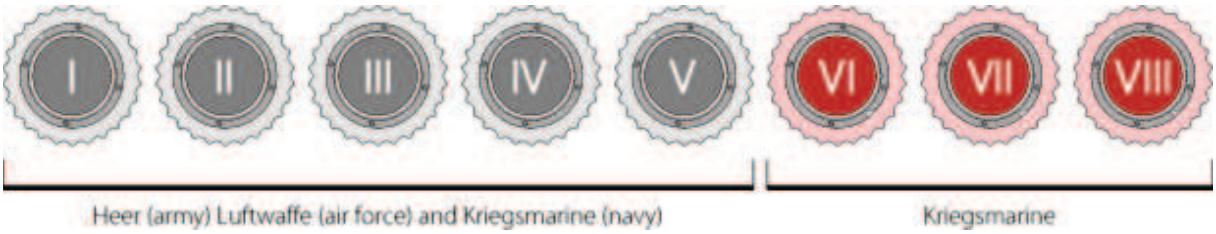
Figura 75 – Máquina de cifragem Enigma M3 a bordo do U-Boot U-124

Fonte: http://www.cryptomuseum.com/crypto/enigma/m4/img/enigma_u124_small.jpg

Inicialmente, a Enigma M3 foi fornecida com 5 rotores de cifragem que foram ligadas de forma idêntica como os rotores da Enigma I. Desta forma, o *Kriegsmarine* foi capaz de trocar mensagens com o Exército e a Força Aérea alemãs. Em 1939 contudo, foram adicionados mais três rotores (VI, VII e VIII) que foram usados exclusivamente pela *Kriegsmarine*. No início da Segunda Guerra Mundial, a divisão U-Boot (submarinos) da *Kriegsmarine* também usou a máquina de cifragem Enigma M3, até que foi substituída inesperadamente pela máquina de cifragem Enigma M4 de 4 rotores em 2 de fevereiro de 1942.

Enquanto as máquinas Enigma da *Wehrmacht* e *Luftwaffe* foram fornecidas com 5 rotores, todas as máquinas navais tinham 8 rotores para escolher (5 rotores padrão + 3 rotores aleatórios). Os cinco primeiros rotores (I-V) eram idênticos aos cinco rotores fornecidos ao resto das forças alemãs, permitindo algum nível de compatibilidade, mas os três rotores adicionais (VI-VIII) foram usados exclusivamente pela *Kriegsmarine* (CRYPTO, 2016).

Figura 76 – Máquina de cifragem Enigma com 5 rotores usados pelo Exército e Força Aérea alemãs e os 3 rotores adicionais para as máquinas Enigmas Navais



Fonte: http://www.cryptomuseum.com/crypto/enigma/m4/img/wheels.png

Dos 8 rotores fornecidos com o Enigma M3, três seriam colocados na máquina a qualquer momento, sujeitos aos atuais ajustes das teclas. Embora 3 rotores de 8 teoricamente dariam um número total de 336 combinações de rotores (8 x 7 x 6), isto foi limitado na prática pelos procedimentos operacionais. Havia uma instrução que um dos três rotores na máquina tinha que ser uma rotor Naval (VI-VIII)

e que aquele rotor naval particular não poderia ser usado na mesma posição em dois dias consecutivos (CRYPTO, 2016).

3.2.8 Máquina de cifragem Enigma M4 ou U-Boot Enigma

A máquina de cifragem Enigma M4 foi desenvolvida durante a Segunda Guerra Mundial como sucessora do modelo M3 que por sua vez era baseado na Enigma I. Era de uso exclusivo para a divisão de submarinos (U-Boot) da *Kriegsmarine*. O modelo M4 representou um papel vital na batalha do Atlântico e foi introduzido em 2 de fevereiro 1942. Causou grande impacto nos decifradores de código aliados em *Bletchley Park* (BP), onde o seu tráfego era conhecido como Shark (tubarão). Os aliados ficaram sem decifrar mensagens navais dos alemães de fevereiro de 1942 até novembro de 1942 até que novos livros de código foram capturados. A introdução da Enigma M4 deu vantagem aos alemães na Batalha do Atlântico.

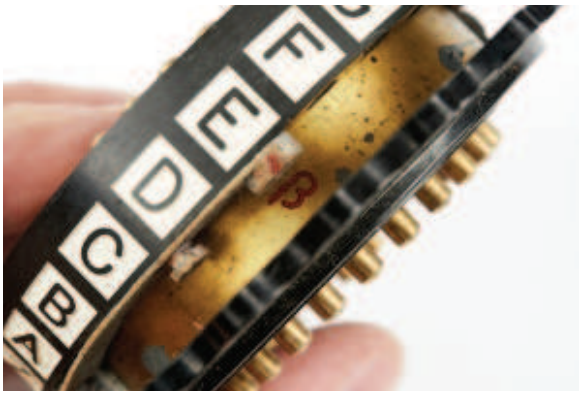
A Enigma M4 era fornecida com 8 rotores de codificação diferentes, (marcadas I a VIII), três dos quais estavam na máquina a qualquer momento. A fiação dos rotores I a V era idêntica à do Enigma I. Ao contrário do Exército no entanto, a Marinha optou por ter letras (A-Z) na circunferência de cada rotor, ao invés de números (01-26).

Nos submarinos, a máquina Enigma era geralmente localizada na sala de rádio, embora em alguns casos fosse levado para o quarto do capitão para uma dupla encriptação (*Sonderschlussel* M). A maioria dos submarinos tinham duas máquinas Enigma disponíveis, para lidar com diferentes chaves no período anterior e posterior da meia-noite. Uma máquina Enigma seria então deixada com as configurações do dia anterior, enquanto que a outra era configurada com as configurações para o novo dia. Como algumas mensagens eram recebidas com atraso, elas poderiam ser rapidamente testadas com ambas as chaves.

Embora a Enigma comercial tivesse 4 rotores que se sobressaem na tampa superior, era na verdade uma máquina de 3 rotores com um refletor ajustável

(UKW). A Enigma M4 entretanto, tem um rotor extra de cifragem à esquerda dos 3 rotores de codificação normais, sendo a única máquina derivada da Enigma I que pode verdadeiramente ser chamada uma máquina de 4 rotores. O 4º rotor adicional foi chamado de *Zusatzwalze* (rotor extra) ou *Griechenwalze* (rotor grego) sendo identificado com a letra grega Beta (β) ou Gamma (γ) (CRYPTO, 2016).

Figura 77 - O 4º rotor adicional foi chamado de *Zusatzwalze* (roda extra) ou *Griechenwalze* (roda grega) como ele foi identificado com a letra grega Beta (β) ou Gamma (γ).



Fonte: http://www.cryptomuseum.com/crypto/enigma/m4/img/300012/151/small.jpg

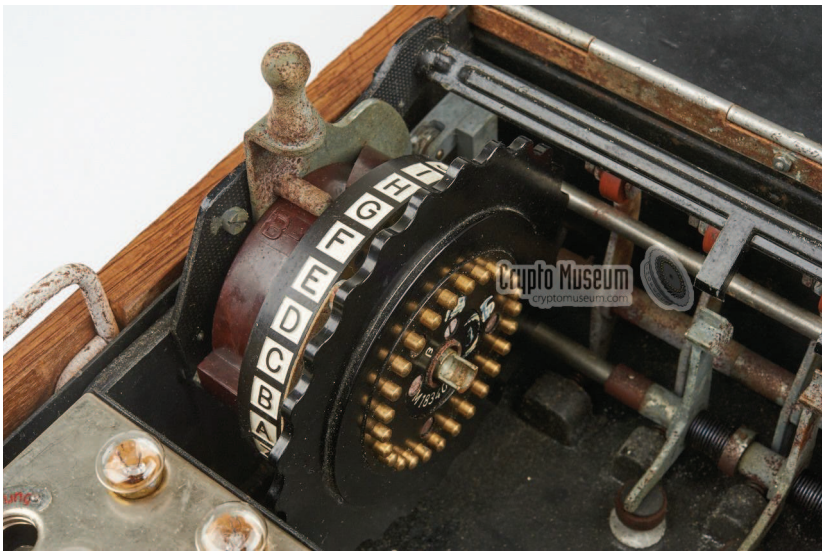
O problema com a *Zusatzwalze* no entanto, foi que ele não poderia ser escolhido a partir do conjunto total de 8 rodas. Em outras palavras: não poderia ser trocado com as outras rodas. A razão para isso é que ele é construído de forma diferente. É mais estreito que os outros e tem contatos de mola de ambos os lados. Além disso, o UKW é mais estreito e tem 26 contatos de face plana, ao invés de pinos. Note que a roda extra não é conduzida pelos outros. Em outras palavras: ele nunca é movido durante o cifrado. De fato, junto com o UKW, é apenas um seletor para 26 UKWs diferentes.

Figura 78 – Máquina de cifragem Enigma M4

Fonte: http://www.cryptomuseum.com/crypto/enigma/m4/img/300012/087/small.jpg

A máquina de cifragem Enigma M4 foi o último modelo utilizado pelos submarinos alemães até o final da Segunda Guerra Mundial. Verifique na tabela 16 os modelos anteriores que deram origem ao modelo M4.

Figura 79 – Máquina Enigma M4 com o rotor extra ou *Zustzwalze*



Fonte: http://www.cryptomuseum.com/crypto/enigma/m4/img/300012/133/full.jpg

Note que embora o *Zustzwalze* possa ser definido para qualquer posição, ele não se move durante o processo de cifragem. Em outras palavras: ele não pode ser movido pela roda à sua direita. Isso pode ser considerado uma desvantagem, pois limita o número de permutações de todo o sistema. A combinação UKW + *Zusatzwalze* pode ser considerada como um seletor entre 26 UKWs diferentes.

Outra desvantagem do mecanismo de rotação do rotor é o fato de que os rotores se movem regularmente. Somente após a roda mais à direita ter completado uma revolução completa, faz com que a próxima roda faça um único passo. Como resultado, o segundo rotor (a partir da direita) só fará um passo a cada 26 caracteres e o terceiro rotor dificilmente se moverá. Isso torna a máquina previsível e mais fácil de quebrar. A única máquina com passo irregular foi a Enigma G ou *Zählwerkmaschine*.

Os três rotores extras VI, VII e VIII têm dois entalhes cada, o que provoca uma rotação mais frequente do rotor e um passo menos regular. Isso foi feito como o rotor 3 (a partir da direita) que quase nunca muda durante o processo de cifragem.

Figura 80 – Rotores de 2 entalhes cada um

Fonte: http://www.cryptomuseum.com/crypto/enigma/m4/img/300012/189/small.jpg

Note-se, no entanto, que as rodas têm 2 entalhes cada. O número 2 entalhes em cada rotor não era um número primo relativo de 26 (26 podem ser divididos por 2) e que os entalhes estão posicionados em frente um do outro. O resultado é que o período de cifra é efetivamente reduzido pela metade, o que era mais uma desvantagem do sistema e um bônus para os *codebreakers* (decifradores de código) de *Bletchley Park*.

A máquina Enigma M4 veio por padrão com o refletor fino b e um rotor extra β (Beta). Eles foram conectados de tal maneira que juntos, com a roda β ajustada para 'A', a combinação se comportou exatamente como UKW-B no Enigma M3 e Enigma I. Isso tornou a máquina compatível com versões anteriores. Veja na figura 74. A máquina de cifragem Enigma M4 foi construída no chassi do M3 (que por sua vez foi baseado no chassis da máquina de cifragem Enigma I). A fim de ajustar o rotor-β extra no espaço existente, o novo refletor, UKW-b, teve que ser menor que o padrão UKW-B (CRYPTO, 2016).

Figura 81 – Refletor da máquina Enigma M4

Fonte: http://www.cryptomuseum.com/crypto/enigma/m4/img/300012/139/small.jpg

A imagem acima mostra o UKW-b, que tem um eixo oco curto montado no seu centro. O eixo oco é colocado sobre um eixo curto dentro da máquina e um pino de alinhamento é usado para manter UKW-b na posição correta. O rotor-β extra é então colocado sobre o eixo oco de modo que seus contatos alinham com os contatos de UKW-b.

Para além do UKW-b, a alternativa UKW-c foi também fornecida juntamente com o rotor extra γ (Gamma). Esta combinação era compatível com a norma UKW-C quando o rotor-γ foi ajustada para "A". Quando se utilizam outras combinações (isto é, UKW-b + γ e UKW-c + β) a máquina não era mais compatível com o M3 e com as máquinas usadas pela *Wehrmacht* e pela *Luftwaffe* (CRYPTO, 2016).

Figura 82 – Peça que substitui o rotor extra e o próprio rotor.

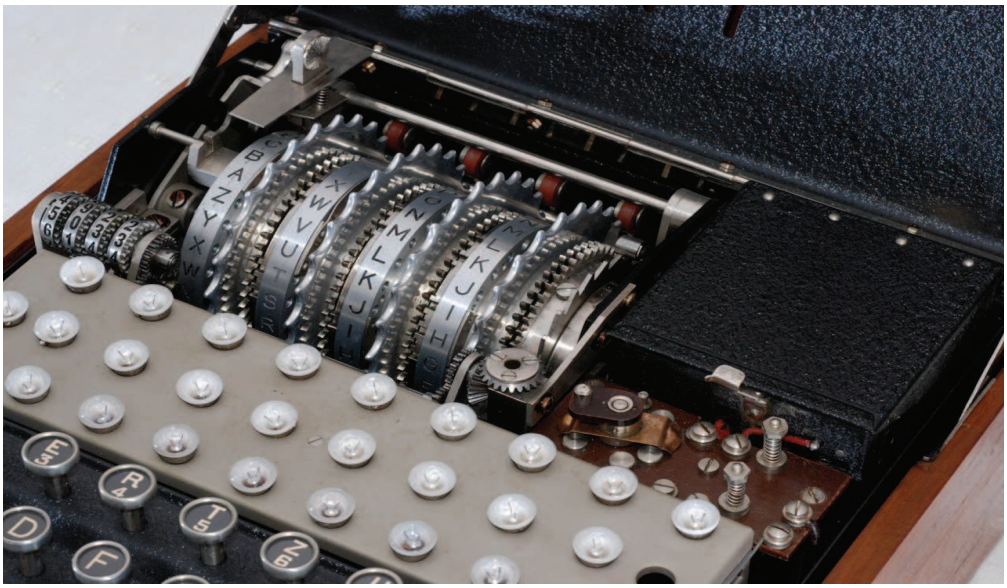
Fonte: http://www.cryptomuseum.com/crypto/enigma/img/300017/001/small.jpg

Durante a Segunda Guerra Mundial, várias tentativas foram feitas para tornar o tráfego da máquina de cifragem Enigma mais seguro. Em janeiro de 1944, um refletor especial, chamado UKW-D, foi introduzido pela *Luftwaffe* (Força Aérea Alemã). É pouco conhecido que um especial UKW-D também foi desenvolvido para o *Kriegsmarine* (Marinha Alemã). A imagem acima mostra um extremamente raro UKW-D com um número de série começando com a letra M, indicando naval-use (Marine). Foi desenvolvido especialmente para a máquina M4, e poderia possivelmente também ser usado na Enigma M3 de 3 rotores. Quando em uso, ele substitui tanto o refletor (UKW) como o rotor extra (*Zusatzwalze*). A letra D é gravada no corpo de UKW-D em tal posição que pode ser vista através da janela mais à esquerda da tampa do rotor da Enigma M4 (CRYPTO, 2016).

3.2.9 Máquina de cifragem *Zählwerk* Enigma (Enigma com contador de caracteres)

A máquina de cifragem Enigma *Zählwerk* foi desenvolvida em 1928 como uma versão melhorada da Enigma D. Uma característica marcante nesta Enigma era um contador de caracteres (Em alemão: *Zählwerk*) à esquerda dos rotores. O número de modelo oficial era A28 e foi dado o designador interno Ch.15 pelo fabricante. Era também conhecido como *Zählwerksmaschine*. Uma variante posterior desta máquina, a Enigma G (G31) tornou-se conhecido como o *Abwehr* Enigma.

Figura 83 - Zählwerk Enigma sem a tampa superior



Fonte: http://www.cryptomuseum.com/crypto/enigma/img/300166/019/full.jpg

A figura 83 mostra a máquina de cifragem Enigma *Zählwerk* com a tampa superior aberta, dando uma visão clara dos rotores de cifra. Os rotores têm as 26 letras do alfabeto gravadas em torno de sua circunferência, são conduzidas por um mecanismo de roda dentada que apresenta passo irregular. Uma manivela pode ser inserida em um pequeno orifício à direita dos rotores de cifra, permitindo que o mecanismo de passo seja controlado manualmente; Para frente e para trás. Isso permitiu ao operador corrigir erros, mas também permitiu inserir passos intermitentes manualmente para fazer parte da chave criptográfica (CRYPTO, 2016).

Ainda na figura 83 é possível observar um contador de caracteres no lado esquerdo do primeiro rotor, acima do painel de lâmpadas. O contador de caracteres está marcando o número 5033.

Figura 84 - Zählwerk Enigma com o contador de caracteres mostrando 7276

Fonte: http://www.cryptomuseum.com/crypto/enigma/img/300166/060/full.jpg

Um contador de quatro dígitos à esquerda dos rotores de cifragem foi usado para contar o número de caracteres em uma mensagem. O número de caracteres foi frequentemente enviado no preâmbulo da mensagem e foi usado principalmente para verificação. Como o contador não pode ser redefinido, o operador anotava o número no início da mensagem e subtraía do valor final (CRYPTO, 2016).

3.2.9.1 Máquina de cifragem Enigma G ou *Zählwerk* Enigma G31

A máquina de cifragem Enigma G foi desenvolvido em 1931 como uma das sucessoras da Enigma Zählwerk (modelo A28) de 1928. Caracteriza um mecanismo de rotor com passo irregular e uma manivela para enrolá-lo para a frente e para trás. O número de modelo oficial da máquina era G31 mas é consultado geralmente como máquina de cifragem Enigma G, porque os números de série começam com a letra "G". O designador oficial é Ch.15ª. Os decifradores de código de *Bletchley Park* chamavam a Enigma G de 11-15-17 (por causa do número de entalhes em cada rotor). É também conhecida como máquina de cifragem *Abwehr* Enigma (CRYPTO, 2016).

Figura 85 - Enigma G ou *Zählwerk* Enigma G31

Fonte: http://www.cryptomuseum.com/crypto/enigma/g/img/301671/014/full.jpg

A máquina de cifragem Enigma G é diferente de todos os outros modelos Enigma, não só por causa do mecanismo de rotor dentado, mas também por causa de seu tamanho menor, seus rotores menores, painel de lâmpada inclinado além de uma alavanca grande saindo no centro superior atrás dos rotores de cifragem.

A máquina de cifragem Enigma G ou G31 foi provavelmente uma tentativa de fazer uma versão menor e mais leve da Enigma *Zählwerk*. A caixa de transporte de madeira é menor do que qualquer um dos anteriores e até mesmo as rotores de cifra são menores, tornando-os mecanicamente incompatível com qualquer outro modelo Enigma. A máquina usa uma bateria muito menor que está montada abaixo do conjunto do interruptor no canto superior direito, mas também pode ser alimentado por uma fonte externa, por exemplo, por um transformador. Uma manivela, que normalmente é armazenada dentro da tampa superior da caixa de madeira, pode ser inserido em um buraco no lado direito da máquina, permitindo que o mecanismo de

passo seja controlado manualmente; Para frente e para trás. Isso permitiu ao operador corrigir erros, e inserir passos intermitentes manualmente para fazer parte da chave criptográfica.

Foram feitas três versões diferentes da Enigma G31. A versão mais comum foi o Ch.15a, a versão padrão que foi fornecida, por exemplo, à *Abwehr* e à Marinha Holandesa. O Ch.15b tinha um soquete da impressora em seu lado esquerdo e o Ch.15c era uma versão especial com um *Steckerbrett* alternativo (painel de plugues) (CRYPTO, 2016).

