

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

THAIS CRISTINE KRISCHER

Um estudo da máquina Enigma

Trabalho de Graduação.

Prof. Dr. Raul Fernando Weber
Orientador

Porto Alegre, janeiro de 2013.

CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Krischer, Thais Cristine

Um estudo da máquina Enigma. / Thais Cristine Krischer. – Porto Alegre: Graduação em Ciência da Computação da UFRGS, 2012.

98 f.: il.

Trabalho de Conclusão (bacharelado) – Universidade Federal do Rio Grande do Sul. Curso de bacharelado em Ciência da Computação, Porto Alegre, BR-RS, 2012. Orientador: Raul Fernando Weber.

1. UFRGS. 2. Máquina Enigma. 3. Máquinas de cifragem. 4. Cifras militares alemãs. 5. Criptoanálise. I. Weber, Raul Fernando. II. Título.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
Reitor: Prof. Carlos Alexandre Netto
Vice-Reitor: Prof. Rui Vicente Oppermann
Pró-Reitor de Graduação: Prof. Sérgio Roberto Kieling Franco
Diretor do Instituto de Informática: Prof. Luís da Cunha Lamb
Coordenador da Ciência da Computação: Prof. Raul Fernando Weber
Bibliotecária-Chefe do Instituto de Informática: Beatriz Regina Bastos Haro

AGRADECIMENTOS

A meus pais, Lenora e Gilberto, por todo o apoio, mesmo quando disfarçado. A meu irmão Cesar, o melhor presente de Natal do mundo e o cara mais sábio que conheço. O amor, a inteligência e o bom humor de vocês são meu esteio e meu porto seguro.

A meu padrinho, tio e amigo Jeová, por sempre ficar do nosso lado e que, com suas palavras de carinho, de apoio e de bom humor, nos passa inspiração, conhecimento e sabedoria.

À Ninora, que acreditou em mim até quando eu não acreditei, ao Dedé, avô amado, ao meu lado em todos os momentos, e à Uxi, que me ensina a ver as diferentes faces da vida com sabedoria e humor. Vocês são fonte de inspiração e os melhores avós do mundo – amo vocês.

A meu namorado José Antônio, pelo apoio, pela atenção e pela paciência. Obrigada pelas inúmeras declarações de amor, de companheirismo e de carinho.

Aos amigos da Esfiles, que mesmo estando distantes, estão presentes nas horas boas e nas horas ruins, sempre com uma palavra de apoio, uma piada e um abraço amigo.

A todos os amigos e colegas, de curso e de caminhada, especialmente ao Ace e ao Felipe Tanus – o carinho e o companheirismo de todos vocês foram muito importantes.

A meu orientador, Raul Weber, professor, chefe e mestre dos magos, por tornar o aprendizado mais interessante e nosso curso mais humano.

Aos professores e funcionários da UFRGS, pelo entusiasmo em transmitir conhecimento e pela vontade constante de melhorar. É um orgulho fazer parte desta Universidade e ter conhecido cada um de vocês.

A todos os professores que tive o privilégio de conhecer, não apenas os das escolas e os das faculdades, mas todos aqueles que doaram seu tempo e sua disposição para passar conhecimento adiante, tornando o mundo um lugar melhor.

E a Deus e a todos os nossos antepassados, que nos guiaram e nos guiam pelo caminho da Verdade, do Bem e do Belo.

SUMÁRIO

AGRADECIMENTOS	3
LISTA DE ABREVIATURAS E SIGLAS	6
LISTA DE FIGURAS.....	7
LISTA DE TABELAS	9
RESUMO.....	10
ABSTRACT	11
1 INTRODUÇÃO	12
2 CIFRAS CLÁSSICAS E O INÍCIO DA MECANIZAÇÃO.....	14
2.1 Cifras de transposição	14
2.2 Cifras de substituição	14
2.2.1 Substituição simples	14
2.2.2 Substituição poligráfica	15
2.2.3 Substituição homófona	15
2.2.4 Substituição por deslocamento	15
2.2.5 Substituição polialfabética.....	15
2.3 A cifra ADFGVX	16
2.4 O início da mecanização da cifragem	17
3 MÁQUINAS DE CIFRAGEM	18
3.1 Máquinas de cifragem baseadas em rotore e seu funcionamento	18
3.2 Máquinas de cifragem baseadas em rotore: o início.....	18
3.3 O início da máquina Enigma	19
3.4 Adoção da Enigma pelas forças armadas alemãs	19
4 A MÁQUINA ENIGMA	21
4.1 Elementos básicos da máquina enigma	21
4.2 Funcionamento de uma máquina Enigma	23
4.3 Configurando uma máquina Enigma	24
4.3.1 Procedimentos operacionais do Exército e da Força Aérea alemães.....	25
4.3.2 Procedimentos operacionais da Marinha alemã	25
4.4 Regras de formatação e abreviações comuns.....	26
4.5 Livro de códigos	27
4.5.1 Livro de Tráfego de Rádio.....	28
4.5.2 Tabelas da Marinha	28
5 PRINCIPAIS MODELOS DA MÁQUINA ENIGMA.....	30
5.1.1 Enigma A.....	32
5.1.2 Enigma B	33
5.1.3 Enigma C	33
5.1.4 Enigma D	34
5.1.5 Enigma I ou Enigma <i>Reichswehr</i> D	34

5.1.6	Enigma II ou Enigma H.....	35
5.1.7	Enigma K.....	36
5.1.8	Enigma Zählwerk ou Enigma G	37
5.1.9	Enigmas M1, M2 e M3.....	38
5.1.10	Enigma M4	39
5.1.11	Enigma T (Tirpitz).....	41
5.1.12	Enigma KD.....	43
5.1.13	Enigma Z	43
5.2	Produção e distribuição das máquinas Enigma.....	44
5.3	Outras máquinas usadas na Segunda Guerra Mundial.....	44
6	SIMULANDO UMA MÁQUINA ENIGMA.....	45
6.1	O que é necessário para criar um simulador	45
6.2	Escolhendo um simulador	46
6.3	Simulação com Enigma Cipher Machine Simulator 7.0.5	47
6.4	Um protótipo de máquina Enigma	54
7	A FORÇA DA CIFRA ENIGMA.....	58
7.1	Configurações possíveis do painel de plugues e dos rotores	58
8	A QUEBRA DO CÓDIGO	61
8.1	Biuro Szyfrów	61
8.1.1	Marian Rejewski.....	63
8.1.2	Bombas criptológicas	67
8.2	Bletchley Park	70
8.2.1	Fraquezas nos procedimentos operacionais.....	71
8.2.2	Fraquezas da máquina Enigma	72
8.2.2.1	Uma letra não pode ser codificada nela mesma	72
8.2.2.2	Passos regulares das rodas.....	72
8.2.2.3	Passos duplos no rotor do meio	72
8.2.2.4	Roda 4 fixa da Enigma M4.....	72
8.2.2.5	Dois entalhes nas rodas extras navais.....	73
8.2.2.6	Uso obrigatório de rodas navais extras.....	73
8.2.2.7	Número fixo de cabos no painel de plugues (Steckerbrett).....	73
8.2.3	Alan Turing	73
8.2.4	Dividindo o problema e as bombas britânicas.....	74
8.2.5	A procura e o uso das informações.....	79
8.2.6	Ultra	80
8.2.7	O fim do segredo	81
9	CONCLUSÃO.....	83
REFERÊNCIAS		84
GLOSSÁRIO		86
ANEXO A LEITURAS RECOMENDADAS.....		90
ANEXO B CURIOSIDADES, PERGUNTAS E RESPOSTAS.....		93
ANEXO C MODELOS COM MAIS DE UM NOME		96
ANEXO D O TELEGRAMA ZIMMERMANN.....		97

LISTA DE ABREVIATURAS E SIGLAS

AG	<i>Aktiengesellschaft</i>
AST	<i>Abwehrstellen</i>
CSKO	<i>Consecutive stecker knock-out</i>
ETW	<i>Eintrittswalze</i>
GC&CS	<i>General Code and Cipher School</i>
GCHQ	<i>Government Communications Headquarters</i>
KDM	<i>Kommando des Meldegebietes</i>
RAF	<i>Royal Air Force</i>
RSHA	<i>Reichssicherheitshauptamt</i>
U-Boot	<i>Unterseeboot</i>
UKW	<i>Umkehrwalze</i>

LISTA DE FIGURAS

Figura 2.1: Exemplo de substituição homófona	15
Figura 2.2: Tableau usado em cifras de substituição polialfabética	16
Figura 2.3: Cilindro de Jefferson.....	17
Figura 3.1: Enigma em uso na batalha da França.....	20
Figura 4.1: Estrutura e componentes de uma máquina Enigma	21
Figura 4.2: Diagrama de um rotor	22
Figura 4.3: Vista esquemática de um rotor.....	22
Figura 4.4: Rotores enfileirados no eixo.	22
Figura 4.5: Rotores reais de uma máquina Enigma.....	23
Figura 4.6: Diagrama simplificado do circuito de uma Enigma I.	23
Figura 4.7: Linguetas e entalhes nos rotores	24
Figura 4.8: Detalhe de um Livro de Tráfego de Rádio.....	28
Figura 4.9: Detalhe de uma tabela da Marinha.....	29
Figura 5.1: Legenda da árvore Enigma	30
Figura 5.2: Árvore Enigma.....	31
Figura 5.3: Página de propaganda promovendo a máquina Enigma	32
Figura 5.4: Modelo A da máquina Enigma	32
Figura 5.5: Modelo B da máquina Enigma.....	33
Figura 5.6: Modelo C da máquina Enigma.....	33
Figura 5.7: Modelo D da máquina Enigma	34
Figura 5.8: Modelo I da máquina Enigma	35
Figura 5.9: Modelo H da máquina Enigma	36
Figura 5.10: Detalhe do modelo K da máquina Enigma	36
Figura 5.11: Modelo G da máquina Enigma	37
Figura 5.12: Rodas genéricas de Enigma e rodas da Zählwerk	38
Figura 5.13: Enigma M3 a bordo de um U-Boot U-124 alemão	39
Figura 5.14: Modelo M4 da máquina Enigma	40
Figura 5.15: Roda adicional (Zusatzwalze) da Enigma M4	41
Figura 5.16: Modelo T da máquina Enigma	42
Figura 5.17: Modelo KD da máquina Enigma	43
Figura 5.18: Modelo Z da máquina Enigma	44
Figura 5.19: Produção e distribuição de máquinas Enigma	44
Figura 6.1: Enigma Simulator v4.3	46
Figura 6.2: Enigma Machine Simulator	47
Figura 6.3: The Enigma Machine	47
Figura 6.4: Máquina Enigma I	48
Figura 6.5: Painel de plugues, 10 pares de letras selecionados.	48
Figura 6.6: Enigma I com painel de plugues sendo usado.	49

Figura 6.7: Máquina Enigma I aberta.....	49
Figura 6.8: Escolha dos rotores e ordem dos rotores: V, III, I	50
Figura 6.9: Configuração dos anéis.....	50
Figura 6.10: Posição inicial dos rotores e início da cifragem com a letra U.....	51
Figura 6.11: Cifrando F, R.	51
Figura 6.12: Cifrando G, S.	51
Figura 6.13: Configuração dos anéis.....	52
Figura 6.14: Anel beta na configuração A-01 e configuração interna completa.....	53
Figura 6.16: Decifrando K, X.....	54
Figura 6.17: Decifrando O, U.....	54
Figura 6.18: Diagrama de funcionamento da máquina Enigma	55
Figura 6.19: Visão geral do protótipo.....	56
Figura 6.20: Teclado de entrada e teclado de saída com LEDs do protótipo.....	56
Figura 6.21: Verso do teclado de entrada e verso do teclado de saída com LEDs.....	56
Figura 6.22: Detalhes da fiação do protótipo.	56
Figura 6.23: Cifragem (decifragem) das letras.....	57
Figura 7.2: Chaves de mensagem cifradas Enigma I	59
Figura 7.3: Chaves de mensagem cifradas Enigma M4	60
Figura 8.1: Marian Rejewski	64
Figura 8.3: Bomba criptológica polonesa	68
Figura 8.4: Bletchley Park	71
Figura 8.7: Circuito completo com 3 máquinas Enigma	76
Figura 8.8: Bomba britânica reconstruída	77
Figura 2: Logotipo da máquina Enigma	93
Figura x: Telegrama Zimmermann.....	98

LISTA DE TABELAS

Tabela 7.1: Combinações possíveis de cabos no painel de plugues	59
Tabela 7.2: Combinações possíveis dos rotores da Enigma I.....	59
Tabela 7.3: Combinações possíveis dos rotores da Enigma M4	60
Tabela 7.1: Chaves de mensagem cifradas	64
Tabela 7.2: Relacionamento parcial de uma chave do dia	65
Tabela 7.3: Relacionamento completo de uma chave do dia	65

RESUMO

Desde os tempos mais remotos existe a necessidade de comunicação de dados sigilosos, seja por motivos políticos, militares, diplomáticos ou comerciais. Embora hoje seja difícil imaginar, já existiu uma época em que as cifragens - que garantiriam esse sigilo – eram feitas manualmente, contando no máximo com o auxílio de dispositivos rudimentares, como cilindros metálicos. Isso começou a mudar no início do século XX com a invenção de máquinas com rotores, que tornaram possíveis as máquinas cifrantes baseadas em princípios eletromecânicos, abrindo uma nova era da cifragem que demanda esforço computacional.

Este trabalho é sobre a principal dessas máquinas, a Enigma, e é um estudo de seu funcionamento, de suas principais características, de sua utilização e da força de sua cifra. É feito ainda um apanhado histórico desde a criação da primeira máquina Enigma até seus códigos serem decifrados pela equipe do *Biuro Szyfrów* polonês e, mais tarde, no centro de criptoanálise criado pelo governo inglês em Bletchley Park.

Palavras-Chave: Máquina Enigma, máquinas de cifragem, cifras militares alemãs, criptoanálise.

A study of the Enigma machine

ABSTRACT

Since ancient times, there is a necessity of secrecy on data communication, if for political, military, diplomatic or commercial reasons. Although nowadays it is difficult to imagine such a fact, there was a time when the ciphers that would ensure this secrecy were done manually, counting only with the aid of rudimentary devices, such as metallic cylinders. That started to change in the beginning of the XX century with the invention of the rotor machines, which enabled cipher machines based on electromechanical principles and opened a new era of ciphering that demands computational efforts.

This work refers to the most important of those machines, the Enigma, and it is a study of its main characteristics, of its operations and utilizations, and of its cipher strength. In addition, there is a historical summary that comes from the creation of the first Enigma machine up to when it had its codes deciphered, by the polish *Biuro Szyfrów* team and, later, by the cryptanalysis center created by the English government in Bletchley Park.

Keywords: Enigma machine, cipher machines, German military ciphers, cryptanalysis.

1 INTRODUÇÃO

Há milhares de anos a humanidade já sentia a necessidade de confidencialidade. Seja por motivos políticos, militares, diplomáticos ou comerciais, o sigilo nas comunicações era – e é – essencial.

Embora hoje seja difícil imaginar, já existiu uma época em que as cifragens, que garantiriam o sigilo nas comunicações, eram feitas manualmente, contando no máximo com o auxílio de mecanismos rudimentares como discos de cifras. No capítulo 2 são abordadas as técnicas clássicas de cifragem e o início da mecanização dessas técnicas.

A partir do início do século XX, com a criação de máquinas com rotores, começou uma nova era da codificação, com máquinas cífrantes baseadas em princípios eletromecânicos. O capítulo 3 mostra os primórdios das máquinas com rotores, que levaram à criação, praticamente ao mesmo tempo e por inventores de países diferentes, das primeiras máquinas de encriptação baseadas em rotores, entre elas a máquina Enigma.