3.2.9.2 Máquina de cifragem Enigma T (*Tirpitz*) ou Enigma japonesa

A máquina de cifragem Enigma T, codinome *Tirpitz*, foi desenvolvida durante a Segunda Guerra Mundial pelos alemães especialmente para uso do exército japonês. Baseava-se na máquina de cifragem Enigma K comercial, mas tinha rotores com fios diferentes (e ETW) e múltiplas rotações em cada rotor. Além disso, tinha um rotor de entrada *Eintrittswalze* (ETW) que era ligado de forma diferente de todas as outras máquinas Enigma. A máquina era destinada para a comunicação entre a marinha alemã e japonesa. O acordo foi assinado em 11 de setembro de 1942 pelo vice-almirante alemão *Erhard Maertens* e o almirante japonês *Tadao Yokoi*. Na época, *Maertens* era Diretor do Serviço de Comunicação Naval da Alemanha e *Yokoi* era o Adido Naval Japonês em Berlim. Isto seguiu o acordo anterior militar japonês-alemão de 18 janeiro 1942.

Toda a comunicação alemã-japonesa seria criptografada com uma máquina que era referida como Enigma T ou Enigma Modelo T. Foi chamado de “TIRPITZ” pelos alemães, e os japoneses chamavam-na “TIRUPITSU”. A Marinha dos Estados Unidos se referiu à máquina como OPAL e o tráfego foi nomeado JN-18. O nome oficial do sistema da máquina era o Código de Uso Conjunto Japonês-Alemão Nº 3.

O sistema consistia de um procedimento operacional, denominado TIRPITZ, e uma lista chave com o nome GARTENZAUN (cerca de jardim). Os procedimentos

operacionais entraram em vigor a partir de 1 de agosto de 1943 até o final da Segunda Guerra Mundial.

Não se sabe exatamente quantas máquinas Enigmas T foram realmente construídas. Os japoneses encomendaram 800 máquinas de cifragem Enigma T, mas por várias razões essa quantidade nunca foi entregue. Houve atrasos na concepção e fabricação, e foi cada vez mais difícil obter materiais além da dificuldade provocada pela guerra. Além disso, os alemães começaram a duvidar da segurança da máquina. Entretanto, os japoneses usaram dois sistemas manuais: Sumatra (mais tarde Sumatra 2) e TOGO (mais tarde TOGO 2) (CRYPTO, 2016).

Figura 86 - Enigma T (*Tirpitz*) ou Enigma japonesa

Fonte: http://www.cryptomuseum.com/crypto/enigma/t/img/enigma_t244.jpg

A máquina Enigma T baseia-se no desenho da Enigma Comercial (K) e não na Enigma I que foi utilizado pelas Forças Armadas Alemãs. Como a máquina deveria ser usada para a comunicação entre as Marinhas da Alemanha e do Japão, eles precisavam de uma cifra forte, mas não queriam "dar" suas joias da coroa (isto é, a Enigma de Serviço com *Steckerbrett* (painel de plugues)). Em vez disso, adotaram como padrão a Enigma K e a modificaram de várias maneiras.

Em primeiro lugar, o rotor de entrada (ETW) foi ligado de forma aleatória, diferente de todas as outras máquinas Enigma. A máquina foi fornecida com 8 rotores de codificação (3 na máquina). A diferença mais importante no entanto, foi a presença de 5 entalhes de rotação em cada um dos 8 rotores (CRYPTO, 2016).

Figura 87 – Rotor da Enigma T com 5 entalhes de rotação

Fonte: http://www.cryptomuseum.com/crypto/enigma/img/300666/000/small.jpg

Isto causou movimentos do rotor mais frequentes e estendeu o período de cifra (como 5 é um número primo relativo de 26). Em alguns casos, o procedimento operacional instruiu o operador a avançar o UKW ajustável manualmente uma posição após cada grupo de 5 letras, adicionando a complexidade extra.

Algumas remessas ficaram perdidas sempre que o U-boat que transportava as máquinas Enigma era afundado. Um caso grave foi uma máquina Enigma T capturada em Guadalcanal em 15 de fevereiro de 1943. Os alemães começaram a duvidar de sua segurança, especialmente quando usavam para um grande volume de tráfego.

O tráfego de JN-18 (isto é, criptografado na Enigma-T) não foi frequentemente interceptado pelos americanos e era portanto muito difícil de quebrar. No fim da guerra, o Enigma T foi usado pelos adidos navais japoneses e mesmo para o tráfego diplomático. Em seguida os japoneses destruíram suas máquinas PURPLE. É conhecido por ter sido utilizado entre estações em Tóquio, Berlim, Estocolmo e

Berna. O procedimento operacional exato é atualmente desconhecido (CRYPTO, 2016).

3.2.9.3 Máquina de cifragem Enigma K

Em 1927, os desenvolvimentos foram iniciados para criar versões melhoradas da máquina Enigma D comercial. Uma das mais importantes foi a Enigma K que foi dado o modelo número A27 e designador interno Ch. 11b. A letra "K" foi provavelmente utilizada para a palavra alemã *Kommerziell* (comercial). Além de algumas modificações, esta máquina é idêntica à Enigma D. A máquina foi fornecida a uma variedade de clientes (internacionais) (CRYPTO, 2016).

Figura 88 – Máquina de cifragem Enigma K

Fonte: http://www.cryptomuseum.com/crypto/enigma/img/300879/004/small.jpg

Inicialmente, todas as máquinas tinham números de série começando (confusamente) com a letra A, e não foi até 1936 que a letra K foi usado como um prefixo para os números de série dessas máquinas. Muitas máquinas Enigma K foram construídas para usuários alemães, como a *Reichsbahn* (ferrovia), mas elas também foram vendidas para um número de usuários estrangeiros. Sabe-se que a Marinha italiana (*Supermarina*) usou a Enigma K durante a Segunda Guerra Mundial. As versões modificadas do Enigma K foram usadas igualmente durante a guerra civil espanhola (1936-1939) e outra pelo exército suíço durante e após a Segunda Guerra Mundial.

Na máquina de cifragem Enigma K, cada rotor tinha um entalhe de giro único (passo regular), mas em variantes posteriores, o número de entalhes foi aumentado. O Enigma T (1942), por exemplo, tinha 5 entalhes em cada rotor e os rotores da Enigma KD (1944) tinham 9 entalhes apresentando (passos irregulares) (CRYPTO, 2016).

3.2.9.4 Máquina de cifragem *Swiss-K* Enigma

A mais famosa e conhecida variante da Enigma K é provavelmente a versão que foi construída para o Exército suíço. Embora não seja um nome oficial, esta máquina é muitas vezes chamada de Swiss-K. As máquinas foram encomendadas pelos suíços antes da Segunda Guerra Mundial e o primeiro lote foi entregue em 1939.

Figura 89 – Máquina de cifragem Swiss-K Enigma com um painel de lâmpadas adicional

Fonte: http://www.cryptomuseum.com/crypto/enigma/img/300879/043/small.jpg

A figura 89 mostra uma típica máquina suíça Enigma K. É um padrão Enigma K que está montado dentro de uma caixa de madeira de carvalho bastante incomum que é mais largo do que uma Enigma usual. O espaço extra é usado para armazenar um painel de lâmpada adicional (veja a figura 90).

Figura 90: Painel de lâmpadas adicional

Fonte: http://www.cryptomuseum.com/crypto/enigma/img/300879/019/small.jpg

O bloqueio do estojo (usado para mantê-lo fechado) é idêntico ao de outras caixas de Enigma, mas dois suportes de metal estão montados à direita da fechadura, permitindo que um cadeado adicional seja usado. Dentro da tampa superior da caixa de madeira de carvalho são os acessórios habituais, como o filtro de lâmpada verde e as lâmpadas sobressalentes. Também está presente na tampa uma pequena braçadeira de metal para permitir que as mensagem sejam cortadas.

Os suíços começaram a usar a máquina Enigma em 1938, quando receberam 14 máquinas Enigma D. Outras 65 máquinas foram encomendadas em 1939. Finalmente, em 1940, um grande número de máquinas foram fornecidas em dois lotes (5 de maio e 10 de julho). Estas eram as máquinas que conhecemos agora como o *Swiss-K*. Em julho de 1942, um total de 265 máquinas estavam em uso, 102 pelo exército suíço e 163 pela força aérea. As máquinas do Ministério das Relações Exteriores foram emprestadas pelo Exército. Inicialmente, todos eles foram fornecidos com a fiação comercial padrão conhecido do Enigma D.

O painel extra de lâmpadas permitia que um segundo operador registrasse a mensagem criptografada para em seguida desencriptá-la.

Um painel de lâmpada externa similar está presente na máquina de cifra NEMA. O NEMA foi projetado para substituir a Enigma K suiça, depois que os suíços descobriram que suas mensagens estavam sendo lidas pelos alemães e as forças Aliadas.

Em 1944, os alemães desenvolveram uma nova versão da máquina Enigma chamada *B-Schreiber*. Em seguida os ingleses lançaram o *Colossus*, o primeiro computador eletrônico do mundo. (DAVIES, 2009, p. 55). No caso dos alemães a cifra da máquina Enigma havia sido descoberta e uma nova versão da Enigma seria de pouca ajuda. No caso dos ingleses além das “bombas de criptografia”, eles tinham um computador funcional que seria usado para decifrar mensagens alemãs cada vez mais rápidas.

Figura 91 – Máquina de cifragem Enigma da Marinha Italiana

Fonte: http://www.wayway.com.br/single-post/2016/06/17/Segredos-de-Bletchley-Park

A tradução do texto abaixo da máquina Enigma da figura 91: “Enigma Naval Italiana – A1214. Os registros mostram que esta máquina Enigma foi entregue por seus fabricantes *Heimsoeth und Rinke* à marinha italiana em 1932. Em 1941, a embaixada italiana em Berlim pediu rotores de reposição para a máquina. Esta máquina Enigma foi recuperada pelos oficiais da marinha dos EUA em 29 de abril de 1945 no norte da Itália. O ditador italiano 1922-1943, Benito Mussolini já possuía essa máquina enigma. Empréstimo da Fundação do Museu Nacional de Criptografia”.

Pelas explicações apresentadas dos principais modelos da máquina Enigma, podemos citar uma tabela contendo alguns modelos da máquina Enigma com mais de uma denominação.

TABELA 17 – Diferentes denominações da máquina Enigma

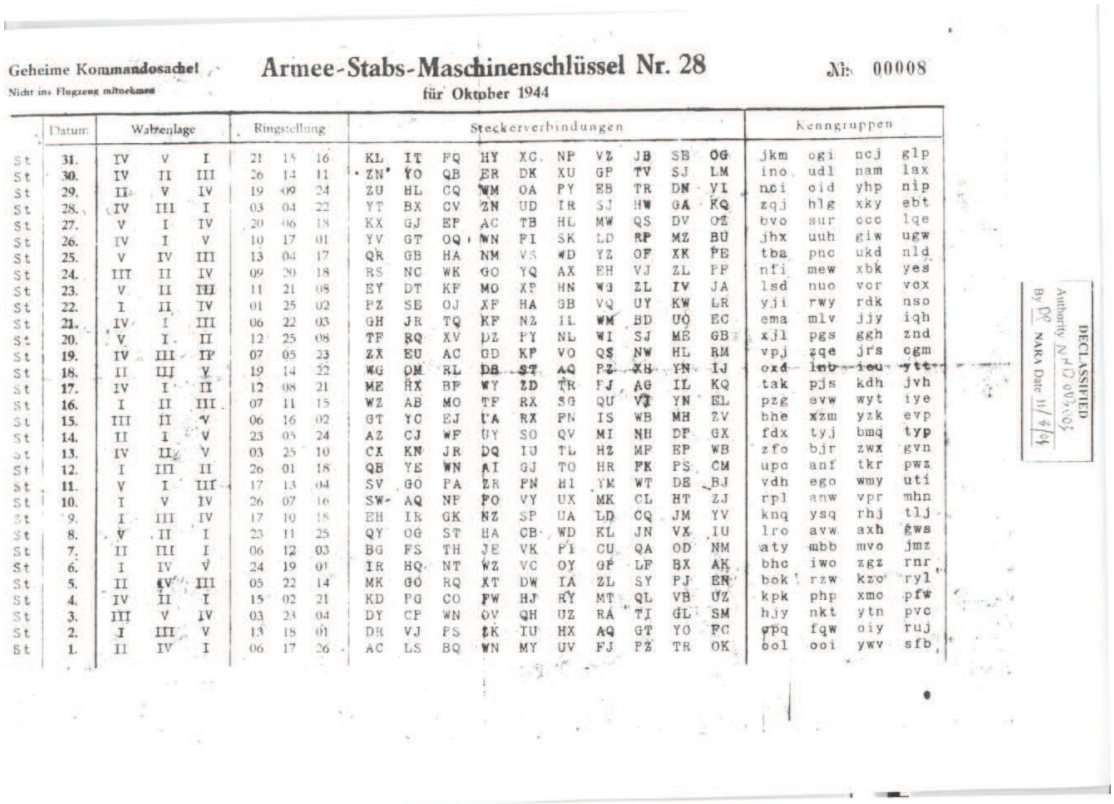
Nome	Designador oficial	Outras denominações
Enigma C	-	*Funkschlüssel* C (variação da Enigma C)
Enigma D	Ch. 8	A26, Enigma Comercial
Enigma *Reichwehr* D Enigma I	Ch. 11a e Ch. 11f	Enigma de Serviço, *Wehrmacht* Enigma, *Heeres* Enigma, Enigma de 3 rotores
Enigma M1, M2, M3	Ch. 11g	Enigma de 3 rotores naval
Enigma M4	Ch. 11g4	*U-Boot* Enigma
Enigma K	Ch. 11b	A27, Enigma Comercial, *Reichbahn* Enigma
Enigma T	-	*Tirpitz*, “Tirupitsu”
Enigma II	Ch. 14	Enigma H, H29
Enigma *Zählwerk*	Ch. 15	Enigma G, *Zählwerkmaschine*, *Abwehr* Enigma, A28

Fonte: Elaborado pelo autor

1. Procedimentos para enviar mensagens criptogradas da *Wehrmacht*

Para obter comunicações seguras, o Exército alemão (*Wehrmacht*) e a *Luftwaffe* (Força Aérea) usaram procedimentos padrão para transmitir e receber mensagens. Para que uma mensagem seja corretamente criptografada e descriptografada, tanto o remetente quanto o receptor precisam configurar sua máquina de cifragem Enigma exatamente da mesma maneira. Essas configurações foram distribuídas em folhas-chave. Por razões de segurança, diferentes partes das forças armadas tinham sua própria rede, com diferentes folhas-chave e com uma rede com seu próprio nome de código. As folhas das chaves foram distribuídas de antemão e continham as configurações básicas por um mês inteiro, por dia. Em geral, as folhas-chave estavam sob custódia de um oficial, responsável por configurar os rotores da máquina e os anéis. Após a configuração, ele poderia bloquear o painel frontal da máquina com uma chave. O operador só pode selecionar a posição de partida do rotor (RIJMENANTS, 2016).

Figura 92 - Folha chaves da Wehrmacht Enigma – Chave da máquina do Exército número 28



Geheime Kommandosache!
Nicht ins Flugzeug mitnehmen

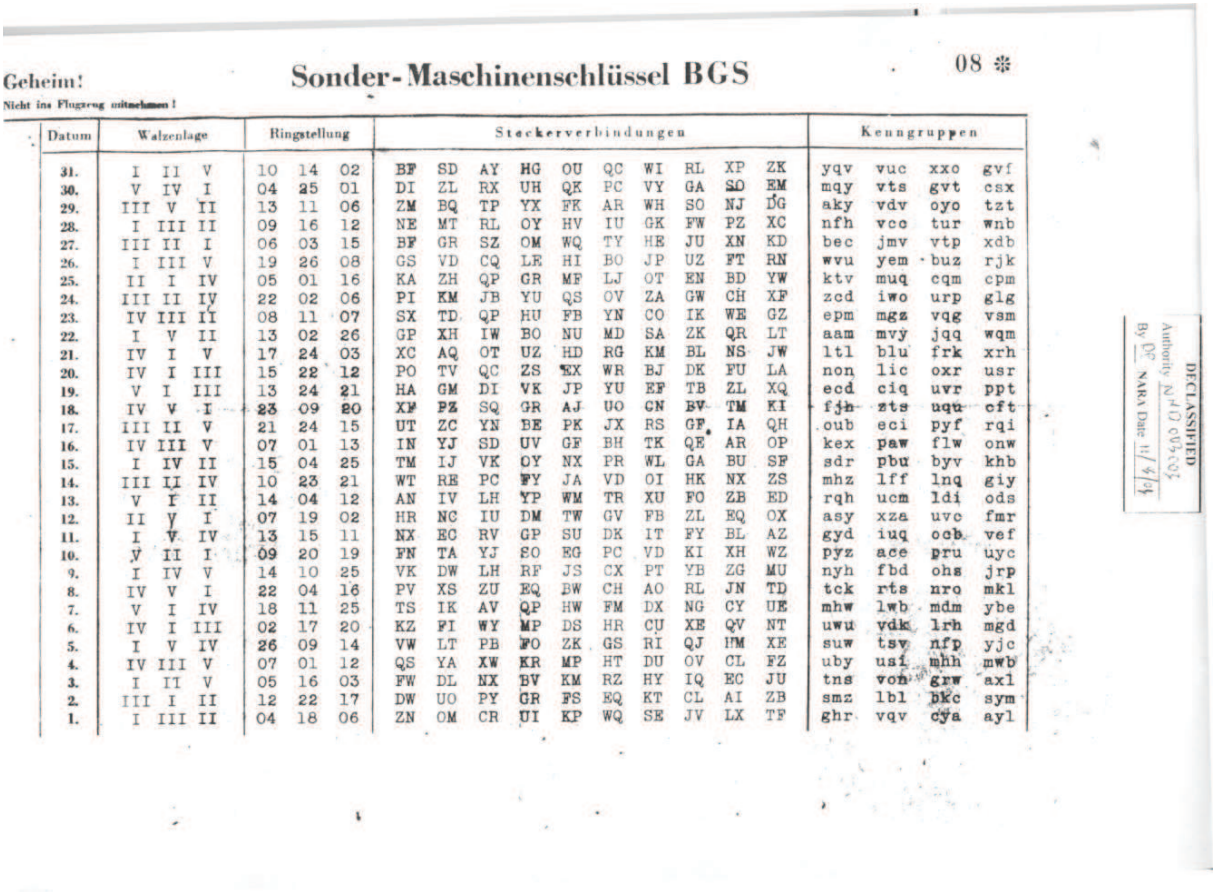
Armee-Stabs-Maschinenschlüssel Nr. 28
für Oktober 1944

№ 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen								Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SB	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	YI	nci	oid	yhp	nip
St	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	KQ	zqj	hlg	xky	ebt
St	27.	V	I	IV	20	06	18	KX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	ccc	lqe
St	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	FI	SK	LD	RP	MZ	BU	jhx	uuh	giw	ugw
St	25.	V	IV	III	13	04	17	QK	GB	HA	NM	VS	WD	YZ	OF	XK	PE	tba	pnc	ukd	nld
St	24.	III	II	IV	09	20	18	RS	NC	WK	GO	YQ	AX	EH	VJ	ZL	PF	nfi	mew	xbk	yes
St	23.	V	II	III	11	21	08	EY	DT	KF	MO	XP	HN	WB	ZL	IV	JA	lsd	nuo	vcr	vox
St	22.	I	II	IV	01	25	02	PZ	SE	OJ	XP	HA	GB	VQ	UY	KW	LR	yji	rwy	rdk	nso
St	21.	IV	I	III	06	22	03	GH	JR	TQ	KP	NZ	IL	WM	BD	UQ	EC	ema	mlv	jjy	iqh
St	20.	V	I	II	12	25	08	TF	RQ	XV	DZ	PY	NL	WI	SJ	ME	GB	xjl	pgs	ggh	znd
St	19.	IV	III	IV	07	05	23	ZX	EU	AC	GD	KP	VO	QS	NW	HL	RM	vpj	zqe	jrs	cgm
St	18.	II	III	V	19	14	22	WG	QM	RL	DB	ST	AQ	PZ	XB	FN	IJ	oxd	inb	icu	ytt
St	17.	IV	I	II	12	08	21	ME	RX	BP	WY	ZD	TR	FJ	AG	IL	KQ	tak	pjs	kdh	jvh
St	16.	I	II	III	07	11	15	WZ	AB	MO	TF	RX	SG	QU	VI	YN	EL	pzg	evw	wyt	iye
St	15.	III	II	V	06	16	02	GT	YC	EJ	LA	RX	FN	IS	WB	MH	ZV	bhe	xzm	yzk	evp
St	14.	II	I	V	23	05	24	AZ	CJ	WF	UY	SO	QV	MI	NH	DP	GX	fdx	tyj	bmq	typ
St	13.	IV	II	V	03	25	10	CX	KN	JR	DQ	IU	TL	HZ	MP	EP	WB	zfo	bjr	zwx	gvn
St	12.	I	III	II	26	01	18	QB	YE	WN	AI	GJ	TO	HR	FK	PS	CM	upc	anf	tkr	pwz
St	11.	V	I	III	17	13	04	SV	GO	PA	ZR	FN	HI	YM	WT	DE	BJ	vdh	ego	wmy	uti
St	10.	I	V	IV	26	07	16	SW	AQ	NP	FO	VY	UX	MK	CL	HT	ZJ	rpl	anw	vpr	mhn
St	9.	I	III	IV	17	10	18	EH	IK	GK	NZ	SP	UA	LD	CQ	JM	YV	knq	ysq	rhj	tlj
St	8.	V	II	I	23	11	25	QY	OG	ST	HA	CB	WD	KL	JN	VX	IU	lro	avw	axh	gws
St	7.	II	III	I	06	12	03	BG	FS	TH	JE	VK	PI	CU	QA	OD	NM	aty	mbb	mvo	jmz
St	6.	I	IV	V	24	19	01	IR	HQ	NT	WZ	VC	OY	GF	LP	BX	AK	bhc	iwo	zgz	rnr
St	5.	II	V	III	05	22	14	MK	GO	RQ	XT	DW	IA	ZL	SY	FJ	EN	bok	rzw	kzo	ryl
St	4.	IV	II	I	15	02	21	KD	FG	CO	PW	HJ	RY	MT	QL	VB	UZ	kpk	php	xmo	pfw
St	3.	III	V	IV	03	23	04	DY	CP	WN	OV	QH	UZ	RA	TI	GL	SM	hjy	nkt	ytn	pvc
St	2.	I	III	V	13	18	01	DB	VJ	FS	EK	IU	HX	AQ	GT	YO	PC	qpq	fqw	oiy	ruj
St	1.	II	IV	I	06	17	26	AC	LS	BQ	WN	MY	UV	FJ	PZ	TR	OK	ool	ooi	ywv	sfb

Fonte: http://users.telenet.be/d.rijmenants/pics/wehrmachtkey-stab.jpg

Figura 93 – Tabela de chaves da *Wehrmacht* Enigma



Geheim! 08 ❊

Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGS

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31.	I II V	10 14 02	BF SD AY HG OU QC WI RL XP ZK	yqv vuc xxo gvf
30.	V IV I	04 25 01	DI ZL RX UH QK PC VY GA SO EM	mqy vts gvt csx
29.	III V II	13 11 06	ZM BQ TP YX FK AR WH SO NJ DG	aky vdv oyo tzt
28.	I III II	09 16 12	NE MT RL OY HV IU GK FW PZ XC	nfh vco tur wnb
27.	III II I	06 03 15	BF GR SZ OM WQ TY HE JU XN KD	bec jmv vtp xdb
26.	I III V	19 26 08	GS VD CQ LR HI BO JP UZ FT RN	wvu yem buz rjk
25.	II I IV	05 01 16	KA ZH QP GR MF LJ OT EN BD YW	ktv muq cqm cpm
24.	III II IV	22 02 06	PI KM JB YU QS OV ZA GW CH XF	zcd iwo urp glg
23.	IV III II	08 11 07	SX TD QP HU FB YN CO IK WE GZ	epm mgz vqg vsm
22.	I V II	13 02 26	GP XH IW BO NU MD SA ZK QR LT	aam mvy jqq wqm
21.	IV I V	17 24 03	XC AQ OT UZ HD RG KM BL NS JW	ltl blu frk xrh
20.	IV I III	15 22 12	PO TV QC ZS EX WR BJ DK FU LA	non lic oxr usr
19.	V I III	13 24 21	HA GM DI VK JP YU EF TB ZL XQ	ecd ciq uvr ppt
18.	IV V I	23 09 20	XF PZ SQ GR AJ UO CN BV TM KI	fjh zts uqu cft
17.	III II V	21 24 15	UT ZC YN BE PK JX RS GF IA QH	oub sci pyf rqi
16.	IV III V	07 01 13	IN YJ SD UV GF BH TK QE AR OP	kex paw flw onw
15.	I IV II	15 04 25	TM IJ VK OY NX PR WL GA BU SF	sdr pbu byv khb
14.	III II IV	10 23 21	WT RE PC FY JA VD OI HK NX ZS	mhz lff lnq giy
13.	V I II	14 04 12	AN IV LH YP WM TR XU FO ZB ED	rqh ucm ldi ods
12.	II V I	07 19 02	HR NC IU DM TW GV FB ZL EQ OX	asy xza uvc fmr
11.	I V IV	13 15 11	NX EC RV GP SU DK IT FY BL AZ	gyd iuq ocb vef
10.	V II I	09 20 19	FN TA YJ SO EG PC VD KI XH WZ	pyz ace pru uyc
9.	I IV V	14 10 25	VK DW LH RF JS CX PT YB ZG MU	nyh fbd ohs jrp
8.	IV V I	22 04 16	PV XS ZU EQ BW CH AO RL JN TD	tck rts nro mkl
7.	V I IV	18 11 25	TS IK AV QP HW FM DX NG CY UE	mhw lwb mdm ybe
6.	IV I III	02 17 20	KZ FI WY MP DS HR CU XE QV NT	uwu vdk lrh mgd
5.	I V IV	26 09 14	VW LT PB FO ZK GS RI QJ PM XE	suw tsv nfp yjc
4.	IV III V	07 01 12	QS YA XW KR MP HT DU OV CL FZ	uby usi mhh mwb
3.	I II V	05 16 03	FW DL NX BV KM RZ HY IQ EC JU	tns von grw axl
2.	III I II	12 22 17	DW UO PY GR FS EQ KT CL AI ZB	smz lbl bkc sym
1.	I III II	04 18 06	ZN OM CR UI KP WQ SE JV LX TF	ghr vqv cya ayl

Fonte: http://users.telenet.be/d.rijmenants/pics/wehrmachtkey-bgs.jpg

Você pode se perguntar por que a ordem dos dias é invertida. A razão é bastante simples. O oficial, responsável pela entrega da chave para esse dia, poderia arrancar o dia atual na parte inferior da folha e entregá-la ao operador de rádio para configurar a máquina. Depois de ser usado, a tira de papel com a chave poderia ser destruída.

TABELA 18 - A tradução do título das colunas da tabela de chaves da *Wehrmacht* Enigma.

Sonder-Maschinenschlüssel	Chaves da máquina especial BGS
Datum	Data

Walzenlage	Posição do rotor
Ringstellunge	Posição dos anéis
Steckerverbindungen	Conectores
Kenngruppen	Grupos

Fonte: Elaborado pelo autor

Para identificar a chave que foi utilizada para uma mensagem específica, o operador teve que inserir um grupo de cinco letras chamado *Buchstabenkenngruppe* (grupo de identificação de letras) como o primeiro grupo da mensagem. O *Buchstabenkenngruppe* é composto por duas letras selecionadas aleatoriamente e um dos quatro *Kenngruppen* de três letras possíveis na folha de chave para esse dia. Se levarmos o dia 31 da chave do pessoal do Exército 28 (imagem X), vemos o *Kenngruppen* JKM, OGI, NCJ e GLP. Neste caso, alguns exemplos de um *Buchstabenkenngruppe* correto são FDJKM, KVOGI ou QNNCJ. Este grupo de cinco letras no início da mensagem não deve ser criptografado com o resto da mensagem. Se uma mensagem fosse dividida em várias partes, o operador precisava inserir outro Buchstabenkenngruppe para cada parte da mensagem. Ao contar as letras para o cabeçalho da mensagem, as cinco letras do *Buchstabenkenngruppe* devem ser incluídas. O operador receptor imediatamente reconheceu qual a chave a ser aplicada observando as últimas três letras do primeiro grupo (RIJMENANTS, 2016).

A configuração da máquina normalmente era válida por um dia. Usar as mesmas configurações para um grande número de mensagens aumentaria a quantidade estatística de dados para quebrar uma determinada chave. Portanto, cada mensagem foi enviada com uma nova posição inicial dos rotores Enigma, selecionados aleatoriamente pelo operador. Isso foi chamado de *Spruchschlüssel* ou chave de mensagem.

Antes de 1940, os militares alemães usavam a chave diária e a posição inicial, de acordo com a folha-chave. O operador selecionou uma chave de mensagem aleatória. Esta chave de mensagem foi codificada duas vezes, para excluir erros. Como exemplo, o trigrama GHK é codificado duas vezes, resultando

em XMC FZQ. Em seguida, o operador move os rotores para a chave de mensagem GHK e codifica a mensagem. Os dois trigramas, sendo a chave de mensagem codificada, foram transmitidos, juntamente com a mensagem. O receptor define a máquina na posição inicial, conforme descrito no livro de códigos, e decodifica os trigramas XMC FZQ novamente na mensagem GHK. Em seguida, ele define a chave de mensagem GHK como posição de início em sua máquina, para continuar decodificando o resto da mensagem. No entanto, esse procedimento foi realmente uma falha de segurança. A chave de mensagem é codificada duas vezes, resultando em uma relação entre primeiro e quarto, segundo e quinto e terceiro e sexto caractere. Além disso, muitas chaves de mensagem em um dia específico teriam a mesma configuração. Este problema de segurança permitiu que o *Polish Cipher Bureau* (Departamento de Cifras Polonês) quebrasse as mensagens de Enigma antes da guerra.

No entanto, os criptólogos alemães estavam cientes da falha de segurança e, a partir de 1940, a *Wehrmacht* mudou os procedimentos-chave da mensagem para aumentar a segurança. Os operadores de rádio da *Wehrmacht* selecionam para cada mensagem uma nova posição de início escolhida aleatoriamente ou *Grundstellung*, digamos WZA, e a mensagem de mensagem aleatória ou *Spruchschlüssel*, digamos SXT. Ele moveu os rotores para a fase de inicialização aleatória WZA e codificou a tecla de mensagem aleatória SXT. Vamos presumir que o resultado foi UHL. Ele configura a tecla de mensagem SXT como inicialização e codifica a mensagem. Em seguida, ele transmite a posição de início aleatório WZA, a chave de mensagem codificada UHL e a mensagem. O receptor configura a posição inicial de acordo com o primeiro trigrama WZA e decodifica o segundo trigrama UHL para obter a chave de mensagem SXT. Em seguida, ele usa a tecla de mensagem SXT como inicialização para decodificar a mensagem real. Se uma mensagem foi dividida em várias partes, o operador tem que inserir uma nova página de início na mensagem para cada parte da mensagem (RIJMENANTS, 2016).

Exemplo de uma típica mensagem da *Wehrmacht*:

1230 = 3tle = 1tl = 250 = WZA UHL =

FDJKM LDAHH YEOEF PTWYB LENDP

MKOXL DFAMU DWIJD XRJZY DFRIO

MFTEV KTGUY DDZED TPOQX FDRIU

CCBFM MQWYE FIPUL WSXHG YHJZE

AOFDU FUTEC VVBDP OLZLG DEJTI

HGYER DCXCV BHSEE TTKJK XAAQU

GTTUO FCXZH IDREF TGHSZ DERFG

EDZZS ERDET RFGTT RREOM MJMED

EDDER FTGRE UUHKD DLEFG FGREZ

ZZSEU YYRGD EDFED HJUIK FXNVB

A mensagem foi criada às 12h30, composta por três partes (3 *teile*), das quais esta é a primeira, e contém 250 caracteres (*Buchstabenkenngruppe* incluído). WZA é a posição inicial (*Grundstellung*) para decifrar a chave de mensagem criptografada (*Spruchschlüssel*) UHL. O *Buchstabenkenngruppe* FDJKM mostra que a chave que foi usada é aquela com *Kenngruppe* JKM (RIJMENANTS, 2016).

Verifique na figura 24 um exemplo de como as mensagens alemãs eram registradas para a realização da criptoanálise em *Bletchley Park*.

Procedimentos para enviar mensagens criptogradas da *Kriegsmarine*

Os procedimentos Kriegsmarine (Marinha de Guerra Alemã) sobre o envio de mensagens com a máquina de cifra Enigma foram muito mais complexos e elaborados do que os procedimentos da *Wehrmatch* e *Luftwaffe*. As folhas chaves *Kriegsmarine* Enigma consistiam em duas partes.

Parte 1) *Schlüsseltafel M Allgemein - Innere Einstellung* (configurações internas), continha os três rotores e suas configurações de anel, rotor beta ou gama e o refletor, e isso apenas para os dias ímpares de um mês. Verifique no anexo J.

Parte 2) *Schlüsseltafel M Allgemein - Aussere Einstellung* (configurações externas), continha as fichas e *Grundstellung* (posição básica inicial) para cada dia do mês. Verifique no anexo K.

Uma chave adicional existia para os oficiais e um *Schlüssel* M NIXE especial foi usado para comunicação privada entre o capitão e o comando do *U-boat*, sem que outros *U-boats* pudessem ler a mensagem.

O sistema *Kriegsmarine* de *Kenngruppen* era completamente diferente do sistema da *Wehrmatch* e *Luftwaffe Kenngruppen*. Além das folhas-chave, a *Kriegsmarine* usou um *Kenngruppenbuch* em suas redes de cifra principais para determinar a chave da mensagem. Este *Kenngruppenbuch* não deve ser confundido com o *Kenngruppenheft* para sinais curtos, que tem um propósito completamente diferente. O *Kenngruppenbuch* continha as seguintes partes:

Parte 1) *Zuteilungsliste* (uma lista de alocação) que informa ao operador qual tabela ele deve usar para uma determinada rede de cifra. Esta lista consiste em duas partes. A primeira parte mostra o número da tabela, dado o nome das redes de cifra, e a segunda parte mostra as diferentes redes de cifra, dado o número da tabela.

Parte 2) *Tauschtafelplan* (ponteiro da tabela) informou ao operador qual coluna de uma determinada tabela foi usada para selecionar os trigramas necessários.

Parte 3) *Spalten* (colunas) com o *Kenngruppen* (grupo de indicadores e criptografia).

O operador teve que selecionar dois das três grades de três letras ou trigramas do Kenngruppenbuch:

Procedimento 1) *Schlüsselkenngruppe* (grupo indicador chave) para identificar qual chave foi usada;

Procedimento 2) *Verfahrenkenngruppe* (grupo de indicadores de criptografia) para obter a chave da mensagem.

Tanto *Schlüsselkenngruppe* quanto *Verfahrenkenngruppe* tinham suas próprias mesas determinadas no *Zuteilungsliste*.

Com a máquina Enigma no *Grundstellung* (a posição básica para esse dia), o operador digitou o *Verfahrenkenngruppe*. O resultado seria a chave de mensagem, usada como posição inicial para cifrar a mensagem. Os dois trigramas juntos (*Schlüsselkenngruppe* e *Verfahrenkenngruppe*) formam o indicador de mensagem.

Finalmente, este indicador de mensagem sofreu uma criptografia de substituição adicional com uma tabela de bigrama chamada Doppelbuchstabentauschtafel ou tabela de conversão de letras duplas.

O Exército alemão e a Força Aérea Alemã transmitiam suas mensagens em grupos de cinco letras. Para tornar a decifragem mais difícil, era proibido o uso de mais de 250 caracteres em uma única mensagem. As mensagens mais longas eram divididas em várias partes, cada uma com sua própria chave de mensagem. A máquina Enigma processava apenas letras, logo os números e a pontuação eram substituídos por combinações de letras raras (RIJMENANTS, 2016).

O Exército alemão usava as seguintes abreviaturas:

KLAM = parêntese ZZ = vírgula

X = fim de sentença YY = ponto

X **** X = aspas

O ponto de interrogação (Fragezeichen, em alemão) era abreviado para FRAGE FRAGEZ ou FRAQ.

Nomes estrangeiros, locais, etc, eram delimitados por duas vezes "X" como em XPARISXPARISX.

As letras CH eram escritas Q. ACHT (oito, em alemão) tornava-se AQT, RICHTUNG (direção, em alemão) tornava-se RIQTUNG.

Números eram escritos como NULL (zero), EINZ (um), ZWO (dois), DREI (três), VIER (quatro), FUNF (cinco), SEQS (seis), SIEBEN (sete), AQT (oito), NEUN (nove).

Era proibido cifrar a palavra "NULL" várias vezes em sucessão. Usava-se no lugar CENTA (00), MILLE (000) e MYRIA (0000). Exemplos: 200 = ZWO CENTA, 00780 = CENTA SIEBEN AQT NULL.

A Marinha de Guerra alemã formatava suas mensagens em grupos de quatro letras. Eram utilizadas as seguintes abreviaturas: (RIJMENANTS, 2016).

X = período

Y = vírgula

UD = ponto de interrogação XX = dois pontos

YY = traço, hífen

KK ** KK = parênteses

J ****** J = acentuação (CRYPTO, 2016).

3.5 Desvantagens da máquina de cifragem Enigma

a) Uma letra não pode ser codificada nela mesma

Uma das principais propriedades do projeto da Enigma era o fato de que uma letra não podia ser cifrada nela mesma. Quando a letra Z, por exemplo, era pressionada, cada lâmpada no painel de lâmpadas podia ser acesa, exceto a letra Z. Esta propriedade é causada pelo uso do refletor (UKW).

b) Passos regulares das rodas

Na maioria das máquinas Enigma, a roda mais à direita precisava completar uma volta completa antes que a roda esquerda seja movida em uma posição. Como resultado, a roda 2 daria um passo apenas uma vez a cada 26 caracteres e a roda 3 quase nunca se moveria. Isso fazia com que o Enigma ficasse mais previsível. Algumas variantes da Enigma (como a Enigma T), no entanto, tinham múltiplos entalhes de movimento, e a Enigma G tinha um mecanismo de roda dentada que causava passos irregulares.

c) Passos duplos no rotor do meio

Sob certas circunstâncias, o rotor do meio podia dar dois passos ao serem pressionadas duas teclas subsequentes. Isso reduzia pela metade o período da cifra.

d) Roda 4 fixa da Enigma M4

Na Enigma M4 naval, a roda extra (Zusatswalze) podia ser configurada em qualquer uma de 26 posições no início da mensagem. Durante a criptografia, no entanto, a roda não se movia. Junto com o UKW (refletor), esta roda pode ser considerada como uma seleção entre 26 refletores diferentes.

e) Dois entalhes nas rodas extras navais

As três rodas extras navais (VI, VII e VIII) tinham cada uma dois entalhes, para causar um movimento mais frequente das rodas. No entanto, como 2 é um primo relativo de 26, e porque as duas ranhuras eram posicionadas de maneiras opostas, o período de cifra é reduzido para metade.

f) Uso obrigatório de rodas navais extras

O operador podia escolher todo dia quaisquer três entre as 8 rodas disponíveis. Em teoria, havia 336 ordens possíveis diferentes de escolha. Na prática, contudo, a Marinha foi instruída a usar pelo menos uma roda adicional a cada dia (VI, VII ou VIII), e de que a roda selecionada não poderia ser utilizada dois dias consecutivos.

g) Número fixo de cabos no painel de plugues (*Steckerbrett*)

O *Steckerbrett* tinha 26 soquetes, um para cada letra do alfabeto, e cabos eram usados para trocar pares de letras. Se um cabo era omitido, esta letra não era trocada. Em teoria, o número de cabos podia variar entre 0 e 13 mas, na prática, os procedimentos ordenavam a utilização de um número exato de cabos todas as vezes (CRYPTO, 2016).

Figura 94 – General alemão *Heinz Wilhelm Guderian*

Fonte:http://cdnlive.warthunder.com/uploads/df/11/71/d08ff460a6ae5fad6c928df2463c404d00_lq/guedrian%20Enigma(11).jpg

Na figura 94, é possível ver o General Alemão *Heinz Wilhelm Guderian* em seu veículo de comando durante a Batalha da França. O General *Heinz Guderian* (de pé), ao seu lado esquerdo vemos o operador de rádio recebendo as mensagens cifradas pela máquina Enigma do remetente. O operador da máquina Enigma verifica as configurações e coloca a mesma configuração da outra máquina Enigma e dessa maneira é possível digitar as mensagens cifradas e revelar o verdadeiro significado das mensagens. Com a adoção da estratégia de *Blitzkrieg* ou guerra relâmpago, que consistia em ações conjugadas entre o exército, marinha e

aeronáutica, os alemães precisavam de um sistema de comunicação extremamente versátil e seguro para evitar que os inimigos conseguissem interpretar as mensagens e anular as estratégias de combate. No início da Segunda Guerra Mundial, os alemães alcançaram inúmeras vitórias no campo de batalha graças ao uso da máquina de cifragem Enigma e o uso de criptografia para tornar as mensagens ininteligíveis para os inimigos.