A máquina Enigma acabou se tornando um marco para a Ciência da Computação na medida em que evidenciou que a comunicação secreta não mais poderia ser cifradas ou decifrada apenas com o esforço humano. A criação de cifras, como a da Enigma, que não mais poderiam ser quebradas apenas com a ajuda de lápis e papel, criou a necessidade de máquinas e de esforço computacional que não existia antes.

O objetivo deste trabalho é mostrar o porquê de a máquina Enigma, uma das muitas máquinas de cifragem, ter se tornado a mais famosa e temida. Para isso, são analisados seus elementos básicos, seu funcionamento, os diferentes e complexos procedimentos operacionais necessários para aumentar a segurança no envio e no recebimento de mensagens, sua cifra e, finalmente, a quebra do código.

O capítulo 4 mostra os elementos básicos e o princípio de funcionamento da máquina Enigma, trazendo informações sobre os procedimentos operacionais usados em sua configuração.

O capítulo 5 lista e descreve os principais modelos de máquinas Enigma, trazendo também uma descrição da produção e da distribuição das máquinas e um apanhado de outras máquinas de cifragem também usadas na Segunda Guerra Mundial.

No capítulo 6 é mostrado o funcionamento de uma máquina Enigma através de um software simulador estado da arte, escolhido entre diversos testados. São mostradas as configurações iniciais possíveis e é feita a cifragem de uma palavra passo a passo com uma máquina Enigma I, usada pelo Exército e pela Força Aérea alemães. Em seguida, é demonstrada uma rara compatibilidade entre ela e a Enigma M4 naval. O capítulo

continua com o protótipo de uma máquina Enigma simplificado, desenvolvido com materiais simples.

O capítulo 7 mostra através de cálculos a força da cifra Enigma, evidenciando como a necessidade da quebra da cifra fomentou a criação de dispositivos computacionais de propósito único, mas já avançados, como o ciclômetro, as bombas criptológicas do *Biuro Szyfrów* e as bombas de Bletchley Park.

O capítulo 8 mostra a quebra do código das máquinas Enigma, primeiro pelo *Biuro Szyfrów* polonês e, mais tarde, pela equipe inglesa de Bletchley Park, com explicações dos métodos e dos equipamentos usados pelos criptoanalistas envolvidos. O capítulo mostra ainda como as informações eram obtidas tratadas depois de decifradas.

O trabalho encerra-se com uma reflexão sobre a guerra dentro da Segunda Guerra Mundial travada entre a cifra Enigma e os criptoanalistas responsáveis por quebrá-la. Graças à máquina Enigma, muitos aparelhos e dispositivos que podem ser considerados ancestrais dos computadores modernos foram criados, trazendo avanços importantes para a Ciência da Computação..

2 CIFRAS CLÁSSICAS E O INÍCIO DA MECANIZAÇÃO

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 criptoanalíticas atuais, elas não são geralmente convenientes para uso prático” (1997, p. 238).

2.1 Cifras de transposição

Para uma cifra de transposição simples com período fixo t , a encriptação envolve agrupar o texto claro em blocos de t caracteres, aplicando a cada bloco uma permutação simples e nos números 1 a t . A chave de encriptação é e .

O exemplo mostrado em Menezes mostra de maneira clara como funciona a cifra:

Considere a cifra de transposição simples com $t = 6$ e $e = (6 \ 4 \ 1 \ 3 \ 5 \ 2)$. A mensagem $m = \text{CAESAR}$ é encriptada para $c = \text{RSCEAA}$. A desencriptação usa a permutação inversa $d = (3 \ 6 \ 4 \ 2 \ 5 \ 1)$. A transposição pode ser representada por uma matriz de duas linhas, com a segunda indicando a posição para a qual o elemento indexado pelo correspondente número da primeira é mapeado para: $(1 \ 2 \ 3 \ 4 \ 5 \ 6 | 3 \ 6 \ 4 \ 2 \ 5 \ 1)$. A encriptação pode ser feita escrevendo um bloco de texto claro embaixo do cabeçalho “3 6 4 2 5 1”, e então lendo os caracteres embaixo em ordem numérica (1997, p. 238).

2.2 Cifras de substituição

As cifras clássicas de substituição são a de substituição simples (ou monoalfabética), a de substituição poligráfica, a de substituição homófona, a de substituição por deslocamento e a de substituição polialfabética.

2.2.1 Substituição simples

Uma substituição simples é uma cifra onde cada letra do texto claro é substituída por outra letra no texto cifrado de forma constante, podendo ser expressa escrevendo o alfabeto numa ordem diferente, que se designa alfabeto de substituição. Esse alfabeto pode ser deslocado de um passo fixo (como na cifra de César) ou embaralhado de forma mais complexa. “Embora seja extremamente vulnerável para aplicações práticas, tem valor teórico, educacional e recreativo” (WIKIPEDIA, 2012).

2.2.2 Substituição poligráfica

A cifra de substituição de polígramos utiliza um grupo de caracteres ao invés de um único caractere individual para a substituição da informação. Um exemplo usando trigramas seria a substituição de ABA por RTQ ou KXS. Segundo a Wikipedia (2012), dois exemplos de cifras de substituição poligráficas são a cifra Playfair e a cifra de Hill.

2.2.3 Substituição homófona

Cada letra do alfabeto pode ser correspondida por mais do que um símbolo na substituição homófona. Normalmente as letras com maior frequência possuem um número maior de correspondências, de modo a dificultar uma análise estatística baseada na frequência.

Em uma mensagem em português, por exemplo, poderiam ser utilizados os símbolos de letras maiúsculas, minúsculas e algarismos, num total de 62 símbolos (26+26+10), como no exemplo abaixo (WIKIPEDIA, 2012):

<i>Alfabeto normal:</i>	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
<i>Alfabeto para a cifragem:</i>	8 F H G 3 1 1 L E I w o M X 6 Q P b V 9 a Z S D j r
	z - k m x n B u 0 - - O A v 5 p - R y f 4 g - - - -
	K - s N q - - - J - - a c - 2 - - T e Y h - - - - -
	7 - - - t - - - - - - W - - C - - - - - - - -
	i - - - - - - - - - - d - - - - - - - - - -

Figura 2.1: Exemplo de substituição homófona (WIKIPEDIA, 2012).

2.2.4 Substituição por deslocamento

Essa cifra não usa um valor fixo para a substituição de todas as letras. Segundo a definição usada por Magalhães (2002), na substituição por deslocamento, uma chave indica quantas posições deve-se avançar no alfabeto para substituir cada letra. Diferente da cifra de César, as letras não são trocadas sempre por uma letra n posições à frente no alfabeto.

Para cifrar, por exemplo, a palavra CARRO utilizando o critério de rotação 023, se substituiria C pela letra que está 0 posições à frente no alfabeto, o A pela letra que está 2 posições à frente e assim por diante, repetindo-se o uso da chave até a cifragem completa do texto claro.

2.2.5 Substituição polialfabética

Numa cifra polialfabética, múltiplos alfabetos são usados. Para facilitar, todos os alfabetos são habitualmente escritos numa grande tabela, ou *tableau*, como a mostrada abaixo. O tableau tem 26 x 26 células, gerando 26 alfabetos de cifragem completos.

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

Figura 2.2: Tableau usado em cifras de substituição polialfabética (WIKIPEDIA, 2012).

O método de preencher o *tableau* e escolher que alfabeto usar definem a cifra polialfabética. A mais popular cifra de substituição polialfabética é a cifra de Vigenère, que usa uma série de diferentes cifras de César baseadas nas letras de uma senha.

A invenção dessa cifra é erradamente atribuída a Blaise de Vigenère; ela foi originalmente descrita por Giovan Batista Belaso em seu livro de 1553 “La cifra del. Sig. Giovan Batista Belaso”. Vigenère inventou a cifra de autochave, mas o nome “cifra de Vigenère” acabou associado à cifra polialfabética (WIKIPEDIA, 2012).