Figura 95 – Oficiais alemães utilizando a máquina Enigma

Fonte: http://www.ww2incolor.com/d/84779-4/en7

A máquina de cifragem Enigma poderia ser usada em praticamente qualquer lugar do campo de batalha. Sua portabilidade lhe permitia acompanhar as tropas para enviar e receber mensagens de outras tropas. Geralmente duas pessoas eram suficientes para operar a máquina de cifragem Enigma. Um operador de rádio recebe as mensagens pelo rádio, anota a mensagem cifrada e entrega pro operador da máquina Enigma que digita a mensagem. O operador do rádio registra a mensagem original em um formulário. A mensagem é entregue ao oficial local.

3.6 Máquinas cifrantes

Os britânicos e americanos, porém, haviam desenvolvido um sistema mecânico de codificação baseado no modelo Enigma. A máquina britânica era conhecida como *Typex*, ou às vezes *Typex-X*; o aparelho americano chamava-se *Sigaba*. As duas máquinas eram complexos sistemas de substituição e soma mecânicas usando um sistema de cinco rotores. A existência desses aparelhos não era segredo. Havia uma referência aberta a eles num ensaio escrito por *Abraham Sinkov,* um criptoanalista da marinha dos Estados Unidos publicado em *Mathematical Recreations and Essays* [Recreações e ensaios matemáticos], de *Rouse Ball*. *Sinkov* comentava que, “no que diz respeito aos atuais métodos criptoanalíticos, os sistemas de cifras derivados de algumas dessas máquinas estão muito próximos da insolubilidade prática” (SINKOV apud CORNWELL, 2003, p. 253).

Figura 96 – Máquina de cifragem SIGABA

Fonte: http://www.cryptomuseum.com/crypto/usa/sigaba/img/300354/100/full.jpg

Os primeiros dispositivos que podem ser chamados de máquinas cifrantes são os baseados em princípios eletromecânicos. As máquinas mais famosas foram usadas durante a Segunda Guerra Mundial e, entre elas, destacam-se a SIGABA (ou ECM Mark II ou CSP-888/889) da Marinha dos Estados Unidos, a Púrpura usada no serviço diplomático japonês (chamada de 97-shiki-O-bun In-ji-ki, que significa máquina de escrever alfabética de 97, onde o 97 se refere ao ano de 2597 dos japoneses que corresponde a 1937) e a Enigma. A mais conhecida, sem dúvida alguma é a máquina Enigma que, mesmo sendo antiga, é a que continua despertando o maior interesse porque, apesar de o princípio de funcionamento ser bastante simples, seu sistema criptográfico tornou-se um dos mais elaborados da história (TKOTZ, 2005, p. 246).

Figura 97 – Máquina de cifragem Typex

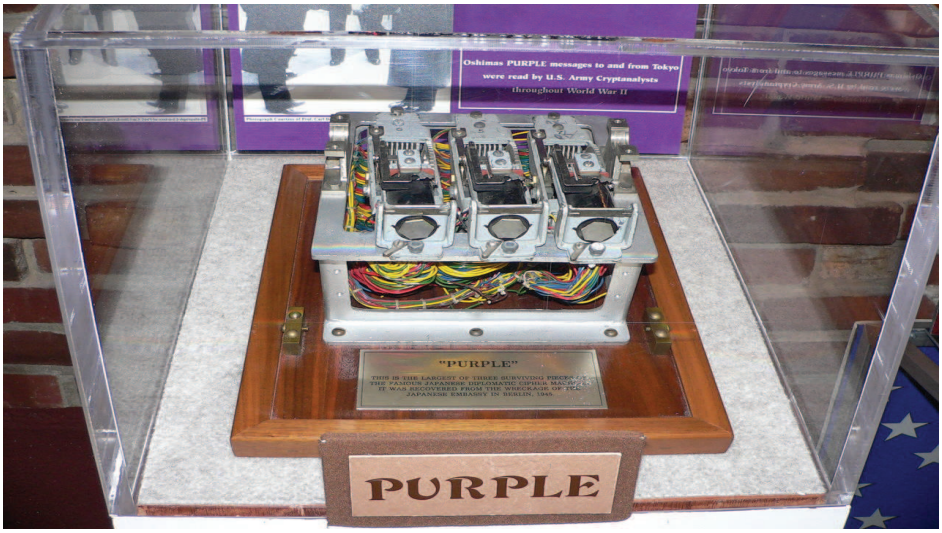
Fonte: http://www.cryptomuseum.com/crypto/uk/typex/img/300703/181/full.jpg

2.6.1 Máquina de cifragem PÚRPURA

A máquina de cifragem Púrpura tinha algumas características diferentes das outras máquinas de cifragem como a SIGABA, Typex e Enigma. A primeira é por apresentar um botão de fase como elemento criptográfico. A máquina Púrpura usava a divisão das letras em seis vogais (com a letra Y) e 20 consoantes. O algoritmo (veja definição no próximo parágrafo) usado para cifrar os dois grupos de caracteres também era diferente. O botão de fase (unisseletor) conectava um terminal de entrada com um dos 25 terminais de saída. Um imã elétrico, anexado ao unisseletor, avançava o "carro" que continha as letras para sua posição seguinte, ou seja, da saída um para a saída dois quando era aplicado um pulso elétrico. Desta forma, o resultado seria a obtenção de até 25 alfabetos cifrados diferentes. A máquina ainda dispunha de quadros de *plugs* de entrada e saída para embaralhar os alfabetos (CRYPTO, 2016).

Segundo Pinto (1990), "um algoritmo é um texto (do tipo receita de bolo) onde cada linha contém uma ação primitiva (ação elementar, passível de execução por um humano ou uma máquina). A função do algoritmo, quando executado, é a de agir (operar) sobre os dados, transformando-os em informações (algumas vezes denominada de dados ou dados operacionais)".

Figura 98 – Máquina de cifragem Púrpura



Fonte: http://s26.postimg.org/owzfcrg09/Purple_code_machine_2.jpg

Era possível conectar máquinas de escrever em qualquer entrada na máquina Púrpura. Se fosse digitada na máquina de escrever a letra “E” e estivesse ligada na entrada da letra “O”, a letra resultante seria cifrada como uma das seis. Se a letra “E” estivesse ligada na letra “C”, seria cifrada com uma das 20. Já as 20 letras são cifradas em três fases do botão. Utilizando o unisseletor uma vez, avançava a cada letra cifrada, então os alfabetos não se repetem até que 15.625 (25 x 25 x 25) letras sejam por sua vez cifradas.

A máquina Púrpura começou a ser usada no Japão em junho de 1938, mas os criptoanalistas estadounidenses e britânicos só conseguiram decifrar algumas mensagens pouco antes do ataque japonês (7 de dezembro de 1941) à base naval dos Estados Unidos que fica em *Pearl Harbor* no arquipélago do Havaí.

Durante a Segunda Guerra Mundial, o embaixador japonês em Berlim, Baron Oshima, enviou informações sobre os militares alemães para Tóquio utilizando mensagens cifradas pela máquina Púrpura via rádio.

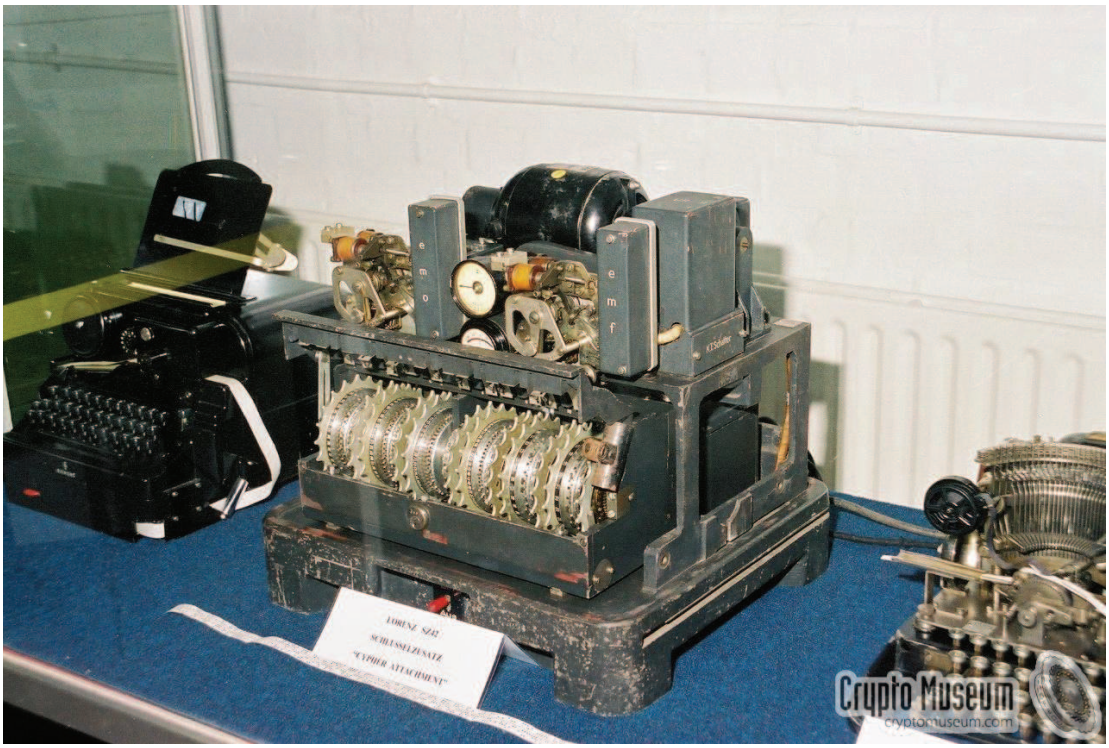
Outro episódio “desastroso” para os alemães foi quando *Oshima* enviou um relatório sobre as fortificações da “Muralha do Atlântico” que visava impedir o desembarque dos Aliados na Holanda até o norte da França. Sem que os alemães e japoneses soubessem, o embaixador relatava aos Aliados muitos dados que ajudaram na preparação do “Dia D” desembarque dos Aliados na Normandia (norte da França) no dia 06 de junho de 1944. Como *Oshima* utilizava a máquina de cifragem Púrpura via rádio, todas as mensagens eram interceptadas e decifradas pelos britânicos e estadounidenses (COUTO, 2008, p. 186).

3.6.2 Máquina de cifragem *Lorenz*

Além da máquina de cifragem Enigma, os alemães utilizavam uma outra máquina de cifragem chamada Lorenz. Geralmente era utilizada pelo alto comando alemão OKW (*Oberkommando der Wehrmacht*). A *Lorenz* funcionava da seguinte forma.

Era um enorme instrumento de precisão com doze reluzentes rotores de aço envoltos em ferro fundido; é pesado, frágil, e precisa de muita gente para suspendê-lo. A máquina, que recebeu o nome da empresa que a fez, mandava suas mensagens por fios terrestres de teletipo (embora pudesse usar também as ondas aéreas), empregando o sistema internacional de sinais digitais de cinco bits, composto de buracos e espaços para representar letras do alfabeto. O código tipo Lorenz usava dois conjuntos de aditivos para confundir. Cada caractere original digitado era mudado acrescentando-se a ele dois conjuntos de caracteres gerados pela máquina. Dessa maneira, os alemães conseguiam obscurecer cada mensagem perfurada original num total de 10^{19} possibilidades.

Figura 99 – Máquina de cifragem Lorenz



Fonte: http://www.cryptomuseum.com/crypto/lorenz/sz40/img/301491/000/full.jpg

A configuração das engrenagens de cifra envolvia mover minúsculos “pesos” mecânicos, 501 ao todo, para um padrão específico mas regularmente alterado, dado pelos codificadores alemães. Os alemães estavam convencidos de que o

código da Lorenz era indecifrável. Como exemplo de sua fé, não apenas deixavam *Hitler* falar diretamente com seus generais usando a máquina, mas em duas ocasiões chegaram a mandar folhas de configuração de código para o mês seguinte na própria máquina *Lorenz*.

Para decifrar uma mensagem codificada na *Lorenz*, o recebedor alemão precisava passar a fita perfurada cifrada numa máquina *Lorenz* idêntica, com as engrenagens configuradas para as mesmas posições de “engrenagem de partida” ordenada em qualquer dia determinado. Essas posições de engrenagem de partida determinavam as configurações das engrenagens como uma roleta “preparada” para girar e parar no que parece uma posição inteiramente aleatória. As posições de partida eram mudadas todo mês a princípio, mas com o avanço da guerra os alemães alteravam toda semana, e por fim todo dia (CORNWELL, 2003, p. 257).

3.7 Era dos Computadores

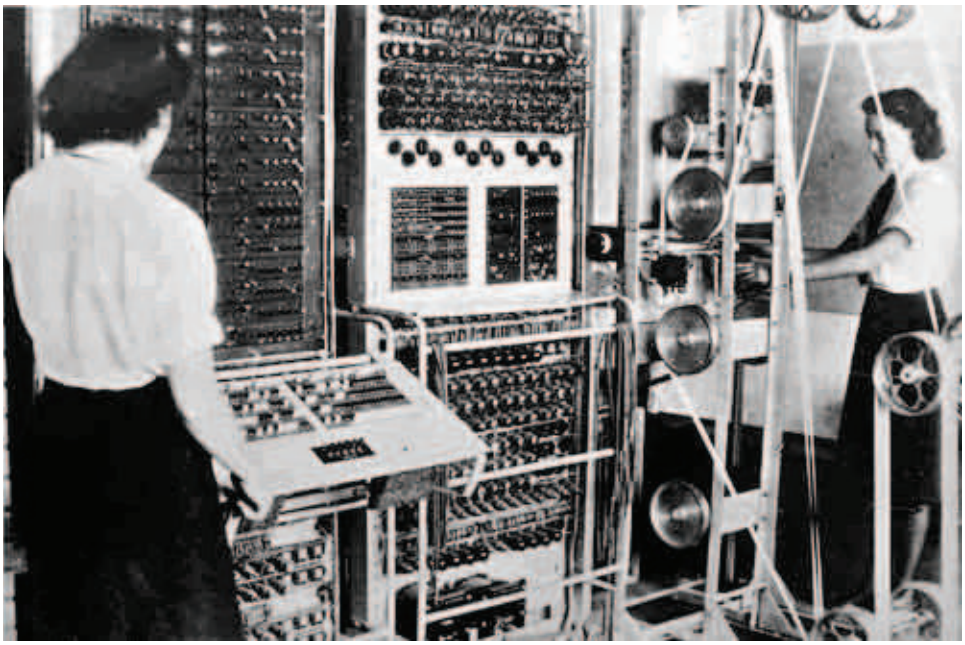
Além da corrida armamentista entre alemães e ingleses, existia a corrida pelos artefatos tecnológicos modernos como os computadores Colossus (inglês) e o computador Z3 (alemão).

3.7.1 Computador *Colossus* (inglês)

Em Londres, num barracão de guerra que agora é museu, encontra-se uma engenhoca que zumbe, estala e chia. A máquina exsuda um fedor ácido de baquelite quente e válvulas eletrônicas, e parece haver sido armada com grandes peças de brinquedos de montar e uma variedade de restos de uma mesa telefônica da década de 1930. São dois armários compostos de painéis, interruptores e guirlandas de fios coloridos, e a coisa toda chega a cerca de três metros de altura, um pouco de largura e uns seis de comprimento. Uma plataforma de aço com reluzentes carretéis faz correr um pedaço de fita de telégrafo por um “olho”

fotoelétrico que lê a informação num ritmo de 5 mil caracteres por segundo. Nas entranhas da máquina, 1.500 válvulas e milhares de plugues e circuitos tremulam e chiam ao processarem a informação da fita.

Figura 100 – Computador Colossus



Fonte: http://www.cryptomuseum.com/crypto/colossus/img/colossus_full.jpg

O *Colossus* foi construído para fazer cálculos “booleanos”: um método de trabalhar com processos lógicos usando símbolos; em outras palavras, expressar ideias como “verdadeiro,falso”, ou “e, ou”, puramente em termos binários de zeros e uns, ou sinais ligado/desligado [on/off]. A inspiração por trás de sua criação muito se deve ao gênio de Alan Turing, o matemático de Cambridge que “inventou” a ideia do computador como uma “experiência de pensamento”, para enfrentar problemas matemáticos por meios mecânicos. Tecnicamente conhecido como “grande calculador lógico programável de válvula eletrônica”, o *Colossus* foi construído para decodificar mensagens da máquina de Lorenz, que embaralhava mensagens de teletipo entre membros do alto comando nazista, incluindo diretivas do próprio Hitler. Cornwell (2003) afirma que, de acordo com historiadores alemães, a informação reunida pelo Colossus, a partir de 1941, encurtou a guerra em pelo menos 2 anos. O

escritor militar alemão *Hans Meckel* acredita que o *Colossus* impediu a Alemanha de ser bombardeada até a submissão como aconteceu com o Japão com uma bomba atômica (CORNWELL, 2003, p. 256).

O *Colossus* foi projetado para descobrir a posição da engrenagem de partida usada nas máquinas *Lorenz* em qualquer dia determinado. Mas os decifradores de código britânicos também tiveram de recriar uma máquina idêntica às funções da própria *Lorenz* para decifrar a mensagem. A versão britânica da máquina *Lorenz*, conhecida como "*Tunny*" [atum] (todas as cifras de teletipo eram apelidadas com nomes de peixes pelos britânicos), foi projetada por engenheiros que estudaram o sistema de cifras da *Lorenz* sem jamais terem visto um exemplo do original alemão. Como os britânicos conseguiram improvisar o primeiro computador do mundo, e a máquina "*Tunny*" que o acompanhava, muito se deve a uma peculiar conjunção de gênio matemático e engenharia.

O tráfego de linhas terrestres de teletipo era praticamente impossível de interceptar em território ocupado pelos nazistas, mas os mesmos sinais eram de vez em quando transportados pelas ondas aéreas em forma de sinal alto para um espaço e de sinal baixo para um ponto, criando um código binário. Próximo ao fim da guerra, os britânicos e os americanos, e a Resistência, visavam linhas terrestres e estações de transmissão de teletipo exatamente para forçar mais tráfego nas ondas aéreas, onde podiam ser interceptadas.

A primeira brecha para a compreensão da natureza da cifra *Lorenz* ocorreu a 30 de agosto de 1941, quando deram a um operador alemão uma mensagem com 3.900 caracteres para enviar por transmissão de rádio. Ele configurou corretamente sua máquina *Lorenz* e digitou a mensagem à mão. Então o recebedor respondeu que o texto não passara e pediu que fosse reenviado. Nesse ponto, cometeu-se um erro fatal. Os dois operadores puseram suas *Lorenz* de volta ao mesmo padrão de posição de engrenagem inicial e o operador que transmitia bateu mais uma vez a mensagem na mesma configuração.

O fenômeno de uma mensagem repetida desse tipo era apelidado de "vau" pelos decifradores de código. Os dois fluxos de cifras haviam sido interceptados na

estação receptora em *Knock-holt*, em *Kent*, e passados para *Bletchley Park* (CORNWELL, 2003, p. 258).

O que o computador *Colossus* fez, em resumo, foi gerar os fluxos de chaves, isto é, a sequência de símbolos das engrenagens da máquina Lorenz alemã. Ele lê a mensagem interceptada à velocidade de 5 mil caracteres por segundo, comparando a fita do texto cifrado interceptado com os fluxos de chaves internamente representados. Depois, efetuando algumas sofisticadíssimas correlações cruzadas, descobre as posições de engrenagem de partida para aquela mensagem cifrada.
A informação processada pelo computador *Colossus* assegurou aos Aliados que *Hitler* acreditava que um grande ataque para invadir o continente viria por *Pas de Calais* (França).

O computador *Colossus* também decifrou mensagens do Marechal-de-Campo *Karl von Rundstet*, após o "Dia D", ordenando que os generais alemães mantivessem as divisões Panzer em reserva na Bélgica, em vez de soltá-las sobre os exércitos aliados no sul. Isso deu a estes maior confiança para consolidar a invasão sem desviar forças para conter um ataque de tanques em grande escala (CORNWELL, 2003, p. 260).

3.7.2 Computador Z1 (alemão)

O engenheiro alemão *Konrad Zuse* (1910-1995) criou uma máquina baseada na calculadora de *Charles Babbage* (1791-1871) que operava com dois estados ("sim" e "não") e cartões perfurados. *Zuse* apresentou em seu projeto a divisão entre o que era *hardware* (parte física) e o que era *software* (parte lógica) (MATO, 2016, p. 185).

Entre 1935-1938, *Konrad Zuse* construiu o Z1, o primeiro computador controlado por programa do mundo. Apesar de certos problemas de engenharia mecânica, tinha todos os ingredientes básicos das máquinas modernas, usando o sistema binário e a separação padrão de armazenamento e controle de hoje. O pedido de patente de 1936 de *Zuse* (Z23139 / GMD Nr. 005/021) também sugere uma arquitetura de *von Neumann* com programa e dados modificáveis em armazenamento. Em 1941, *Zuse* completa o Z3, o primeiro computador programável

totalmente funcional do mundo. Em 1945: *Zuse* descreve *Plankalkuel*, a primeira linguagem de programação de nível superior do mundo, contendo muitos recursos padrão das linguagens de programação atuais. A linguagem de programação FORTRAN chegou quase uma década depois. *Zuse* também usou *Plankalkuel* para projetar o primeiro programa de xadrez do mundo (JÜRGEN SCHMIDHUBER, 2017, Trad. nossa).

Figura 101 – Konrad Zuse e o computador Z1

Fonte: http://people.idsia.ch/~juergen/zuse4.jpg

Explicamos, neste capítulo, o desenvolvimento de máquinas de cifragem na primeira metade do século XX, com ênfase no período da Segunda Guerra Mundial, com riqueza de detalhes técnicos. Destacamos como um livro publicado em 1923, de autoria de *Winston Churchill*, revelou a maneira como os britânicos se apossaram dos códigos navais secretos da Alemanha durante a Primeira Guerra Mundial, fatos muitas vezes desconhecidos por muitos alemães, mesmo após 5 anos do término do

conflito. Essa descoberta fez os militares alemães desenvolver um complexo sistema de inteligência consubstanciado nos diversos modelos da máquina Enigma.

Mais de 50 modelos da Enigma foram desenvolvidos, segundo TKOTZ (2005) e foram fabricadas entre 100.000 e 200.000 máquinas, vendidas para alguns países como Itália, Hungria e Espanha. Só o governo japonês encomendou 800 Enigma T (codinome Tirpitz) mas não recebeu esse montante devido a dificuldade de obtenção dos materiais durante a guerra e também pelo fato de alguns submarinos alemães terem sido afundados antes da entrega das máquinas. Em 1943 uma Enigma T foi capturada em Guadalcanal pelas forças aliadas capitalistas.

Mostramos como era feita a comunicação alemã-japonesa através da Enigma T e como a marinha dos Estados Unidos se referia à máquina como Opal e o tráfego do sistema da máquina como Código de Uso Conjunto Japão/Alemanha nº 3.

No confronto de sistemas de inteligência verificado no decorrer da Segunda Guerra Mundial, os britânicos desenvolveram uma máquina conhecida como *Typex* e os americanos fabricaram outra denominada SIGABA. Os japoneses usavam, desde 1938 a máquina Púrpura mas os americanos e britânicos só conseguiram decifrar algumas mensagens em 1941. Além da máquina de cifragem Enigma, os alemães utilizaram outra máquina de cifragem chamada *Lorenz*.

Desenvolvida durante a Segunda Guerra Mundial, a máquina de cifragem *Lorenz* era utilizada pelo alto comando alemão, *Hitler* se comunicava diretamente com seus generais usando a máquina de cifragem *Lorenz.*

A portabilidade da máquina Enigma permitia aos militares usar a máquina no campo de batalha, com apenas dois operadores. Apesar do funcionamento relativamente simples, a máquina Enigma tinha o sistema criptográfico extremamente elaborado que despertava o maior interesse e dificuldade de decodificação, o que ajuda a explicar o esforço dos britânicos para o lançamento do *Colossus*, considerado o primeiro computador eletrônico do mundo. As mensagens alemãs decifradas pelo computador *Colossus* contribuíram para o êxito aliado na invasão do “Dia D”, que foi um dos eventos decisivos para o final da guerra na Europa.

4 Considerações Finais

Identificamos no Egito Antigo o surgimento da criptografia através das primeiras técnicas para a ocultação de mensagens.

A mitologia grega mostra o personagem Édipo adivinhando um enigma que a esfinge lhe propôs. Se Édipo errasse a resposta, seria destruído pela esfinge. Pode-se fazer uma analogia entre o código secreto da máquina de cifragem Enigma com os enigmas da esfinge. Decifra-me ou lhe devorarei. Decifre o código da máquina de cifragem Enigma ou será destruído. Outra abordagem seria de que todas as cifras criadas para ocultar o verdadeiro significado das mensagens seria um enigma para ser decifrado (desvelado).

Ao historiador grego Políbio é atribuída a invenção de um sistema criptográfico de transliteração de letras em números. A cifra de Políbio como é conhecida foi criada por *Cleoxeno* e *Democleto.* A cifra de Políbio foi utilizada até o século XIX.

Com o passar dos séculos os métodos de codificação e de decodificação sofreram um processo de diversificação e complexificação. A atual Associação Internacional para a Pesquisa Criptológica, organização científica que coordena a pesquisa na área, considera a Criptologia (criptografia + criptoanálise) como ciência e não mais como arte, como era antigamente.

Na história recente da criptografia, parte mais substantiva desta dissertação analisamos a Primeira Guerra Mundial, com os métodos de decodificação, o Tratado de Versalhes e o período entre guerras, com destaque para a Segunda Guerra Mundial.

Na Primeira Guerra Mundial explicitamos o exemplo do tenente francês Georges Painvain que conseguiu decifrar algumas mensagens criptografadas pelos alemães que utilizavam a cifra ADFGVX. Painvain utilizou análise de frequência estatística até conseguir decifrar algumas mensagens alemãs e ajudar o alto comando Aliado a reposicionar os exércitos para evitar a tomada de Paris pelos alemães.

No período entre-guerras os poloneses conseguiram acumular experiências na área de criptografia quando decifraram os códigos secretos dos russos e conseguiram expulsá-los de seu território. Mesmo com o sucesso na guerra russo-polonesa, os poloneses continuaram a monitorar os países vizinhos principalmente a Alemanha que devido ao Tratado de Versalhes foi obrigada a ceder territórios para os poloneses depois da Primeira Guerra Mundial. Os criptoanalistas poloneses (*Marian Adam Rejewski, Jerzy Witold Różycki* e *Henryk Zygalski*) foram os primeiros a conseguir decifrar o código da máquina de cifragem Enigma dos alemães. Os poloneses criaram uma máquina chamada "bomba criptológica" que permitia decifrar, por tentativa e erro, mensagens processadas pela máquina de cifragem Enigma. Pouco antes da invasão alemã ao território polonês, *Rejewski* e sua equipe fugiram para a França. E antes dos alemães invadirem a França, eles se deslocaram para a Inglaterra onde compartilharam seus conhecimentos com os criptoanalistas britânicos de *Bletchley Park*.

Este trabalho demonstra como o domínio da informação pelos ingleses foi crucial durante a Segunda Guerra Mundial. Os alemães tinham a rede de comunicações mais segura do mundo no início deste conflito. No campo de batalha os alemães criaram uma nova estratégia chamada de "*blitzkrieg*" ou guerra relâmpago. Desta forma o inimigo fica confuso pois com uma combinação de veículos blindados, tanques de guerra, aviação e divisões secundárias atuando em sincronismo e alguns casos com a marinha de guerra alemã juntamente com comunicações via rádio criptografadas pela máquina de cifragem Enigma, tornaram as Forças Armadas alemãs imbatíveis no período (1939-1941). Com as conquistas dos alemães sobre os aliados da Grã-Bretanha na Europa (França, Bélgica e Holanda), o país ficou isolado dependendo dos comboios de suprimentos vindos de suas colônias e principalmente dos Estados Unidos da América. Inicialmente os alemães bombardeavam somente alvos militares como pontes, entroncamentos ferroviários, portos, aeródromos da *Royal Air Force* – Força Aérea Real Britânica, fábricas em geral e bases militares. Este episódio ficou conhecido como a Batalha da Inglaterra (1940-1941). Quando os alemães estavam quase conseguindo a vitória nos céus da Inglaterra, a estratégia mudou e os bombardeiros alemães começaram a jogar suas bombas nas cidades em vez de alvos militares. Isto deu novo fôlego para restaurar os aeródromos e fábricas de aviões ingleses. O fato mais importante

deste período foram as mensagens decifradas dos alemães pelos criptoanalistas de *Bletchley Park*. Era possível saber a quantidade de aviões e as coordenadas do ataque aéreo.

Os Alemães tinham diferentes objetivos militares dos italianos e japoneses. Por exemplo: os alemães só comunicaram os italianos que o ataque à União Soviética tinha começado no primeiro dia da invasão no dia 22 de junho de 1941. Os italianos invadiram o Egito sem consultar os alemães e os japoneses não informaram os alemães e italianos do ataque à base naval estadounidense de Pearl Harbor no Havaí no dia 07 de dezembro de 1941 obrigando os Estados Unidos a entrar na Segunda Guerra Mundial junto com a Grã-Bretanha e União Soviética. Outro problema foi a falta de padronização das comunicações dos países do Eixo. Os japoneses só começaram a usar a máquina Enigma em 1942 depois da Batalha de *Midway* (4 a 7 de junho de 1942) e os italianos estavam usando a máquina Enigma comercial e suas mensagens eram facilmente decifradas pelos países Aliados.

Segundo Tkotz (2005) foram desenvolvidas mais de 50 modelos da máquina de cifragem Enigma e fabricadas entre 100.000 e 200.000 máquinas. As máquinas Enigma comerciais foram colocadas no mercado. Os modelos usados no sistema de inteligência recebiam configurações que eram segredo de Estado. Alguns desses modelos foram vendidos para equipar a marinha da Itália, da Holanda, o exército da Hungria e do Japão. Foram vendidas também para a Espanha e a Suíça.

Enfatizamos como a Segunda Guerra Mundial foi, dentre outras razões, um confronto de sistemas de inteligência, com o desenvolvimento de máquinas de cifragem cada vez mais complexas como a *Lorenz*, do alto comando alemão.

O cientista e matemático inglês *Alan Turing* foi designado pelo governo Britânico junto com uma equipe de cientistas e linguistas para decifrar o código das máquinas de cifragem Enigma e Lorenz dos alemães. De posse de uma máquina Enigma capturada pelos poloneses em Berlim, os cientistas Ingleses começaram um trabalho para decifrar o código da máquina Enigma que mudava todo dia exatamente a meia-noite. Os cientistas Ingleses conseguiram decifrar algumas palavras pela análise de frequência da distribuição das letras mas o volume de

informações diária tornava a tarefa quase impossível. As mensagens alemãs sempre começavam com cinco letras aleatórias mas alguns operadores alemães colocavam nomes próprios no início das mensagens e com isso as mensagens poderiam ser decifradas pela posição das letras e gerar a chave criptográfica do dia.

Sob o nome código Ultra que foi um dos maiores serviços de inteligência da história, os Ingleses puderam decifrar diversas mensagens criptografadas pela máquina de cifragem Enigma alemã. Outra questão em jogo seria escolher alguns ataques contra os alemães para que eles não desconfiarem que o código da máquina de cifragem Enigma tinha sido decifrado.

Decifrar o Código Enigma contou com o esforço de milhares de criptoanalistas e à fabricação do primeiro protótipo de um grande computador chamado *Colossus* em 1943. A Inglaterra manteve essa parafernália tecnológica oculta até 1975, mas o algoritmo utilizado permanece secreto (MATO, 2016, p. 180).

Os alemães conseguiram desenvolver em 1941, o computador Z3, o primeiro computador programável totalmente funcional do mundo. *O* engenheiro alemão *Konrad Zuse* foi o responsável por este projeto mas somente a indústria aeronáutica se interessou. Se os alemães tivessem colocado o computador Z3 para decifrar códigos criptográficos dos Aliados, o resultado da Segunda Guerra Mundial teria sido diferente.

Atualmente, *Bletchley Park*, ao norte de Londres, funciona como museu e ali é possível ver o *Colossus*, uma máquina de 5 metros de comprimento e 2 metros de altura. A construção do *Colossus* foi baseada em um sistema binário inspirado nos princípios de *Alan Turing*. Enquanto o *Colossus* I tinha 1500 válvulas, a *Colossus II* teve 2400 válvulas e a fabricada em 1946 apresentou 17.465 válvulas. A máquina em exibição no museu é a reconstrução do modelo original que foi mantido oculto até a década de 1970. Em *Bletchley Park* também se pode ver o último modelo da máquina de cifragem Enigma.

Das dez máquinas de decodificação fabricadas antes de terminar a guerra, oito foram destruídas por ordem do Primeiro Ministro Britânico *Winston Churchill* (MATO, 2016, p. 184). O Governo Britânico vetou toda informação sobre as máquinas durante 30 anos.

Após 6 anos de conflito, chegou ao fim, em 1945, a Segunda Guerra Mundial na Europa com a rendição da Alemanha e na Ásia depois que os americanos despejaram duas bombas atômicas sobre os japoneses, fazendo dos civis as grandes vítimas. É uma guerra que ainda hoje desperta interesse. Pessoalmente tive um avô materno José Mendes Rosa (in memoriam) que participou do conflito, defendendo o Brasil nos campos da Itália, onde atuou por um ano. Isto ajuda a explicar a minha paixão pelo tema.

Os historiadores podem expor seus conhecimentos através de dispositivos audiovisuais, assim como analisar filmes como discursos históricos autônomos em relação à historiografia escrita. E a Segunda Guerra Mundial tem proporcionado diversas interpretações sobre o conflito através da grande quantidade de filmes. Citamos uma cinebiografia no primeiro capítulo e quatro filmes no segundo capítulo. No terceiro capítulo, fizemos extensa análise, como estudo de caso do filme “O jogo da imitação”, que tem a Segunda Guerra Mundial como contexto histórico. Segundo o filme: “O jogo da imitação, 2014”, os ingleses decifravam mensagens da máquina Enigma alemã e as informações não eram repassadas aos russos por vias oficiais. Gilbert (2014) diz que “na Grã-Bretanha as mensagens Enigma eram utilizadas pelo interesse do país e da Rússia”. Ás vezes *Winston Churchill* enviava informações sobre os alemães para o próprio *Josef Stálin* por vias oficiais.

Os filmes, na sua maioria refletem uma visão dos Aliados em relação à Alemanha Nazista. São obras engajadas que enfatizam, geralmente o que houve de pior no modelo alemão da era *Hitler*.

Provavelmente a Segunda Guerra Mundial vai ensejar novas interpretações pois, no confronto entre as duas maiores potências mundiais da primeira metade do século XX, a Alemanha saiu derrotada nas duas vezes e, no entanto, em algumas décadas tornou-se, novamente, a maior potência da Europa na atualidade. O que explica esse fenômeno? Tema para uma nova pesquisa.

REFERÊNCIAS

BALDWIN, H. *Batalhas ganhas e perdidas*; tradução Cel. Álvaro Galvão. Rio de Janeiro: Biblioteca do Exército, 1978.

BARNETT, C. *Os Generais de Hitler*, Rio de Janeiro: Jorge Zahar Editor Ltda, 1991.

BEKKER, C. *A história da Luftwaffe*; tradução José Dinis Zambujo, Amadora – Portugal: Editora Ibis, Ltda, 1968.

BRISSAUD, A. *Almirante Canaris – O príncipe da espionagem alemã*; tradução Anita Souza Costa de Toledo. Rio de Janeiro: Biblioteca do Exército, 1978.

BURNS, E. M. *História da Civilização Ocidental*, Volume II, Rio de Janeiro: Editora Globo, 1966.

CALHAU, Lélio Braga. *Bullying: o que você precisa saber: identificação, prevenção e repressão.* 3ª Ed. Niterói, RJ: Impetus, 2011.

CARLOS, M. C. [et al]. *ICPEdu Introdução a Infraestrutura de Chaves Públicas e Aplicações*. Rede Nacional de Pesquisa – RNP. Rio de Janeiro: RNP/ESR, 2014.

CARVALHO, D. *Segurança de dados com criptografia – Métodos e Algoritmos*. Rio de Janeiro: Editora Book Express Ltda, 2000.

CHURCHILL, W. *Memórias da Segunda Guerra Mundial*; tradução Vera Ribeiro. Rio de Janeiro: Nova Fronteira, 1995.

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro: Instituto Nacional de Matemática Pura e Aplicada, IMPA, 2003.

CORNWELL, J. *Os cientistas de Hitler: ciência, guerra e o pacto com demônio*; tradução: Marcos Santarrita, Rio de Janeiro: Editora Imago, 2003.

COUTO, S. P.. *Códigos & Cifras – da Antiguidade à Era Moderna*. Rio de Janeiro: Novaterra Editora e Distribuidora Ltda, 2008.

CRYPTO Museum. The Polish Bomba. Disponível em: http://www.cryptomuseum.com/crypto/bombe/>. Acesso em: mai. 2016.

CRYPTO Museum. Working principle of the Enigma. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/working.htm>. Acesso em: mai. 2016.

CRYPTO Museum. Enigma A - Printing Enigma machine. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/a/index.htm>. Acesso em: mai. 2016.

CRYPTO Museum. Enigma B - Improved printing Enigma. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/b/index.htm>. Acesso em: mai. 2016.

CRYPTO Museum. Enigma H - Model H29 - Enigma-II. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/h/index.htm>. Acesso em: mai. 2016.

CRYPTO Museum. Enigma C - The first lamp-based Enigma. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/c/index.htm>. Acesso em: mai. 2016.

CRYPTO Museum. Enigma D - Commercial Enigma A26. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/d/index.htm>. Acesso em: mai. 2016.

CRYPTO Museum. Enigma I - The Service Enigma Machine. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/i/index.htm>. Acesso em: mai. 2016.

CRYPTO Museum. Enigma M1, M2 and M3 - 3-wheel Naval Enigma. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/m3/index.htm> Acesso em: mai. 2016.

CRYPTO Museum. Enigma M4 - U-Boot Enigma. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/m4/index.htm>. Acesso em: mai. 2016.

CRYPTO Museum. Zählwerk Enigma - Commercial Enigma A28. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/g/a28.htm>. Acesso em: mai. 2016.

CRYPTO Museum. Enigma G - Zählwerk Enigma G31. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/g/index.htm>. Acesso em: mai. 2016.

CRYPTO Museum. Enigma T (Tirpitz) - The Japanese Enigma. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/t/index.htm>. Acesso em: mai. 2016.

CRYPTO Museum. Enigma K - A family of commercial machines A27. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/k/index.htm>. Acesso em: mai. 2016.

CRYPTO Museum. Swiss-K - Enigma K variant for Switzerland. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/k/swiss.htm>. Acesso em: mai. 2016.

FANTE, C. *Fenômeno bullying : como prevenir a violência nas escolas e educar para a paz.* 6ª Ed. Campinas, SP: Verus Editora, 2005.

GILBERT, M. *A Segunda Guerra Mundial – Os 2.174 dias que mudaram o mundo*; tradução: Ana Luisa Faria e Miguel Serras Pereira, 1ª ed. – Rio de Janeiro: Casa da Palavra, 2014.

HEIFERMAN, R; SHERMER, D; MAYER, S.L, *Guerras do Século 20*. Rio de Janeiro: Editora Primor Ltda, 1975.

HITLER, A. *Minha Luta – Mein Kampf*. São Paulo: Editora Moraes Ltda, 1983.

HERNÁNDEZ, Jesús. *100 historias secretas de la segunda guerra mundial*. 3ª ed. Barcelona: Roca Editorial de Libros, 2016.

ISNENGHI, M. *História da Primeira Guerra Mundial*; tradução: Mauro Lando e Isa Mara Lando, São Paulo: Editora Ática.