A ideia usada na cifra de Vigenère é que as cifras polialfabéticas são mais difíceis de quebrar por análise de frequência, mas têm uma fraqueza se a chave é curta e constantemente repetida: como resultado, palavras comuns vão provavelmente aparecer criptografadas segundo as mesmas letras da chave, levando à descoberta de padrões repetidos no texto (WIKIPEDIA, 2012).

Ainda segundo a Wikipedia (2012), durante mais de 300 anos, a cifra de Vigenère foi julgada inquebrável, mas graças ao trabalho de Charles Babbage (1791-1871) e de Friedrich Kasiski (1805-1881), que de maneiras independentes encontraram um modo de resolvê-la, a cifra se tornou obsoleta em meados do século XIX.

Outros métodos polialfabéticos incluem a cifra de Gronsfeld, que é idêntica à de Vigenère usando apenas 10 alfabetos e chave numérica, a cifra de autochave, que mistura texto claro com uma chave para evitar a periodicidade e a cifra de chave corrente, com uma chave muito longa, obtida a partir de um texto (WIKIPEDIA, 2012).

2.3 A 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

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 (2011, p. 122).

2.4 O início da mecanização da cifragem

Utilizando-se de uma cifra clássica, o primeiro disco de cifras foi construído no século XV pelo arquiteto italiano Leon Battista Alberti (1404-1472). O aparato consistia de dois discos de cobre concêntricos, de tamanhos ligeiramente diferentes, com um alfabeto gravado em cada um. O princípio usado era a cifra de deslocamento simples de César. Uma roda de codificação semelhante foi usada pelos confederados na Guerra de Secessão Americana (1861-1865).

Por volta de 1795, Thomas Jefferson (1743-1826) inventou um cilindro para codificação, o cilindro de Jefferson, que consistia em 36 discos, com as letras do alfabeto impressas em diferentes sequências, montados num eixo. Esse mecanismo implementava uma cifra de substituição polialfabética .



Figura 2.3: Cilindro de Jefferson (WIKIPEDIA, 2012).

Esses aparelhos, no entanto, meramente mecanizavam o trabalho, e não tornavam as mensagens menos impenetráveis ao ataque apenas pelo fato de terem sido geradas por um dispositivo. Logo, tornava-se necessário um novo rumo nas codificações, com novas cifras e máquinas que não apenas acelerassem o processo de codificação e decodificação, mas que aumentassem a segurança do texto criptografado (LEAVITT, 2007).

3 MÁQUINAS DE CIFRAGEM

3.1 Máquinas de cifragem baseadas em rotores e seu funcionamento

A máquina de rotores foi inventada em 1915 na Holanda por dois oficiais da Marinha, R.P.C. Sprengler (1875-1955) e Theo van Hendel (1875-1939) (CRYPTO, 2012).

Os primeiros dispositivos que podem ser classificados como máquinas de cifragem foram os baseados em princípios eletromecânicos e tinham como base o uso de rotores.

Segundo Menezes (1997, p. 243), uma máquina de rotores genérica simplificada consiste em certo número de rotores, cada um implementando uma diferente substituição monoalfabética, mapeando um caractere de sua entrada para sua saída. Um caractere de texto claro que entra no primeiro rotor gera uma saída que é a entrada do segundo rotor, e assim por diante, até que se chegue ao caractere cifrado final. Um banco de rotores de posição fixa implementa em conjunto uma substituição monoalfabética, composta das substituições definidas por cada rotor.

Para uma substituição polialfabética, o encriptamento de cada caractere do texto claro tem que fazer com que vários rotores se movam. O movimento mais simples desse tipo pode ser exemplificado como o do odômetro de um carro, com apenas um rotor sendo movido até que uma completa revolução seja dada, quando então o rotor adjacente dá um passo, e assim sucessivamente.

A chave da cifra é definida pelas substituições monoalfabéticas determinadas pela fiação física do rotor e as posições iniciais do rotor. Mudar a ordem dos rotores aumenta a variabilidade, assim como a disponibilidade de mais rotores do que os que estão sendo utilizados (MENEZES, 1997, p. 243-244).

3.2 Máquinas de cifragem baseadas em rotores: o início

Assim como o uso das ondas de rádio, descoberto em vários lugares praticamente ao mesmo tempo, a criação de máquinas que automatizavam o trabalho de cifragem também floresceu em mais de um lugar na mesma época, e indivíduos de diferentes nacionalidades foram responsáveis pelo desenvolvimento das primeiras máquinas de cifragem baseadas no princípio de rotores.

Quatro inventores de quatro nacionalidades diferentes tiveram quase ao mesmo tempo a ideia de usar uma máquina com rotores como máquina de cifragem: Edward Hebern (1869-1952), dos Estados Unidos, em 1917; Arthur Scherbius (1878-1929), da Alemanha, em 1918; Hugo Alexander Koch (1870-1928), da Holanda, em 1919 e Arvid Gerhard Damm (?-1927), da Suécia, em 1919 (MENEZES, 1997, p. 244-245).

Segundo Menezes (1997, p. 244-245), em 1918 o norte americano Edward Hebern (1869-1952) construiu o primeiro aparato usando rotores, baseado em uma máquina de escrever modificada com conexões cabeadas para gerar uma substituição monoalfabética, com a saída usando originalmente indicadores iluminados.

A primeira patente de rotor foi preenchida em 1921, quando a *Hebern Electric Code, Inc.* tornou-se a primeira companhia de máquinas de cifragem norte americana. A Marinha do país chegou a usar algumas das máquinas de cinco rotores entre 1929-1930 e alguns anos depois, mas a companhia acabou falindo em 1926.

Em 07 de outubro de 1919, Hugo Alexander Koch patenteou na Holanda uma “máquina de escrever secreta” com princípios de rotores, que acabou não sendo produzida. Três dias depois de Koch, Arvid Gerhard Damm preencheria na Suécia uma patente descrevendo um dispositivo com dois rotores, que mais tarde se tornaria a base da máquina de rotor B-21, usada pelo Exército da Suécia (MENEZES, 1997, p. 245).

3.3 O início da máquina Enigma

Em 23 de fevereiro de 1918, o engenheiro elétrico e inventor alemão Arthur Scherbius submeteu sua patente para uma máquina de cifragem usando rotores.

Na mesma época, em 1918, Scherbius fundou a empresa Scherbius & Ritter, junto com seu amigo Richard Ritter. Singh (2011) relata o começo:

Era uma firma de engenharia inovadora que trabalhava que trabalhava com tudo, de turbinas a travesseiros aquecidos. Scherbius estava encarregado da área de pesquisa e desenvolvimento e buscava sempre novas oportunidades. Um de seus projetos era substituir os sistemas de criptografia inadequados, usados na Primeira Guerra Mundial, trocando-se as cifras de papel e lápis por uma forma de cifragem que usasse a tecnologia do século XX. [...] ele desenvolveu uma máquina criptográfica que era, basicamente, uma versão elétrica do disco de cifras de Alberti. Chamada de Enigma, a invenção de Scherbius se tornaria o mais terrível sistema de cifragem da História.

Scherbius e Ritter procuraram a Marinha alemã, mas não houve interesse pela máquina. Os oficiais acreditavam que a máquina provia boa segurança, mas não acharam que houvesse tráfego suficiente de informações para torná-la necessária.

Segundo uma sugestão dos próprios quadros da Marinha, Scherbius procurou o Escritório de Relações Exteriores, oferecendo a Enigma como uma solução para cifragem de correspondências diplomáticas. Mais uma vez, não houve interesse.

Scherbius e Ritter então transferiram os direitos de patente para a *Gewerkschaft Securitas*. Em 09 de julho de 1923, a *Securitas* fundou a *Chiffriermaschinen Aktien-Gesellschaft* (ou Máquinas de Cifragem Sociedade Anônima), em cuja diretoria estavam Scherbius e Ritter.

Em 1927, Scherbius adquiriu a patente do holandês Koch, que havia desenvolvido em 1919 o princípio dos rotores de forma autônoma. Quando Scherbius morreu em um acidente de carruagem em 1929, foi Willi Korn quem deu continuidade aos negócios.

3.4 Adoção da Enigma pelas forças armadas alemãs

Embora não tenha vingado comercialmente, a máquina Enigma, com algumas alterações, foi finalmente adotada pela Marinha alemã em 1926 (KAHN, 1991, p. 40) e, alguns anos mais tarde, em 1928, e com mais alterações, pelo Exército. Citando Tkotz:

A partir de 1933, a Enigma estava em uso não só no exército e na marinha, como também no serviço diplomático [...] Os modelos usados na inteligência eram diferentes dos modelos comerciais e suas configurações eram segredo de Estado (2005, p.247).

Estima-se que entre 30 e 200 mil máquinas tenham sido produzidas (CRYPTO, 2012), e que tenham sido as mais utilizadas durante a Segunda Guerra Mundial, embora houvesse ainda outros métodos de cifragem menos conhecidos, e as informações estratégicas fossem “submetidas a poucos dispositivos mais complexos” (TKOTZ, 2005).

Citando Crypto (2012), com relação a patentes, embora pareça que a maioria das relacionadas às máquinas Enigma tenha sido preenchida antes da Segunda Guerra Mundial, na verdade muitas patentes foram preenchidas secretamente durante a guerra. Com o fim da guerra, muitas dessas patentes foram ou destruídas ou confiscadas pelo inimigo.



Figura 3.1: Enigma em uso na batalha da França (WIKIPEDIA, 2012).

4 A MÁQUINA ENIGMA

Como outras máquinas com rotores, a máquina Enigma é uma combinação de subsistemas elétricos e mecânicos. (WIKIPEDIA, 2012).

4.1 Elementos básicos da máquina enigma

Uma máquina Enigma genérica tinha seis componentes principais: um teclado, similar ao de uma máquina de escrever, um painel com pequenas lâmpadas, uma para cada letra, um conjunto de rotores (rodas, discos, rolos ou misturadores, usados como sinônimos), um refletor, um painel de plugues e uma bateria (CRYPTOOL, 2012).

O teclado servia para a digitação dos textos claros, a unidade central de cifragem composta de rotores em fila em um eixo transformava os caracteres claros em caracteres cifrados e o quadro de lâmpadas mostrava os caracteres cifrados.

Quando uma tecla era pressionada, um circuito se fechava, com a corrente fluindo através de vários componentes até finalmente fazer com que uma lâmpada fosse acesa no mostrador, indicando a letra de saída. (WIKIPEDIA, 2012).

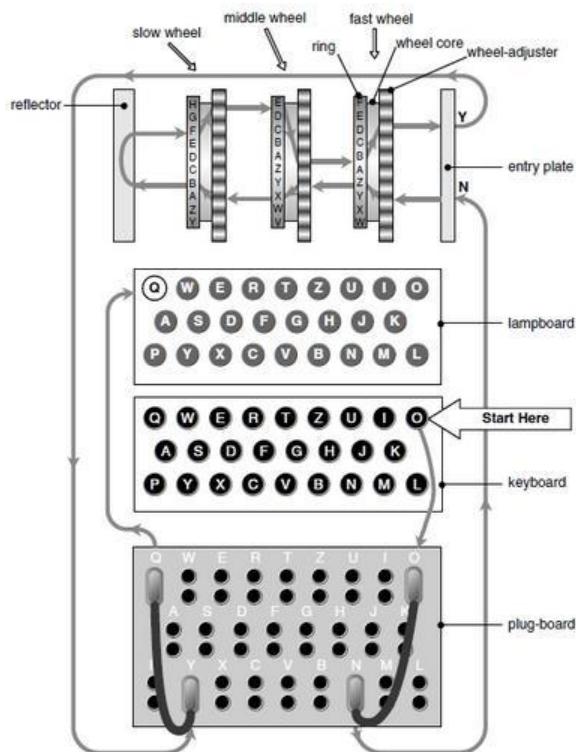


Figura 4.1: Estrutura e componentes de uma máquina Enigma (CRYPTOOL, 2012).

Os rotores que compunham a unidade de cifragem, considerados a parte principal da máquina Enigma, eram “discos grossos com contatos de entrada e de saída em ambas as faces e ligações elétricas entre os contatos. Esses contatos não são ligados aos pares, mas embaralhados.” (TKOTZ, 2005, p. 248).

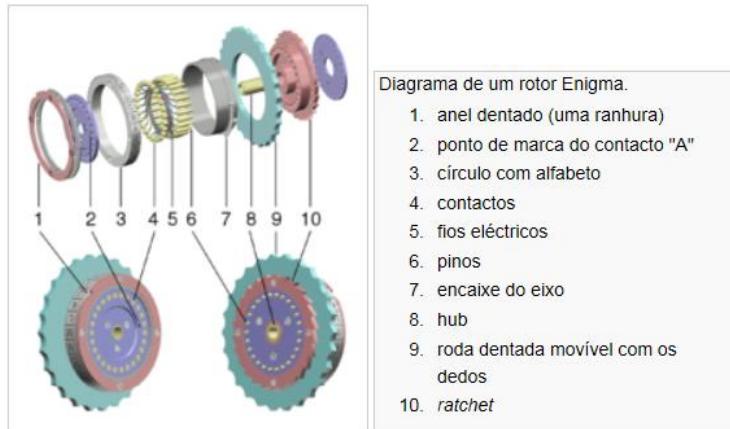


Figura 4.2: Diagrama de um rotor (WIKIPEDIA, 2012).

No interior de cada rotor, um conjunto de 26 fios elétricos ligava cada pino de metal saliente disposto em círculo de um lado a um contato elétrico do outro lado, segundo um padrão fixo complexo. Cada uma dessas ligações representava uma letra do alfabeto, de A a Z, e cada rotor tinha um esquema diferente (WIKIPEDIA, 2012).



Figura 4.3: Vista esquemática de um rotor (CRYPTO, 2012).

Cada rotor tinha aproximadamente 10 cm de diâmetro e era feito de borracha dura ou baquelite (um tipo antigo de plástico). Quando enfileirados no eixo, os pinos de um rotor tocavam nos contatos do rotor vizinho, formando um circuito elétrico (WIKIPEDIA, 2012).

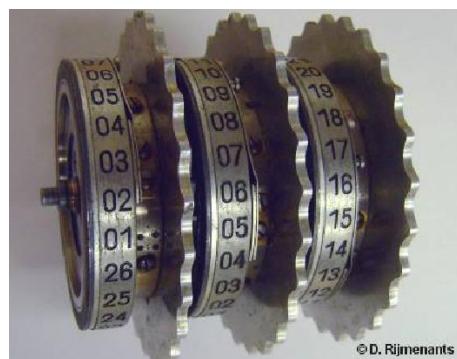


Figura 4.4: Rotores enfileirados no eixo (RIJMENANTS, 2012).

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. Quando passou a ser possível intercambiar rotores, eles passaram a ter uma numeração baseada em algarismos romanos.

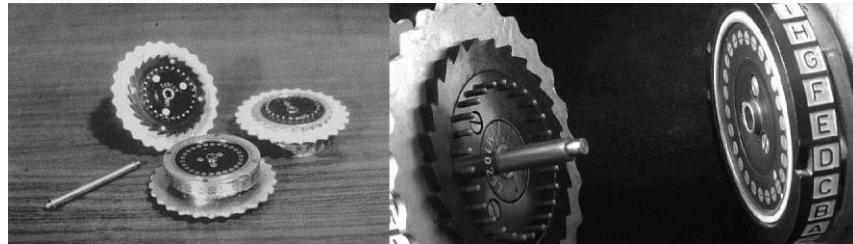


Figura 4.5: Rotores reais de uma máquina Enigma (WIKIPEDIA, 2012).

Caso os rotores ficassem estáticos, a Enigma implementaria uma cifra de substituição simples. A genialidade do sistema consistia em os rotores serem girados depois de cada letra ser cifrada, de forma que cada tecla pressionada cause pelo menos um giro do rotor mais à direita.