JOGO DA IMITAÇÃO, O (*The Imitation Game*). Reino Unido/Estados Unidos. Direção: Morten Tyldum. Produção: Nora Grossman, Ido Ostrowsky, Teddy Schwarzman. Roteiro: Graham Moore. Elenco: Benedict Cumberbatch, Keira Knightley, Matthew Goode, Mark Strong, Charles Dance, Allen Leech, Matthew Bard, Rory Kinnear. Música: Alexandre Desplat. Cinematografia: Óscar Faura. Edição: William Goldenberg. Produtoras: Black Bear Pictures, Bristol Automotive. Distribuição: Studio Canal (Reino Unido), The Weinstein Company (Estados Unidos), 2014, cor, 114 min.

JORDAN, D. *Atlas da II Guerra Mundial: Alemanha versus Inglaterra*: volume I; tradução Tatiana Napoli – São Paulo: Editora Escala, 2008.

JÜRGEN SCHMIDHUBER Home Page. *KONRAD ZUSE (1910-1995).* Disponível em: < http://people.idsia.ch/~juergen/zuse.html>. Acesso em mai. 2017.

KAHN, D. *The code-breakers. The Story of Secret Writing*, New York, NY: Scribner, 1996.

LEAVITT, D. *O homem que sabia demais – Alan Turing e a invenção do computador*; tradução Samuel Dirceu. Ribeirão Preto - SP: Novo Conceito Editora, 2011.

MAGALHÃES FILHO, F. de B. B. *História Econômica 10ª edição*. São Paulo: Editora Saraiva, 1986.

MATO, Omar López. *Ciencia y mitos en la Alemania de Hitler*. 1ª ed. Ciudad Autónoma de Buenos Aires: JavierVergara Editor, 2016.

MANDEL, E. *O significado da 2ª Guerra Mundial*. São Paulo: Editora Ática, 1989.

MASSON, P. *A Segunda Guerra Mundial – História e Estratégias*; tradução Ângela M. S. Corrêa – São Paulo: Editora Contexto, 2015.

MÉNARD, R. *Mitologia greco-romana* – Volume 1; tradução Aldo Della Nina – São Paulo: Opus, 1991.

MÉNARD, R. *Mitologia greco-romana* – Volume 2; tradução Aldo Della Nina – São Paulo: Opus, 1991.

MENEZES, Alfred; OORSCHOT, Paul van; VANSTONE, Scott. *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1997.

NOGUEIRA, Rosa Maria César Del Picchia de Araújo. *A prática de violência entre pares: o bullying nas escolas.* Fundação Joaquim Nabuco. Disponível em: http://www.fundaj.gov.br/geral/educacao_foco/bullyng2.pdf. Acesso em 20 de janeiro de 2017.

NÓVOA, J., FRESSATO S., FEIGELSON, K.(organizadores) *CINEMATÓGRAFO um olhar sobre a história.* - Salvador: EDUFBA; São Paulo: Ed. da UNESP, 2009.

PATERSON, M. *Decifradores de Códigos*. Tradução Elvira Serapicos. São Paulo: Larousse do Brasil, 2009.

PINTO, W. S. *Introdução ao desenvolvimento de algoritmos e estruturas de dados*. São Paulo: Érica, 1990.

RIJMENANTS, D. CIPHER MACHINES AND CRYPTOLOGY. Disponível em: < http://users.telenet.be/d.rijmenants/en/enigmaproc.htm>. Acesso em: mai. 2016.

SANTAELLA, Lúcia. *Corpo e comunicação: sintoma da cultura*. 3ª. Ed. São Paulo: Paulus, 2008.

SHIRER, W. L. *Ascensão e queda do III Reich* – Volume 1. Rio de Janeiro: Editora Civilização Brasileira S.A., 1967.

SHIRER, W. L. *Ascensão e queda do III Reich* – Volume 2. Rio de Janeiro: Editora Civilização Brasileira S.A., 1967.

SINGH, S. *O livro dos códigos*. Rio de Janeiro: Editora Record Ltda, 2014.

SONDHAUS, L. *A Primeira Guerra Mundial*, tradução Roberto Cataldo Costa. São Paulo: Editora Contexto, 2013.

STALLINGS, W. *Criptografia e segurança de redes*. Tradução Daniel Vieira, 4.ed., São Paulo: Pearson Prentice Hall, 2008.

TANENBAUM, A, *Redes de Computadores*. Tradução Vandenberg D. de Souza, Rio de Janeiro: Elsevier, 2003.

TELEGRAPH, The. Bletchley Park commander not the 'baddy' he is in The Imitation Game, family say. Disponível em: < http://www.telegraph.co.uk/news/celebritynews/11256888/Bletchley-Park-commander-not-the-baddy-he-is-in-The-Imitation-Game-family-say.html>. Acesso em: mai. 2016.

TELEGRAPH, *The. The Imitation Game: who were the real Bletchley Park codebreakers?*. Disponível em: < http://www.telegraph.co.uk/films/2016/07/31/the-imitation-game-who-were-the-real-bletchley-park-codebreakers/>. Acesso em: mai. 2016.

TKOTZ, V. *Criptografia – Segredos embalados para viagem*. São Paulo: Novatec Editora Ltda, 2005.

VOLKMAN, E. *A História da Espionagem*. São Paulo: 1ª Ed. Editora Escala LTDA., 2013.

WERTH, A. A Rússia na guerra – Estalinegrado. Tradução J. M. da Costa. Portugal: Publicações Europa-América, 1971.

WINTERBOTHAM, F. W. *Enigma – O segredo de Hitler*. 1.ed. Rio de Janeiro: Biblioteca do Exército - Editora, 1978.

WISKEMANN, E. *A Guerra Russo-polonesa – História do Século 20*. São Paulo: Editora Abril S.A. Cultural e Industrial, 1974.

ZOCHIO, M. *Introdução à Criptografia*. São Paulo: Novatec Editora Ltda, 2016.

GLOSSÁRIO

Abwehr: Serviço de Inteligência Alemão (1921-1944). Foi substituído em 1944 pelo *Reichssicherheitshauptamt* (RSHA).

Abwehrstellen (Ast): agências de Inteligência locais do *Abwehr.*

Almirantado: responsável pela Marinha Real Britânica.

Bamburismo: bamburismus, processo criptoanalítico desenvolvido por Alan Turing que usava probabilidade condicional sequencial.

Biuro Szyfrów: Birô de Cifras Polonês.

Bureau du Chiffre: Birô de Cifras Francês.

Cabos: são feitos por diversos filamentos finos, o que lhes dá maleabilidade.

Chave: informação que controla a operação de um algoritmo de criptografia.

Chiffrierstelle: Agência de Criptografia, escritório encarregado de administrar as comunicações cifradas da Alemanha.

Chiffriermaschinen: máquina de cifragem.

Cifra: um ou mais algoritmos que cifram e decifram um texto.

Cifragem: processo de conversão de um texto claro para um código cifrado.

Cillies: ou cílios, chaves de mensagens previsíveis. Tolices que os operadores das máquinas Enigma persistiam em fazer, mesmo contra os procedimentos operacionais.

Código Morse: sistema de comunicação através de um sinal codificado enviado intermitentemente

Crab: passo simultâneo de dois rotores.

Crash: quando a mesma letra aparecia na mesma posição em um *crib* e em um criptograma.

Cribs: partes do texto claro que sabidamente correspondem a uma parte do código.

Criptoanálise: esforço de descodificar ou decifrar mensagens sem que se tenha o conhecimento prévio da chave secreta que as gerou.

Criptografia: estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, para que possa ser conhecida apenas por seu destinatário.

Criptologia: disciplina que estuda os conhecimentos e técnicas necessários à criptoanálise (solução de criptogramas) e à criptografia (escrita codificada).

Decifragem: processo de recuperar o texto original a partir de um texto cifrado.

Eintrittswalze (ETW): rotor ou roda de entrada.

Fêmeas: letras repetidas em certas posições entre as chaves de mensagem.

Fios: são feitos de um único e espesso filamento, e por isso são rígidos.

Funkspruch: formulário de mensagem.

Funkverkehrsheft für die Küstenverteidigung: Livro de Tráfego de Rádio para a Defesa Costeira.

Gardening: jardinagem, provocar o envio de mensagens por atividades como espalhar minas submarinas para gerar "*kisses"*.

Gartenzaun: cerca do jardim.

Gebrauchsanweisung für die Chiffriermaschine Enigma: Manual de operação da máquina de cifragem Enigma.

General Code and Cipher School (GC&CS): Escola de Cifras e Códigos do Governo Britânico. Sucedida pelo *Government Communications Headquarters* (GCHQ) em 1946.

Glühlampen: lâmpadas incandescentes.

Glühlampenmaschine: máquina de lâmpadas incandescentes.

Government Communications Headquarters (GCHQ): Quartel General de Comunicações do Governo, responsável pela quebra de códigos a partir de 1946 no lugar da Escola de Cifras e Códigos do Governo britânico.

Griechenwalze: roda grega (era identificada com as letras gregas beta ou gama).

Grundstellung: posição inicial das rodas, equivalente neste caso à chave diária.

Heer: Exército alemão a partir de 1955.

Hut: casinhas ou cabanas de madeira construídas nos jardins de *Bletchley Park*.

Innere Einstellung: configurações internas.

JABJAB: um dos tipos de *cillies*.

Kenngruppen: grupos para identificar a chave para o receptor.

Kenngruppenbuch: livro com os grupos para identificar a chave para o receptor.

Kenngruppenheft: folheto de características de grupo.

Kisses: criptogramas que foram enviados com virtualmente o mesmo conteúdo, mas com cifragens diferentes.

Kommando des Meldegebietes: agências de Inteligência internacionais.

Kommerziell: comercial.

Kriegsmarine: Marinha de Guerra Alemã, de 1935 a 1945.

Kurzsignalheft: folheto de mensagens curtas.

Lobster: passo simultâneo de três rotores.

Loop: ligação entre o texto cifrado e o assumido texto claro.

Luftwaffe: Força Aérea alemã.

Lückenfüllerwalze: roda "tapa-buraco".

Militärisches Amt: Gabinete Militar.

Mímese: imitação

Notch: entalhe ou chanfro.

Pawl: lingueta.

Princípio de Kerckhoffs: um sistema criptográfico (militar) deve ser seguro mesmo se tudo sobre o sistema, com exceção da chave, for de conhecimento público.

Quadro de tomadas: painel de plugues.

Ratchet: catraca, ou dispositivo mecânico que consiste de uma roda dentada envolvido com uma lingueta que permite que ele se mova em uma única direção.

Reichsbahn: Ferrovia Imperial Alemã.

Reichsmarine: Marinha alemã (1919-1935): Tornou-se *Kriegsmarine*.

Reichswehr: Forças Armadas alemãs (1921-1935): Tornou-se *Wehrmacht*

Reichssicherheitshauptamt (RSHA): Gabinete Central de Segurança do *Reich* Alemão, criado em 1939.

Ringstellung: configuração dos anéis, a posição do anel alfabético relativa à fiação do rotor.

Rotor: tudo aquilo que gira em torno de seu próprio eixo produzindo movimentos de rotação. Neste estudo, são usados os termos disco, roda, rolo e misturador como sinônimos de rotor no contexto de máquinas Enigma.

Royal Air Force (RAF): Força Aérea Real Britânica.

Ruthless: impiedoso, impiedosa.

Sala 40: seção do Almirantado britânico ligada à criptoanálise criada em 1914.

Schlüsselanleitung für die Chiffriermaschine Enigma: Instruções de uso das chaves da máquina Enigma.

Sonderschlüssel: chave especial.

Stecker: plugue.

Steckerbrett: painel de plugues.

Steckerverbindungen: conexões dos plugues, feitas no painel de plugues

Stepping: processo em que os rotores giram, em passos.

Telegrafia sem fio: termo que se aplica a antigas técnicas de comunicação por rádio telégrafo, antes do termo rádio se popularizar.

Turnover: movimento.

U-Boat: termo em inglês para designar qualquer submarino alemão.

U-Boot: do alemão *Unterseeboot* ("pequeno barco debaixo d'água"), este termo é usado para designar qualquer submarino.

Umkehrwalze (UKW): roda fixa reversa, ou refletor.

Walzenlage: ordem dos rotores, a escolha dos rotores e a ordem em que eles eram colocados.

Wehrmacht: Forças Armadas alemãs (1935-45).

Wetter: tempo, no sentido usado para previsão do tempo.

Wetterkurzschlüssel: chaves curtas de previsão do tempo.

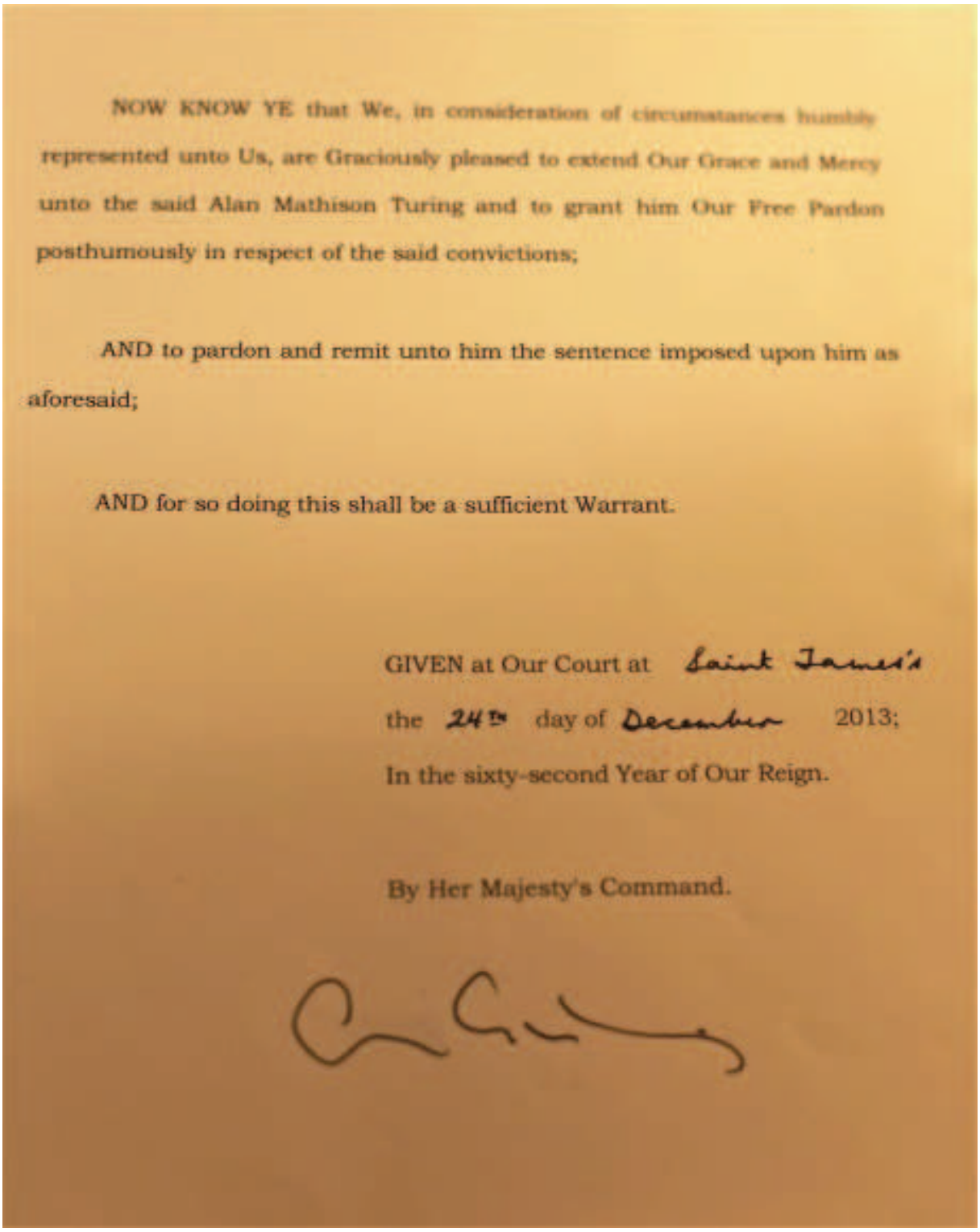
Zählwerk: contador.

Zusatzwalze: roda adicional.

Zuteilungsliste: lista de alocação.

Anexo A

Carta de perdão real destinada a Alan Turing.



NOW KNOW YE that We, in consideration of circumstances humbly represented unto Us, are Graciously pleased to extend Our Grace and Mercy unto the said Alan Mathison Turing and to grant him Our Free Pardon posthumously in respect of the said convictions;

AND to pardon and remit unto him the sentence imposed upon him as aforesaid;

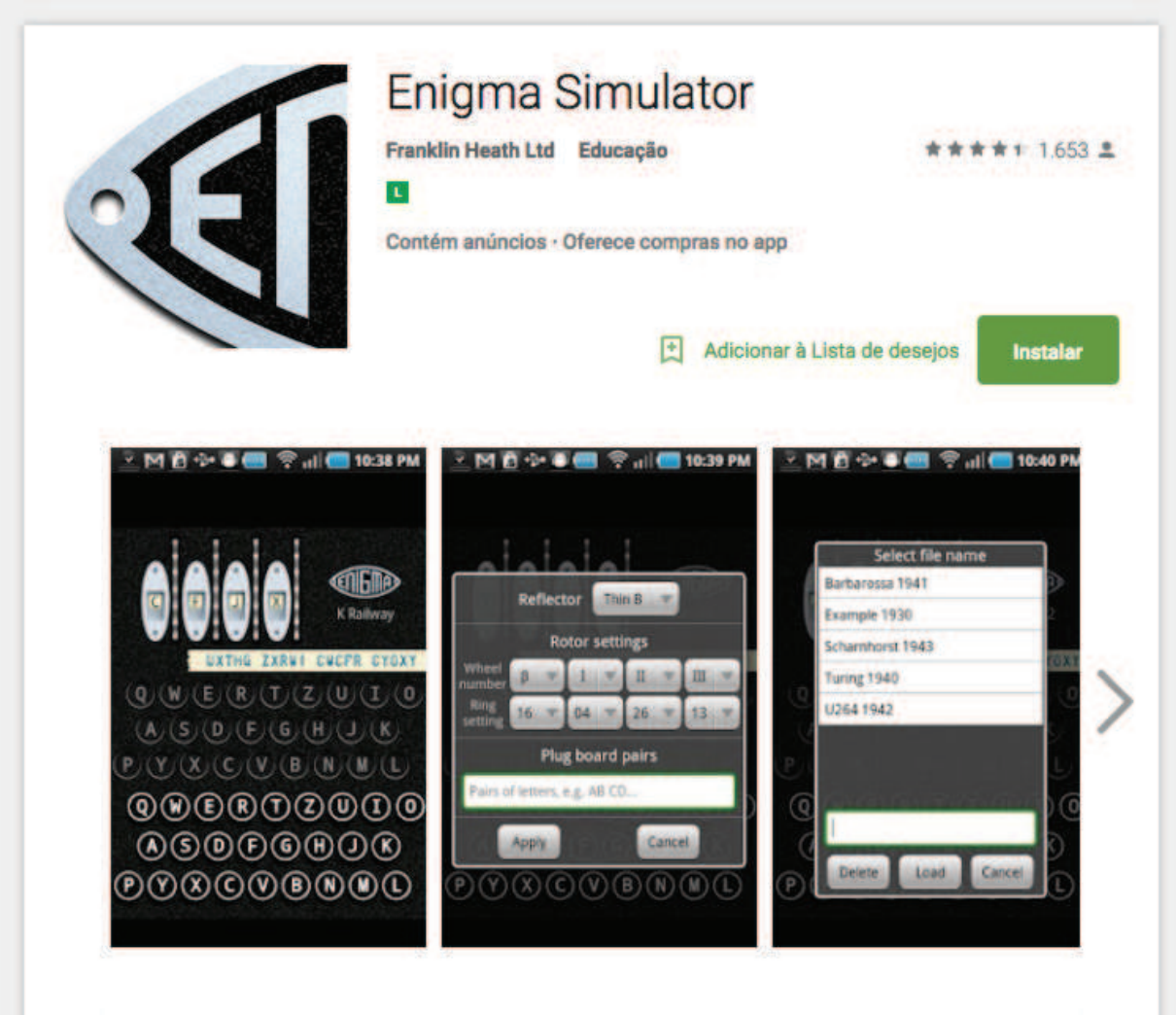
AND for so doing this shall be a sufficient Warrant.