A cada 26 vezes que este rotor era girado, o rotor adjacente à esquerda era girado uma vez. Após este ser girado 26 vezes, seu vizinho à esquerda giraria uma vez. Ou seja, era implementada uma cifra de substituição polialfabética (WIKIPEDIA, 2012).

Vale lembrar que houve diversos modelos diferentes de máquinas Enigma, e nem todos eles funcionavam com para-passo de 26.

O painel de plugues, usado nas máquinas Enigma militares, servia para trocar letras aos pares, e funcionava como uma segurança adicional para a cifra.

4.2 Funcionamento de uma máquina Enigma

Existiam diversos modelos de máquinas Enigmas, com variações entre eles. Essas diferenças faziam com que uma mensagem codificada usando um modelo de Enigma não pudesse normalmente ser decodificada usando outro.

O diagrama de circuito de uma máquina Enigma padrão a seguir tem como fonte Crypto (2012), e mostra o funcionamento de uma Enigma I do Exército.

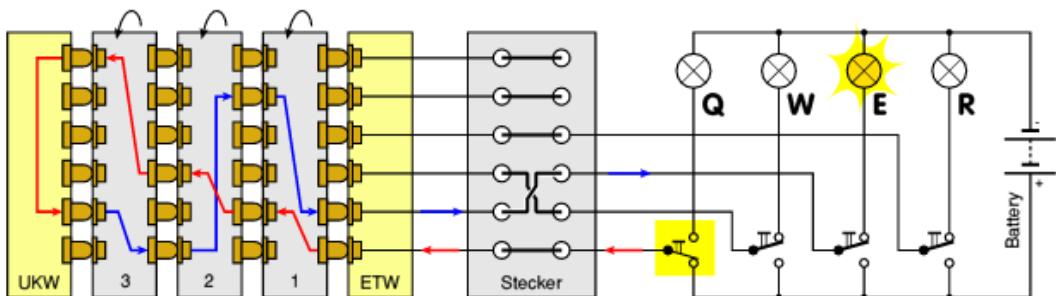


Figura 4.6: Diagrama simplificado do circuito de uma Enigma I (CRYPTO, 2012).

As letras lidas do teclado eram misturadas por um conjunto de rodas rotativas, cada uma com 26 contatos em cada lado. Cada contato de um lado estava ligado (cabeados) a

um contato do outro lado de uma forma aleatória. Alguns modelos, como a Enigma de Serviço e a Enigma M3, tinham três rotores. Já o modelo M4, usado mais tarde na guerra exclusivamente pelos U-Boots alemães, tinha quatro rotores (CRYPTO, 2012).

Segundo a Wikipedia (2012), cada vez que uma tecla era pressionada, a roda mais à direita era girada em um passo, o que resultava em um mapeamento diferente dos fios internos. Como resultado, cada nova letra era codificada de modo diferente.

Cada roda tinha uma ou mais ranhuras, que podiam fazer com que a roda seguinte fosse movida em uma posição também. Se uma roda tinha apenas um entalhe, ela precisa completar uma volta completa antes que a roda da esquerda gire um passo.

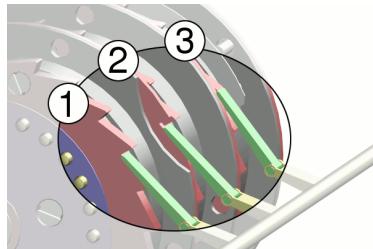


Figura 4.7: Linguetas e entalhes nos rotores (WIKIPEDIA, 2012).

O teclado na maior parte das máquinas Enigma era composto por 26 teclas, de A a Z. Sempre que uma tecla, no exemplo acima Q, fosse pressionada, as rodas eram movidas para uma nova posição e um contato era fechado, gerando uma corrente elétrica. Os fios das 26 teclas eram conectados a uma roda fixa chamada rotor de entrada ou *Eintrittswalze* (ETW). A ordem em que as teclas eram ligadas aos contatos no ETW variava entre os diferentes modelos de máquinas Enigma (CRYPTO, 2012).

Ainda segundo Crypto (2012), após passar pelo ETW, a corrente entrava no rotor mais à direita através de um de seus contatos no lado direito. O cabeamento interno daquele rotor traduzia a corrente para um dos contatos em seu lado esquerdo e, a partir daí, a corrente era entregue para a roda seguinte, e assim por diante.

À esquerda dos rotores ficava o refletor, ou *Umkehrwalze* (UKW). Esta roda enviava a corrente de volta para as rodas rotativas, mas desta vez a corrente fluía da esquerda para a direita, até que atingisse o ETW novamente. A partir do ETW, a corrente vai para o painel de lâmpadas onde a letra correspondente (E, no exemplo acima) será acesa. É inerente ao design que uma letra nunca seja codificada nela mesma (CRYPTO, 2012).

4.3 Configurando uma máquina Enigma

Antes de iniciar o processo de codificação, a Enigma precisava ser configurada de uma maneira conhecida por ambos os lados envolvidos na comunicação. Isto significava a ordem dos rotores (*Walzenlage*), o ajuste do anel (*Ringstellung*), que colocava na posição combinada os anéis de índice ajustáveis de cada rotor, a posição inicial de cada um dos rotores (*Grundstellung*) e a conexão dos plugues (*Steckerverbindungen*). Em versões, era ainda necessário o ajuste do cabeamento do refletor reconfigurável.

As máquinas Enigma comerciais não possuíam painel de plugues, restrito aos modelos usados pelas Forças Armadas. O painel de plugues (*Steckerbrett*) permitia a

troca de zero a treze pares de letras entre si usando cabos. Rotineiramente, as máquinas Enigma do Exército usavam 6 cabos, com dois de reserva (KAHN, 1991, p. 42).

Os procedimentos operacionais, no entanto, variavam bastante entre os diversos modelos de máquinas Enigma sendo usados pelos diferentes ramos das Forças Armadas em suas redes de comunicação próprias.

4.3.1 Procedimentos operacionais do Exército e da Força Aérea alemães

O Exército e a Força Aérea alemães utilizavam procedimentos padrão para transmitir e receber as mensagens de maneira segura: tanto o emissor quanto o receptor tinham de colocar sua máquina Enigma exatamente da mesma maneira. Essas definições eram distribuídas em folhas com as chaves. “Por razões de segurança, as diferentes partes das Forças Armadas tinham suas próprias redes, com diferentes folhas de chave e com cada rede tendo seu próprio nome de código” (RIJMENTANTS, 2012).

Segundo Rijmenants:

As folhas de chave eram distribuídas de antemão, e continham as configurações básicas para um mês inteiro, separadas por dia. Em geral, as folhas com as chaves vinham sob a custódia de um oficial, responsável por estabelecer os rotores de máquinas e configurações do anel. Após a instalação, ele podia bloquear o painel frontal da máquina com uma chave. O operador poderia selecionar apenas a posição inicial do rotor (2012).

4.3.2 Procedimentos operacionais da Marinha alemã

A Marinha alemã usou durante a Segunda Guerra Mundial uma variedade de livros de código em combinação com as máquinas Enigma. Os procedimentos para cifrar as mensagens e a definição das chaves eram mais complexos e elaborados do que os procedimentos do Exército e os da Força Aérea, o que tornou a comunicação da *Kriegsmarine* uma das mais difíceis de ser quebradas em Bletchley Park.

Os procedimentos consistiam de configurações de chave da Enigma, do livro com os grupos para identificar a chave para o receptor, tabelas com esses grupos de identificação, tabelas com pares de letras a serem trocados, livros de mensagens curtas, livros de código climático, etc.

Os procedimentos operacionais instruíam também sobre a utilização de, pelo menos, uma das 3 rodas navais (VI-VIII) a cada dia, e essa roda não podia ser usada na mesma posição em dias sucessivos. Isso era conhecido em Bletchley Park e reduzia o número de permutações possíveis (CRYPTO, 2012), como será visto mais à frente.

O operador devia primeiro selecionar uma chave de mensagem a partir de uma série de livros de códigos e tabelas. Cada mensagem era convertida em uma série de mensagens curtas, que eram traduzidas em grupos de letras.

Conforme Rijmenants (2012), as folhas de chaves usadas pela Marinha consistiam de duas partes: *Schlüsseltafel M Algemein - Innere Einstellung*: configurações internas, continham os três rotores e as configurações dos anéis, a escolha do rotor fino beta ou gama e a posição do refletor, tudo isto apenas para os dias ímpares do mês, e *Schlüsseltafel M Algemein - Äussere Einstellung*: configurações externas, continham os plugues e a posição básica inicial para cada dia do mês

Uma chave adicional existiu para os oficiais e uma especial, *Schlüssel M NIXE*, foi usada para a comunicação privada entre o capitão e o comando U-Boot, sem que outros U-Boots pudessem ser capazes de ler a mensagem.

Ainda conforme Rijmenants (2012), o sistema de grupos para identificar a chave para o receptor (*Kenngruppen*) da Marinha era completamente diferente do usado pelo Exército e pela Força Aérea. Em adição às folhas de chaves, era usado um livro com os grupos para identificar a chave para o receptor (*Kenngruppenbuch*) nas redes de cifras principais para determinar a chave da mensagem.

O operador tinha de selecionar dois grupos de três letras do *Kenngruppenbuch*. Tanto o *Schlüsselkenngruppe* (grupo identificador de chaves, para identificar qual chave foi usada) quanto o *Verfahrenkenngruppe* (grupo identificador de codificação, para obter a chave de mensagem) tinham suas próprias tabelas.

A Enigma era então ajustada para a posição base para o dia (*Grundstellung*) e o operador colocava o *Verfahrenkenngruppe*, a fim de obter a chave de mensagem. Os dois trigramas mencionados acima (*Schlüsselkenngruppe* e *Verfahrenkenngruppe*) eram utilizados como o indicador de mensagem.

Esse indicador da mensagem era submetido a uma encriptação por substituição adicional com uma tabela de conversão de duas letras (*Doppelbuchstabentauschtafeln*). Um conjunto de tabelas bigramas consistia de nove tabelas diferentes. Um calendário determinava qual das tabelas de substituição seria usada determinado dia. A tabela bigrama era recíproca, o que fazia com que se um bigrama fosse AB fosse codificado em KW, KW seria decodificado em AB.

O operador escrevia os dois trigramas do indicador da mensagem um embaixo do outro, mas adicionava uma letra aleatória qualquer no começo do primeiro trígrama e uma letra aleatória qualquer no fim do segundo trígrama. Para codificar, os bigramas eram tomados verticalmente do indicador da mensagem e codificados de acordo com a tabela de bigramas. Os dois grupos de quatro letras resultantes (o indicador da mensagem codificado) eram adicionados ao começo da mensagem e eram repetidos ao seu final.

Em adição a isto, as mensagens do U-Boats eram convertidas em mensagens menores usando *Kurzsignalheft* (folheto de mensagens curtas), *Kenngruppenheft* (folheto, não ser confundido com *Kenngruppenbuch*) e o *Wetterkurzschlüssel* (chaves de previsão do tempo).

A rede de máquinas Enigma M4 era chamada Triton, ou *Shark*, como era chamada em Bletchley Park (RIJMENANTS, 2012).

4.4 Regras de formatação e abreviações comuns

O Exército e a Força Aérea 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.

O Exército usava as seguintes abreviaturas (RIJMENANTS, 2012):

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.

Para tornar ainda mais difícil a criptoanálise, foram introduzidas mais complicações aos procedimentos de mensagens das Forças Armadas (*Wehrmacht*) durante a guerra.

Como o terceiro rotor (mais à esquerda) avançava apenas a cada 676 passos, ele não tinha muito efeito durante a cifragem, uma vez que as mensagens longas haviam sido proibidas por razões de segurança. No entanto, o operador podia cifrar um código de quatro letras na mensagem e mudar a posição do rotor da esquerda. Quando o operador recebendo a mensagem encontrasse esse conjunto de letras, ele também trocaria o rotor mais à esquerda para outra posição.

Outra complicação, adicionada ao final da guerra, era a colocação dos rotores “com rotação”. A cada 8 horas, uma dada posição dos rotores era girada no sentido horário.

A Marinha formatava suas mensagens em grupos de quatro letras. Eram utilizadas as seguintes abreviaturas (RIJMENANTS, 2012):

X = período

Y = vírgula

UD = ponto de interrogação

XX = dois pontos

YY = traço, hífen

KK ** KK = parênteses

J ***** J = acentuação

4.5 Livro de códigos

Um livro de códigos é um documento utilizado para a implementação de um código, e é um método muito antigo e eficaz para ocultar o conteúdo de uma mensagem. Ele contém uma tabela de referência para a codificação e a decodificação. Para decifrar

mensagens escritas em código, cópias correspondentes do livro de código devem estar disponíveis em cada uma das extremidades da comunicação (WIKIPEDIA, 2012).

Um livro de códigos é normalmente organizado como um dicionário e é constituído de duas partes: uma para a conversão de texto simples para texto cifrado, a outra para a conversão do texto cifrado em texto simples. Sobre os livros de código, conforme Crypto:

Em muitos casos, as palavras usadas com frequência ou mesmo frases completas são substituídas por abreviações de três ou cinco letras. Isso tornaria mais fácil (e mais barato) enviar uma mensagem a uma grande distância. [...] Durante a Segunda Guerra, os livros de códigos eram usados para cifrar uma mensagem, algumas vezes em adição a outros métodos de criptografia, tais como a Enigma ou cifras feitas à mão (2012).

Quebrar um livro de códigos é uma tarefa difícil para um criptoanalista, mas uma vez que o livro de códigos seja capturado, o segredo é completamente perdido. Eles podem, portanto, ser classificados como Segurança por Obscuridade: por si sós, não são muito seguros, mas, quando utilizados em combinação com outros métodos de codificação, podem se tornar o pesadelo de um quebrador de códigos mediano (CRYPTO, 2012).

4.5.1 Livro de Tráfego de Rádio

Durante a Segunda Guerra Mundial, as Forças Armadas alemãs usaram o *Funkverkehrsheft für die Küstenverteidigung*, ou Livro de Tráfego de Rádio para Defesa Costeira, junto com outros métodos de codificação. Ele tornava as mensagens mais curtas e mais eficientes, criando ainda uma camada extra de obscuridade em uma mensagem criptografada.

Ele continha certo número de entradas que podiam ser alteradas manualmente. O livro mostrado abaixo foi usado pelos alemães para a defesa da costa holandesa. Os nomes de cidades e vilas estão escritos no livro a lápis (CRYPTO, 2012).



Figura 4.8: Detalhe de um Livro de Tráfego de Rádio (CRYPTO, 2012).

4.5.2 Tabelas da Marinha

Os livros de código do departamento U-Boot da Marinha eram impressos com tinta vermelha solúvel em água sobre papel vermelho claro. Quando deixados para trás em submarinos prestes a afundar, os livros de código se desfariam automaticamente, o que tornava muito difícil a captura de um deles (CRYPTO, 2012).

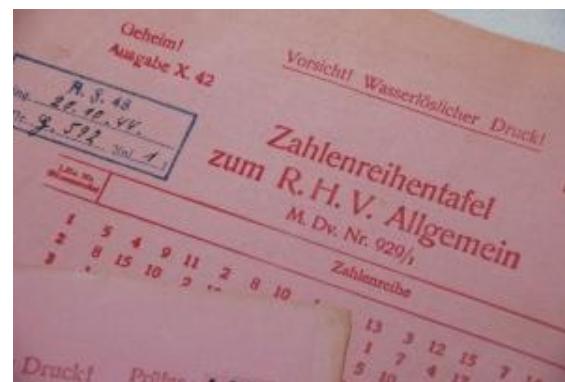


Figura 4.9: Detalhe de uma tabela da Marinha (CRYPTO, 2012).

A expressão “Vorsicht! Wasserlöslicher Druck!” na parte superior da página (exemplo abaixo) avisava: “Atenção! Impressão solúvel em água!”.