GIVEN at Our Court at Saint James's
the 24th day of December 2013;
In the sixty-second Year of Our Reign.

By Her Majesty's Command.

Anexo B

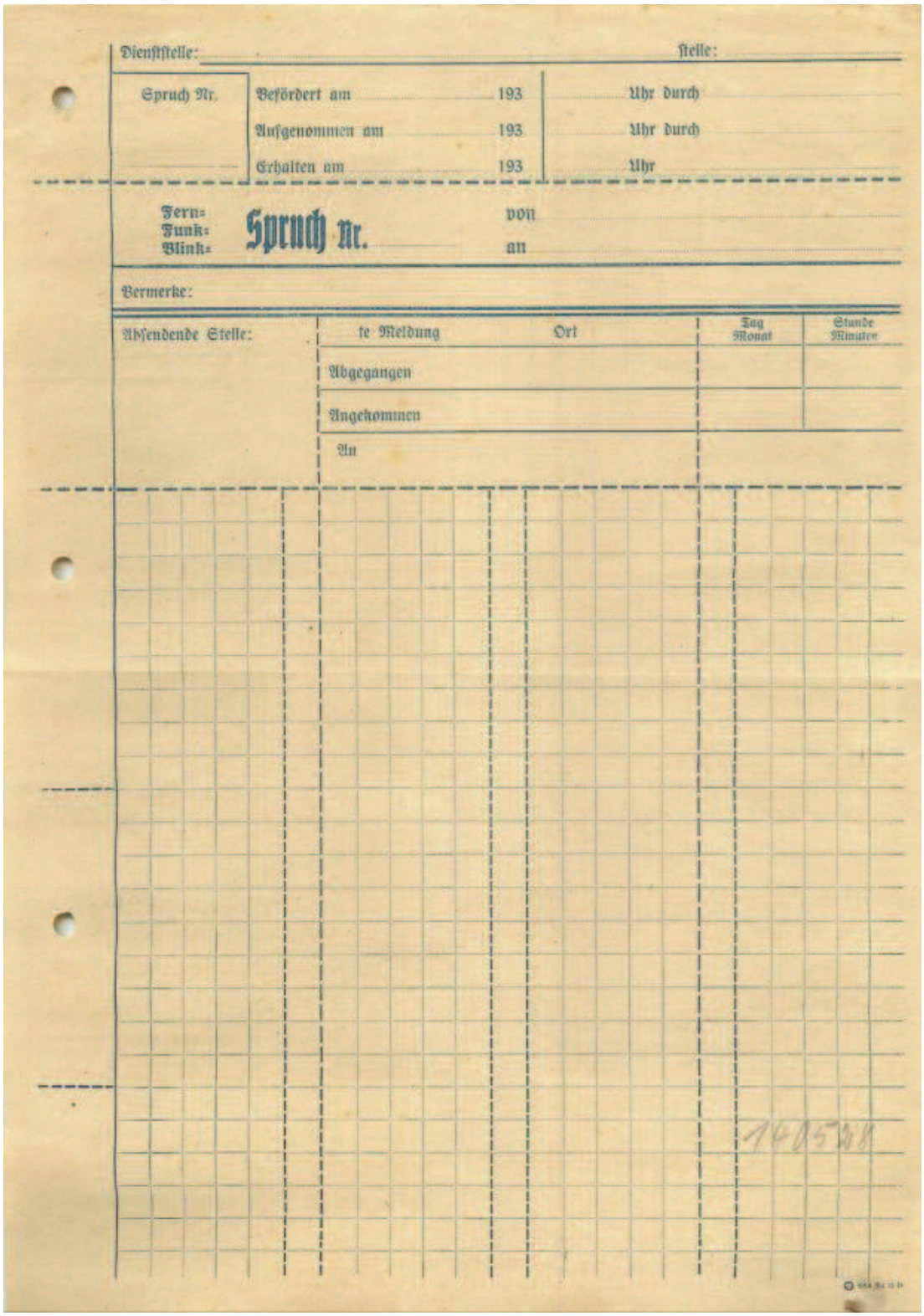
Simulador da máquina de cifragem Enigma de Franklin Heath Ltd.



Fonte: Play Store da empresa Google

Anexo C

Formulário para registrar as mensagens da máquina de cifragem Enigma



Anexo D

Kit de montagem de sua própria máquina de cifragem Enigma.

Fonte: http://www.cryptomuseum.com/kits/enigma/index.htm

Anexo E

Características idiomáticas do espanhol, italiano, inglês, francês e alemão

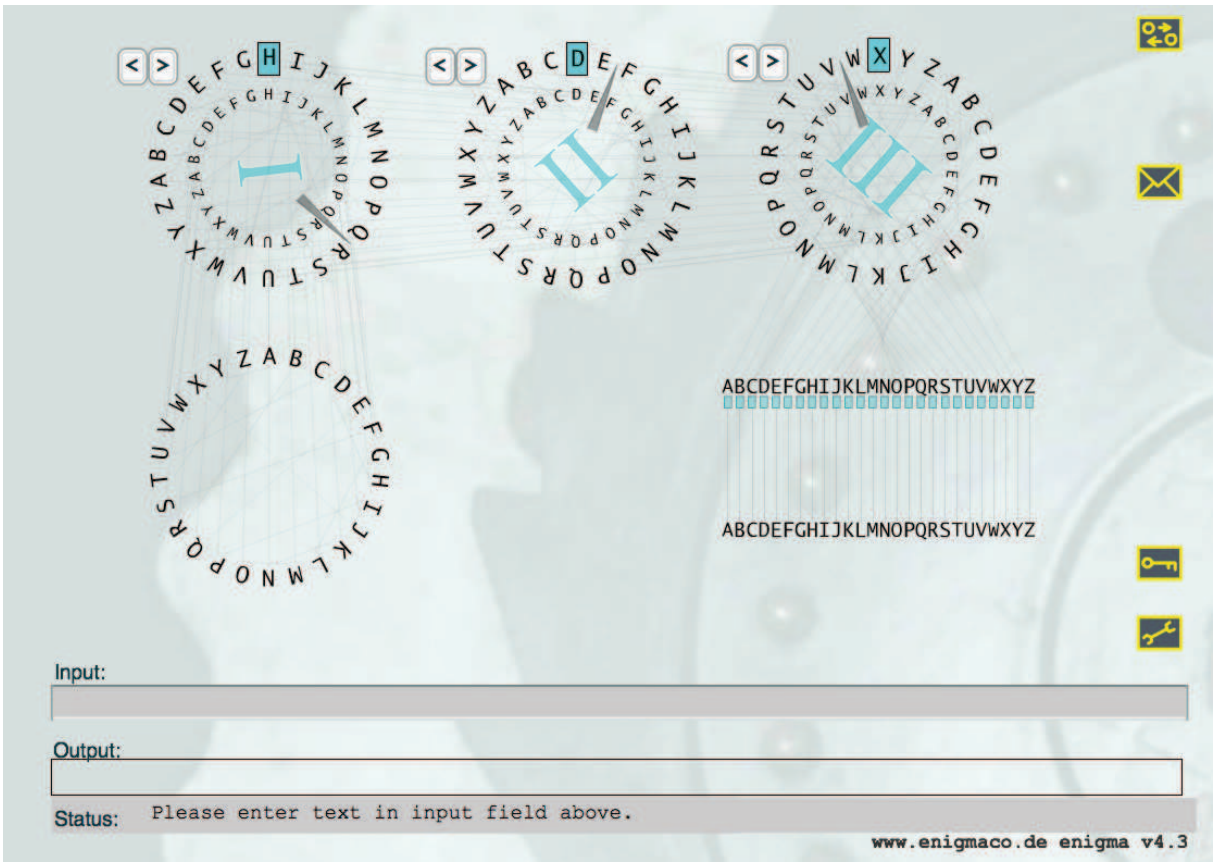
Característica	Espanhol	Italiano	Inglês	Francês	Alemão
Comprimento médio das palavras	4,96	4,5	4,5	4,3	4,84
Letra mais frequente	E (14%)	E (12%)	E (12%)	E (17%)	E (17-18%)
Ordem das letras	E A O I N S R L D T C U M P V G B Q F Y H Z J X K W	E A I O N L R T S C D P U M V G H F B Q Z J X K W Y	E T A O N I R S H L D C U P F M W Y B G V K Q X J Z	E A S I N T R L U O D C P M V G F B Q H X J Y Z K W	E N I R S A T H D U L C G M O B W F K Z V P J X Q Y
Vogais	47%	48%	40%	44-45%	38-40%
Letras de baixíssima frequência	J Y Z K W	J X K W Y	V Q X J Z	J Y K W Y	V P J X Q Y
Digramas	EM DE ES EL LA AL NT RE ER ON OS AD AR EU RA CI AS TE SE CO	ER ES ON RE EL EM DE DI TI SI AL AN RA NT TA CO	TH HE AN IN ER RE ES ON ST NT EN ED ND AT TI TE OR AR HA OF	ES DE LE EN RE NT ON ER TE EL AN SE ET LA AI IT ME OU EM IE	EN ER CH TE EI DE IN IE ND GE UN IC HE NE ES AN BE ST SE AU
Trigramas	ENT QUE NTE DEL ELA ION DAD CIO COM EST ADE ALI IDA NCI EAL ODE ACI CIA ESE IEN	CHE ERE ZIO DEL ECO QUE ARI ATO EDI IDE ESI IDI ERO PAR NTE STA	THE AND ING ION NTH TER INT OFT THA ERE TIO HER FTH ETH ATI HAT ATE STH EST	ENT LES EDE DES QUE AIT LLE SDE ION EME ELA RES MEN ESE DEL ANT TIO PAR ESD TDE	ICH EIN UND DER SCH DIE INE CHT CHE DEN GEN NDE TEN ACH HEN TER SIE BER TTE NEN
Palavras curtas mais	DE LA EL QUE EN NO CON	LA DI CHE IL NON SI LE UNA LO	THE AND TO I A OF IT IN YOU	DE IL LE ET QUE JE LA NE CE	UND DIE DER ER ICH SIE ZU

frequentes	UN SE SU LAS LOS ES ME AL LO SI MI UMA DEL POR SUS MUY HAY MAS	IN PER UM MI IO PIU DEL MA SE	WAS MY HE SHE AS HIS NOT BUT FOR AT ME IS BE SO ON HIM ALL HAD	SE SON MON PAS LUI ME AU UNE DES SA QUI EST DU	IN DAS ES DEN DA MIT EIN SO DEM WAR ALS DU AUF IST WIE VON AN
Iniciais de palavras	C P A S M E D T H V R U N I L B O F Q G J Z	S P A C D V T M F I G Q R E B L N O U Z H	T A S I H W O M B D F C L N P Y G R E U V K Q J	P A S M C E D T V F R B L G J I Q N O H U Y X Z	D S E W A U I G M H B N Z V F K T L R J P O Q
Finais de palavras	O A S E N R D L I Z	O E A I R L D N	E A O S M R T D U N Y I L G F H Z K W P C B X V	E S T R N D A I X Z L C U P F Y	R M T N D U E L I Y H G F A O S Z K W P B

Fonte: TKOTZ, 2005, p. 271

Anexo F

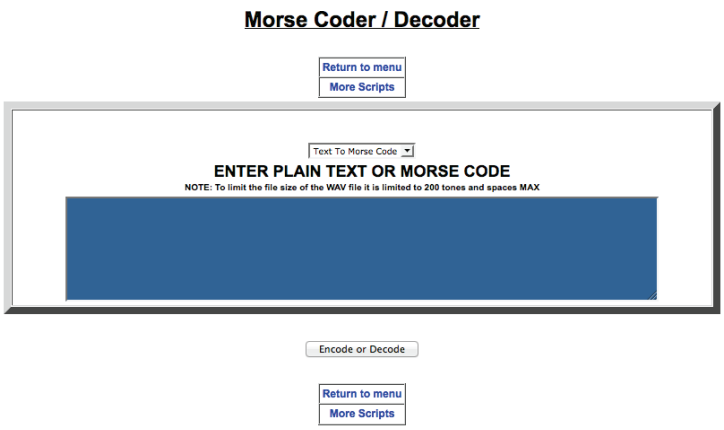
Simulador da máquina Enigma disponível em: http://enigmaco.de/enigma/enigma.html



Fonte: http://enigmaco.de/enigma/enigma.html

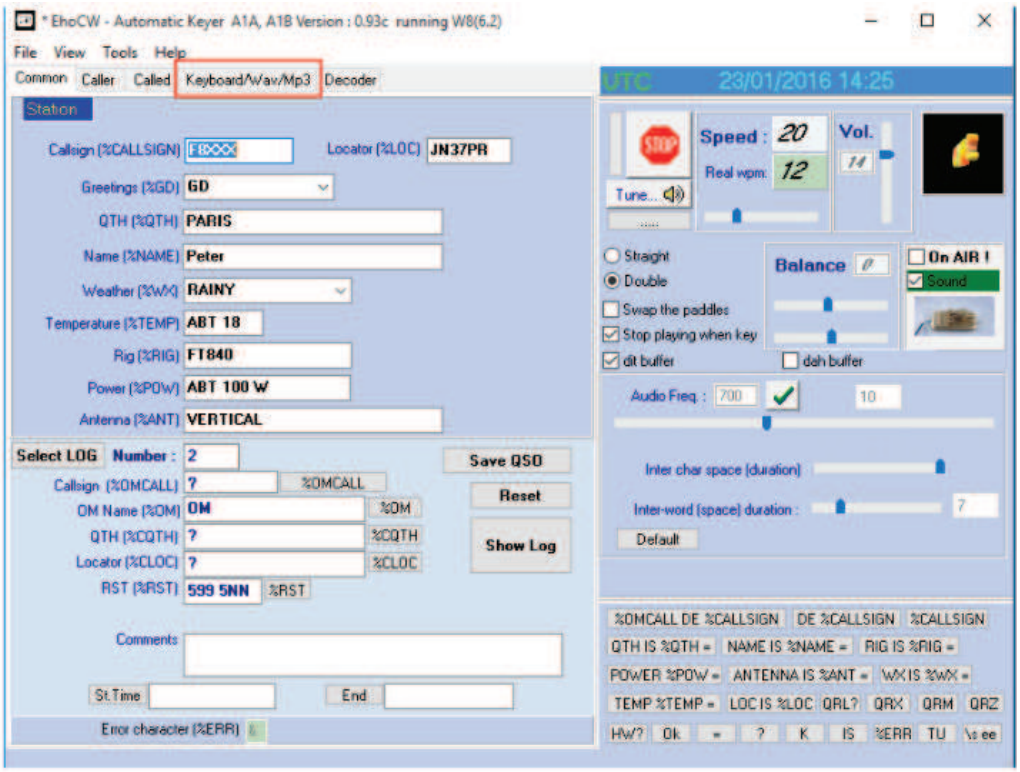
Anexo G

Programa que converte texto em código morse disponível em: https://webnet77.net/cgi-bin/helpers/morse.pl



Fonte: https://webnet77.net/cgi-bin/helpers/morse.pl

Se você quiser converter o texto em código morse em um arquivo de áudio, baixe o programa chamado EhoCW disponível em: http://www.f8eho.net/content/downloads



Fonte: http://www.f8eho.net/content/downloads

Anexo H

Principais acontecimentos da Primeira Guerra Mundial

1914	
28 de junho	Francisco Ferdinado, herdeiro do trono da Áustria-Hungria é assassinado em Sarajevo por um nacionalista bósnio.
28 de julho	A Áustria declara guerra à Sérvia.
1º de agosto	A Alemanha declara guerra à Rússia; a Itália declara neutralidade.
2 de agosto	Alemanha ocupa Luxemburgo
3 de agosto	A Alemanha invade a Bélgica e declara guerra à França.
4 de agosto	Grã-Bretanha declara guerra à Alemanha.
5 de agosto	A Áustria declara guerra à Rússia.
20 de agosto	Os alemães ocupam Bruxelas.
28 de agosto	Os alemães derrotam os russos em Tannemberg.
5 de setembro	Começa a batalha do Marne.
27 de setembro	Os russos invadem a Hungria.
2 a 5 de novembro	A Entente declara guerra à Turquia.
6 de dezembro	Os alemães conquistam Lodz (Polônia).
17 de dezembro	O Egito é declarado protetorado inglês.
1915	
19 de fevereiro	Bombardeio franco-inglês em Dardanelos.
11 de março	A Inglaterra declara bloqueio da Alemanha
25 de abril	Os anglo-franceses desembarcam em Galípoli
26 de abril	As potências da Entente e a Itália assinam o Pacto de Londres.

7 de maio	Um submarino alemão afunda o transatlântico Lusitânia.
23 de maio	A Itália declara guerra à Áustria.
1º de junho	Primeiro ataque aéreo a Londres com zepelins.
9 de julho	As colônias alemãs do Sudoeste Africano se rendem.
5 de agosto	Os Alemães entram em Varsóvia.
22 de setembro	Começa a ofensiva francesa em Champagne.
5 de outubro	As tropas aliadas desembarcam em Salonica.
1916	
19 de janeiro	Ofensiva russa na Galícia.
21 de fevereiro	Batalha de Verdun.
31 de maio	Batalha naval da Jutlândia.
27 de agosto	A Romênia entra em guerra contra a Áustria
28 de agosto	A Itália declara guerra contra a Alemanha.
21 de novembro	Morte de Francisco José, imperador da Áustria-Hungria.
6 de dezembro	Os alemães invadem Bucareste.
1917	
31 de janeiro	A Alemanha anuncia a guerra submarina total.
12 de março	Revolução Russa.
6 de abril	Estados Unidos declaram guerra à Alemanha.
1º de agosto	Nota do Papa Benedito XV sobre a paz.
3 de setembro	Os alemães invadem Riga.
7 de novembro	Lenin toma o poder na Rússia.
5 de dezembro	Armistício entre russos e alemães.

9 de dezembro	Armistício entre Romênia e os impérios centrais.

1918

9 de fevereiro	A Ucrânia independente assina a paz.
3 de março	A Rússia assina a paz em Brest-Litovsk
21 de março	Início da grande ofensiva alemã no oeste.
14 de abril	Os alemães ocupam Helsinki.
27 de maio	Nova ofensiva alemã a oeste.
2 de agosto	Os japoneses desembarcam na Sibéria.
29 de setembro	A Bulgária assina o armistício
20 de outubro	A Alemanha suspende a guerra submarina.
30 de outubro	A Turquia assina o armistício.
2 de novembro	Abdicação do Imperador Carlos I.
3 de novembro	Derrota do exército Austro-Húngaro. Assinatura do armistício.
9 de novembro	Abdicação e fuga do Kaiser.
11 de novembro	A Alemanha assina o armistício

Fonte: (ISNENGHI, 1995)

Anexo I

Principais acontecimentos da Segunda Guerra Mundial

1º de setembro de 1939	A Alemanha invade a Polônia, dando início à Segunda Guerra Mundial na Europa.
3 de setembro de 1939	Honrando sua garantia de segurança às fronteiras da Polônia, a Grã-Bretanha e a França declaram guerra à Alemanha.
27 a 29 de setembro de 1939	Varsóvia, capital da Polônia, se rende no dia 27 de setembro. Membros do governo polonês fogem para o exílio através da Romênia. A Alemanha e a União Soviética dividem a Polônia entre si.
9 de abril de 1940 a 9 de junho de 1940	A Alemanha invade a Dinamarca e a Noruega. A Dinamarca se rende no dia do ataque; a Noruega resiste até 9 de junho.
10 de maio de 1940 a 22 de junho de 1940	A Alemanha ataca a Europa Ocidental – França e os Países Baixos neutros. Luxemburgo é ocupado no dia 10 de maio; a Holanda se rende em 14 de maio, e a Bélgica em 28 do mesmo mês. Em 22 de junho, a França assina um acordo de armistício pelo qual os alemães ocupam a parte norte do país e toda a linha costeira do Atlântico; e no sul da França é estabelecido um regime colaborador dos nazistas com capital em Vichy.
10 de junho de 1940	A Itália entra na guerra, e invade o sul da França em 21 de junho.
28 de junho de 1940	A União Soviética força a Romênia a ceder a província oriental da Bessarábia e metade da região norte da Bucovina para a Ucrânia Soviética.
14 de junho de 1940 a 6 de agosto de 1940	A União Soviética ocupa os países bálticos entre 14 e 18 de junho, articulando golpes de estado comunistas em cada um deles entre 14 e 15 de

	julho, para em seguida anexá-los como Repúblicas Soviéticas, entre 3 e 6 de agosto
10 de julho de 1940 a 31 de outubro de 1940	A guerra aérea conhecida como a Batalha da Grã-Bretanha termina em derrota para a Alemanha nazista.
13 de setembro de 1940	Os italianos invadem o Egito, parte do então Mandato Britânico, através da Líbia sob domínio italiano.
27 de setembro de 1940	A Alemanha, a Itália e o Japão assinam o Pacto Tripartite.
Outubro de 1940	A Itália invade a Grécia cruzando a Albânia em 28 de outubro.
Novembro de 1940	A Eslováquia (23 de novembro), a Hungria (20 de novembro) e a Romênia (22 de novembro) unem-se ao Eixo.
Fevereiro de 1941	Os alemães enviam o *Afrika Korps*, destacamento do exército alemão, para reforçar as tropas italianas enfraquecidas.
1º de março de 1941	A Bulgária une-se ao Eixo.
6 de abril de 1941 a junho de 1941	A Alemanha, a Itália, a Hungria e a Bulgária invadem e dividem a Iugoslávia. A Iugoslávia se rende em 17 de abril. A Alemanha e a Bulgária invadem a Grécia em apoio aos italianos. A resistência na Grécia chega ao fim no início de junho de 1941.
22 de junho de 1941 a novembro de 1941	A Alemanha nazista e seus parceiros do Eixo (com a exceção da Bulgária) invadem a União Soviética. A Finlândia, procurando reparação de suas perdas territoriais para a União Soviética no armistício que finalizou a Guerra de Inverno, une-se ao Eixo pouco antes da invasão. Os alemães rapidamente invadem os países bálticos e, com ajuda dos finlandeses realizam um cerco a Leningrado (atual São Petersburgo) no mês de

	setembro. Mais ao centro da União Soviética os alemães conquistam Smolensk no início de agosto e, em outubro, parte rumo a Moscou. Ao sul, as tropas alemãs e romenas conquistam Kiev (Kyiv) em setembro e Rostov, às margens do rio Don, em novembro.
6 de dezembro de 1941	Uma contra-ofensiva soviética leva os alemães estacionados nos subúrbios de Moscou a uma retirada caótica.
7 de dezembro de 1941	O Japão bombardeia a base naval norte-americana de Pearl Harbor.
8 de dezembro de 1941	Os Estados Unidos declaram guerra ao Japão, entrando assim na Segunda Guerra Mundial. As tropas japonesas desembarcam nas Filipinas, na Indochina Francesa (Vietnã, Laos e Camboja), e na colônia britânica de Cingapura. Em abril de 1942, as Filipinas, Indochina e Cingapura caem sob domínio japonês.
11 a 13 de dezembro de 1941	A Alemanha nazista e seus parceiros do Eixo declaram guerra aos Estados Unidos.
30 de maio de 1942 a maio de 1945	Os britânicos bombardeiam a cidade de Köln, ou Colônia, trazendo a guerra para dentro do território alemão pela primeira vez. Durante os três anos seguintes bombardeios anglo-americanos reduzem cidades alemãs a escombros.
Junho de 1942	As frotas navais norte-americanas e britânicas conseguem impedir o avanço naval japonês na área central do Oceano Pacífico, no atol de *Midway*.
28 de junho de 1942 a setembro de 1942	A Alemanha e seus parceiros do Eixo iniciam uma nova ofensiva na União Soviética. As tropas alemãs abrem seu caminho até Stalingrado, (Volgograd) no rio Volga, até meados de setembro, penetrando profundamente na região

	do Cáucaso, após a conquista da Península da Criméia.
Agosto a novembro de 1942	Em Guadalcanal, nas Ilhas Salomão, as tropas norte-americanas conseguem impedir o avanço japonês, que ia abrindo caminho conquistando ilha a ilha, em direção à Austrália.
23 a 24 de outubro de 1942	As tropas britânicas derrotam alemães e italianos em El Alamein, no Egito, fazendo com que as forças militares do Eixo se retirassem de forma caótica através da Líbia até a fronteira leste da Tunísia.
8 de novembro de 1942	As tropas norte-americanas e britânicas desembarcam em diversos pontos nas praias da Argélia e do Marrocos, no norte da África sob controle francês. O fracasso das tropas colaboracionistas da França de Vichy em se defender contra a invasão, permite que os Aliados se movam rapidamente até a fronteira oeste da Tunísia, o que provoca a ocupação do sul da França pelos alemães, em 11 de novembro.
23 de novembro de 1942 a 2 de fevereiro de 1943	As tropas soviéticas contra-atacam destruindo as linhas de defesa húngaras e romenas nas regiões a noroeste e a sudoeste de Stalingrado, e imobilizando o Sexto Exército Alemão estacionada naquela cidade. Proibidos por Hitler de se retirarem ou tentarem escapar do cerco soviético, os sobreviventes se rendem em 2 de fevereiro de 1943.
13 de maio de 1943	As forças do Eixo na Tunísia se rendem aos Aliados, acabando com a campanha no norte da África.
5 de julho de 1943	Os alemães iniciam uma forte ofensiva com tanques perto de Kursk, na União Soviética. Os soviéticos enfraquecem aquele ataque em uma semana e começam uma ofensiva contra os

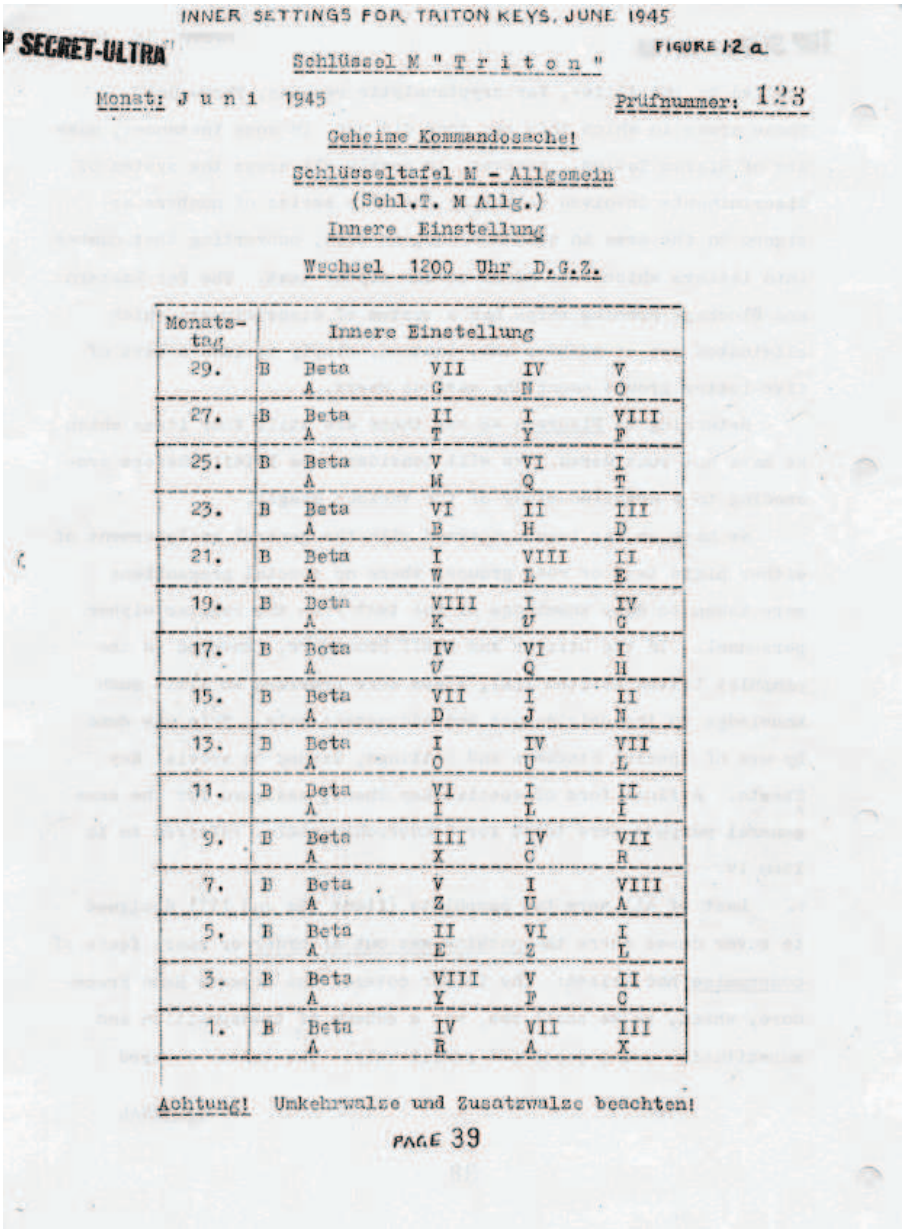
	alemães.
25 de julho de 1943	O Grande Conselho Fascista depõe Benito Mussolini, permitindo que o marechal italiano Pietro Badoglio institua um novo governo.
8 de setembro de 1943	O governo de Badoglio rende-se incondicionalmente aos Aliados. Os alemães imediatamente tomam controle de Roma e do norte da Itália, estabelecendo um regime fascista fantoche sob o controle de Mussolini, que foi libertado da prisão por soldados alemães de elite em 12 de setembro.
6 de novembro de 1943	As tropas soviéticas libertam Kiev.
6 de junho de 1944	As tropas britânicas e norte-americanas desembarcam com sucesso nas praias da Normandia, na França, e abrem a “Segunda Frente” contra os alemães.
20 a 25 de agosto de 1944	As tropas Aliadas chegam a Paris e, no dia 25 de agosto, as Forças Francesas Livres, com o apoio dos Aliados, entram na capital francesa. Em setembro, os Aliados chegam até a fronteira alemã; em dezembro, quase toda a França, a maior parte da Bélgica, e a parte sul dos Países Baixos são libertadas.
16 de dezembro de 1944	Os alemães iniciam a ofensiva final no oeste, conhecida como a Batalha do Bulge, em uma tentativa de reconquistar a Bélgica e dividir as forças Aliadas ao longo de toda a fronteira alemã. Em 1º de janeiro de 1945 os alemães batem em retirada.
7 de maio de 1945	A Alemanha se rende aos Aliados ocidentais.
6 de agosto de 1945	Os Estados Unidos lançam uma bomba atômica sobre a cidade de Hiroshima, no Japão.
8 de agosto de 1945	A União Soviética declara guerra contra o Japão e invade a Manchúria, província chinesa tomada

	pelo Japão em 1931.
9 de agosto de 1945	Os Estados Unidos lançam uma bomba atômica sobre a cidade de Nagasaki, no Japão.
2 de setembro de 1945	Rendição incondicional do Japão

Fonte: Adaptado de United States Holocaust Memorial Museum, Washington, DC. Disponível em https://www.ushmm.org/wlc/ptbr/article.php?ModuleId=10007306. Acessado em dez. 2017

Anexo J

Configurações internas “TRITON”



INNER SETTINGS FOR TRITON KEYS, JUNE 1945

SECRET-ULTRA

FIGURE 12 a

Schlüssel M "T r i t o n"

Monat: J u n i 1945 Prüfnummer: 123

Geheime Kommandosache!

Schlüsseltafel M - Allgemein

(Schl.T. M Allg.)

Innere Einstellung

Wechsel 1200 Uhr D.G.Z.

Monats-tag	Innere Einstellung				
29.	B	Beta A	VII G	IV N	V O
27.	B	Beta A	II T	I Y	VIII F
25.	B	Beta A	V W	VI Q	I T
23.	B	Beta A	VI B	II H	III D
21.	B	Beta A	I W	VIII L	II E
19.	B	Beta A	VIII K	I U	IV G
17.	B	Beta A	IV U	VI Q	I H
15.	B	Beta A	VII D	I J	II N
13.	B	Beta A	I O	IV U	VII L
11.	B	Beta A	VI I	I L	II I
9.	B	Beta A	III X	IV C	VII R
7.	B	Beta A	V Z	I U	VIII A
5.	B	Beta A	II E	VI Z	I L
3.	B	Beta A	VIII Y	V P	II C
1.	B	Beta A	IV R	VII A	III X

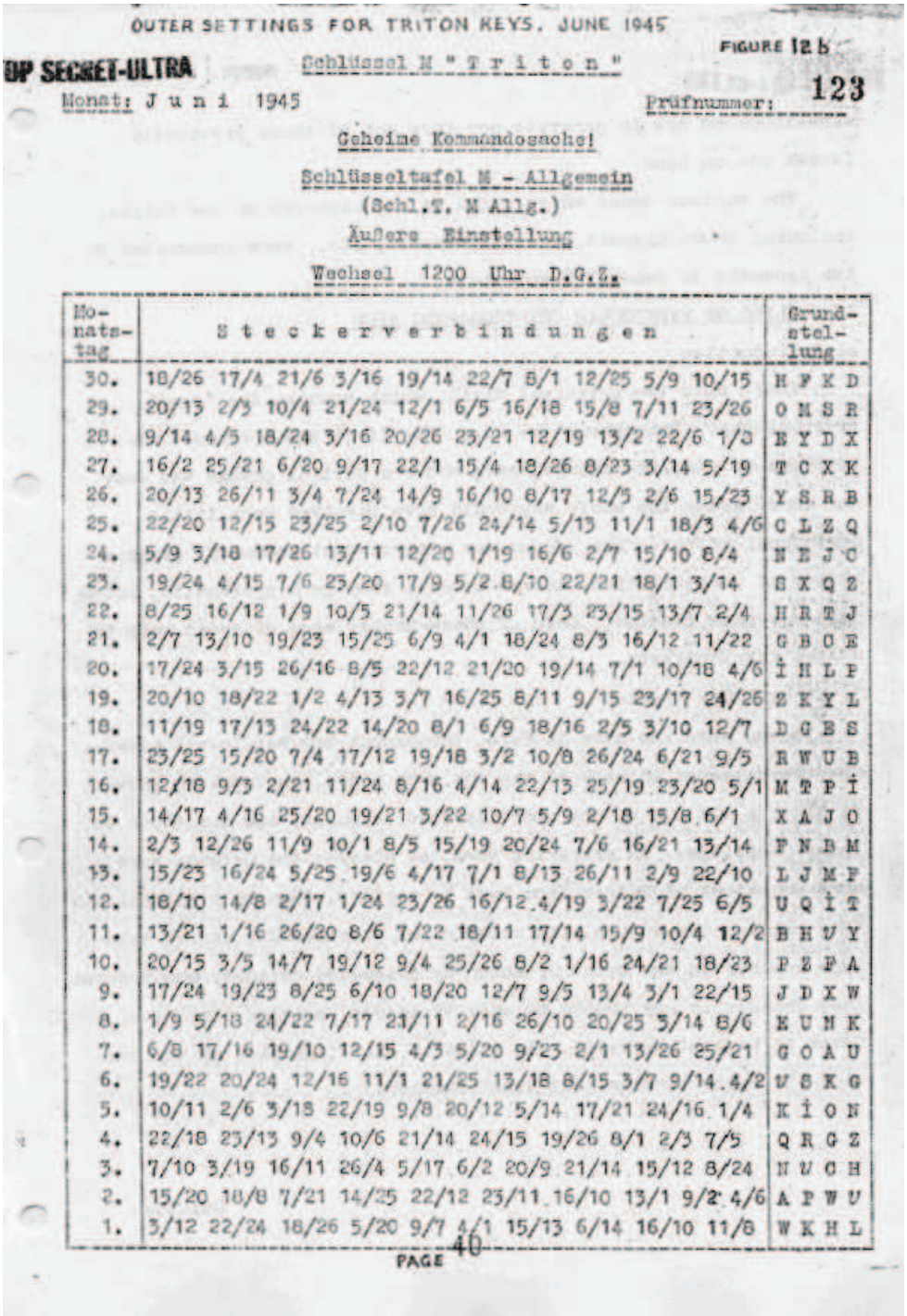
Achtung! Umkehrwalze und Zusatzwalze beachten!

PAGE 39

Fonte: http://users.telenet.be/d.rijmenants/pics/triton1.jpg

Anexo K

Configurações externas “TRITON”



OUTER SETTINGS FOR TRITON KEYS. JUNE 1945

FIGURE 12 b

TOP SECRET-ULTRA

Schlüssel M "T r i t o n"

Monat: J u n i 1945

Prüfnummer: 123

Geheime Kommandosache!

Schlüsseltafel M - Allgemein

(Schl.T. M Allg.)

Äußere Einstellung

Wechsel 1200 Uhr D.G.Z.

Monatstag	S t e c k e r v e r b i n d u n g e n	Grundstellung
30.	18/26 17/4 21/6 3/16 19/14 22/7 8/1 12/25 5/9 10/15	H F K D
29.	20/13 2/3 10/4 21/24 12/1 6/5 16/18 15/8 7/11 23/26	O M S R
28.	9/14 4/5 18/24 3/16 20/26 23/21 12/19 13/2 22/6 1/3	E Y D X
27.	16/2 25/21 6/20 9/17 22/1 15/4 18/26 8/23 3/14 5/19	T C X K
26.	20/13 26/11 3/4 7/24 14/9 16/10 8/17 12/5 2/6 15/23	Y S R B
25.	22/20 12/15 23/25 2/10 7/26 24/14 5/13 11/1 18/3 4/6	C L Z Q
24.	5/9 3/18 17/26 13/11 12/20 1/19 16/6 2/7 15/10 8/4	N E J C
23.	19/24 4/15 7/6 25/20 17/9 5/2 8/10 22/21 18/1 3/14	S X Q Z
22.	8/25 16/12 1/9 10/5 21/14 11/26 17/3 23/15 13/7 2/4	H R T J
21.	2/7 13/10 19/23 15/25 6/9 4/1 18/24 8/3 16/12 11/22	G B O E
20.	17/24 3/15 26/16 8/5 22/12 21/20 19/14 7/1 10/18 4/6	I H L P
19.	20/10 18/22 1/2 4/13 3/7 16/25 8/11 9/15 23/17 24/26	Z K Y L
18.	11/19 17/13 24/22 14/20 8/1 6/9 18/16 2/5 3/10 12/7	D G B S
17.	23/25 15/20 7/4 17/12 19/18 3/2 10/8 26/24 6/21 9/5	R W U B
16.	12/18 9/3 2/21 11/24 8/16 4/14 22/13 25/19 23/20 5/1	M T P I
15.	14/17 4/16 25/20 19/21 3/22 10/7 5/9 2/18 15/8 6/1	X A J O
14.	2/3 12/26 11/9 10/1 8/5 15/19 20/24 7/6 16/21 13/14	F N B M
13.	15/23 16/24 5/25 19/6 4/17 7/1 8/13 26/11 2/9 22/10	L J M F
12.	18/10 14/8 2/17 1/24 23/26 16/12 4/19 3/22 7/25 6/5	U Q I T
11.	13/21 1/16 26/20 8/6 7/22 18/11 17/14 15/9 10/4 12/2	B H V Y
10.	20/15 3/5 14/7 19/12 9/4 25/26 8/2 1/16 24/21 18/23	P Z P A
9.	17/24 19/23 8/25 6/10 18/20 12/7 9/5 13/4 3/1 22/15	J D X W
8.	1/9 5/18 24/22 7/17 21/11 2/16 26/10 20/25 3/14 8/6	K U N K
7.	6/8 17/16 19/10 12/15 4/3 5/20 9/23 2/1 13/26 25/21	G O A U
6.	19/22 20/24 12/16 11/1 21/25 13/18 8/15 3/7 9/14 4/2	V S K G
5.	10/11 2/6 3/18 22/19 9/8 20/12 5/14 17/21 24/16 1/4	K I O N
4.	22/18 23/13 9/4 10/6 21/14 24/15 19/26 8/1 2/3 7/5	Q R G Z
3.	7/10 3/19 16/11 26/4 5/17 6/2 20/9 21/14 15/12 8/24	N V C H
2.	15/20 18/8 7/21 14/25 22/12 23/11 16/10 13/1 9/2 4/6	A P W V
1.	3/12 22/24 18/26 5/20 9/7 4/1 15/13 6/14 16/10 11/8	W K H L

PAGE 40

Fonte: http://users.telenet.be/d.rijmenants/pics/triton2.jpg