5 PRINCIPAIS MODELOS DA MÁQUINA ENIGMA

Mais de 50 modelos de máquina Enigma foram desenvolvidos e fabricados ao longo dos anos (CRYPTO, 2012). Segundo o Tkotz (2012, p. 247), foram fabricadas entre 100 e 200 mil máquinas.

A árvore de derivações de máquinas Enigma mostrada abaixo é um resumo dos principais modelos e suas características. A árvore foi desenvolvida por Paul Reuvers e Frode Weirud e está disponível em Crypto (2012).

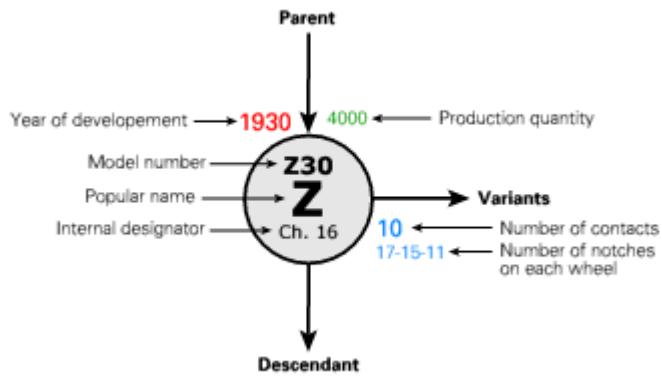


Figura 5.1: Legenda da árvore Enigma (CRYPTO, 2012).

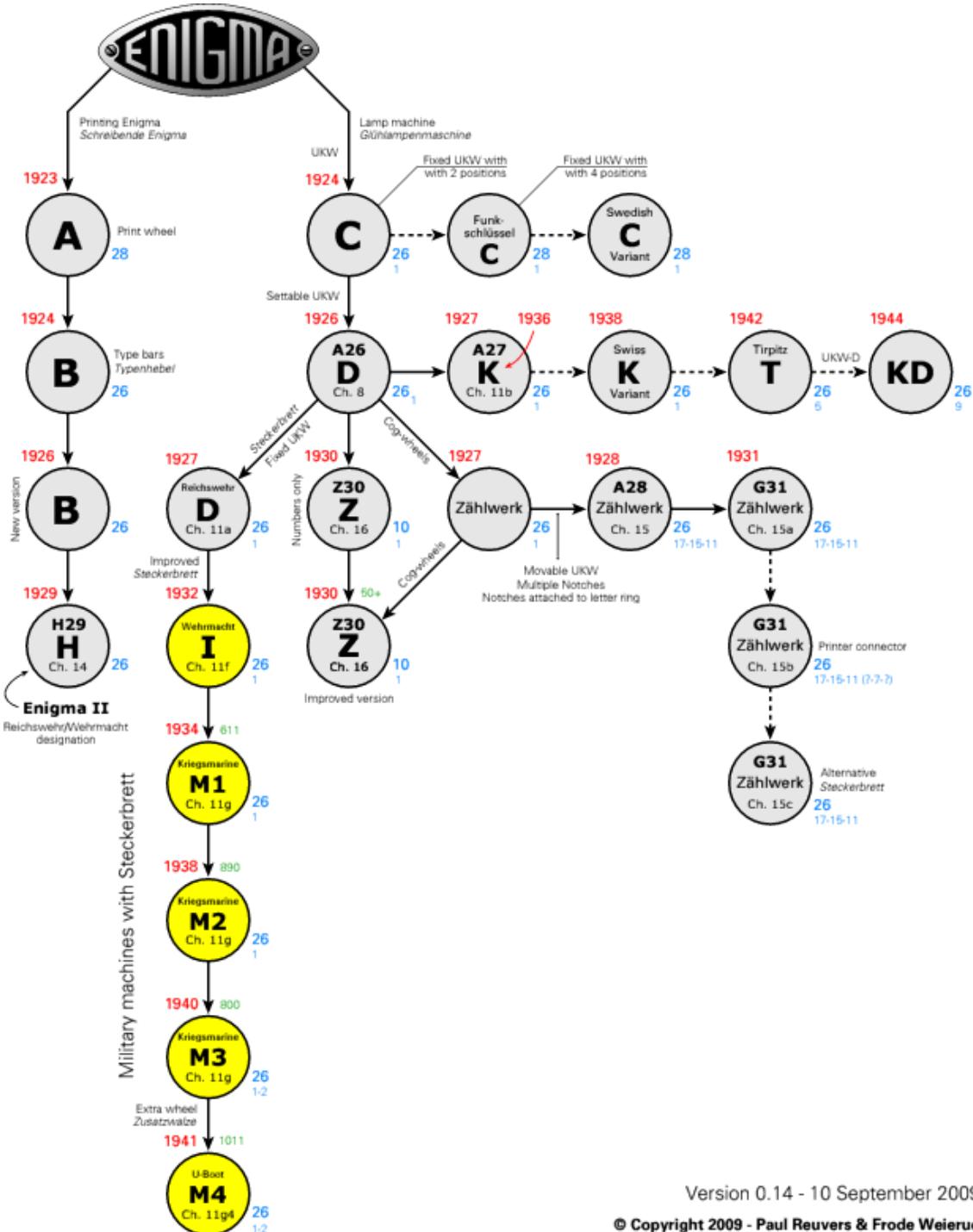


Figura 5.2: Árvore Enigma (CRYPTO, 2012).

A descrição a seguir mostra as características dos principais modelos mostrados na árvore, seguindo o material de Crypto (2012).

5.1.1 Enigma A

A Enigma A foi a primeira máquina vendida com a marca Enigma e foi lançada no mercado em 1923, mesmo ano em que foi exibida no Congresso da União Postal Internacional, em Berna, na Suíça. Ela era grande, pesada e volumosa, e sua entrada de dados era uma máquina de escrever regular, com saída de dados diretamente em papel.



Figura 5.3: Página de propaganda promovendo a máquina Enigma (KRUH, 2002).

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. A máquina foi desenvolvida pela companhia berlimense Scherbius & Ritter, mas foi colocada em produção pela também berlimense *Gewerkschaft Securitas* (que mais tarde se tornaria *Chiffriermaschinen AG*).

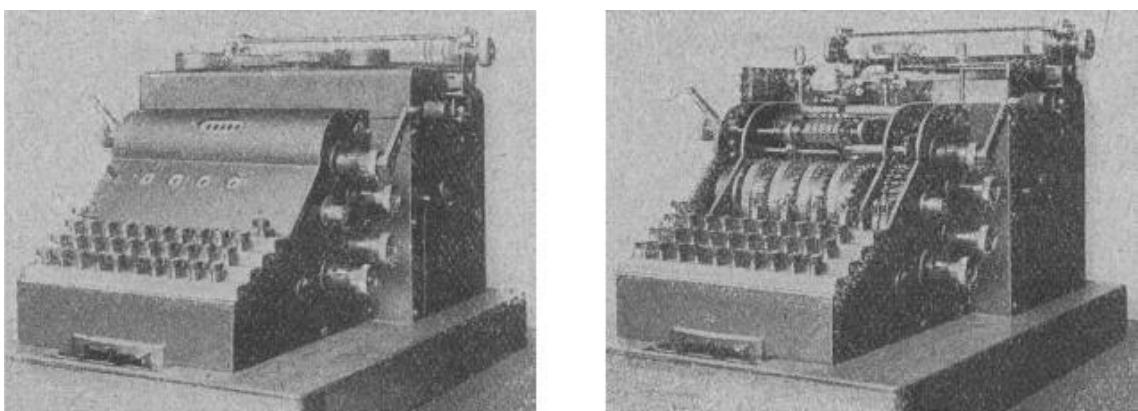


Figura 5.4: Modelo A da máquina Enigma (CRYPTO, 2012).

5.1.2 Enigma B

O modelo foi desenvolvido em 1924, era bastante pesado e também imprimia diretamente no papel sua saída. 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 e era 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.

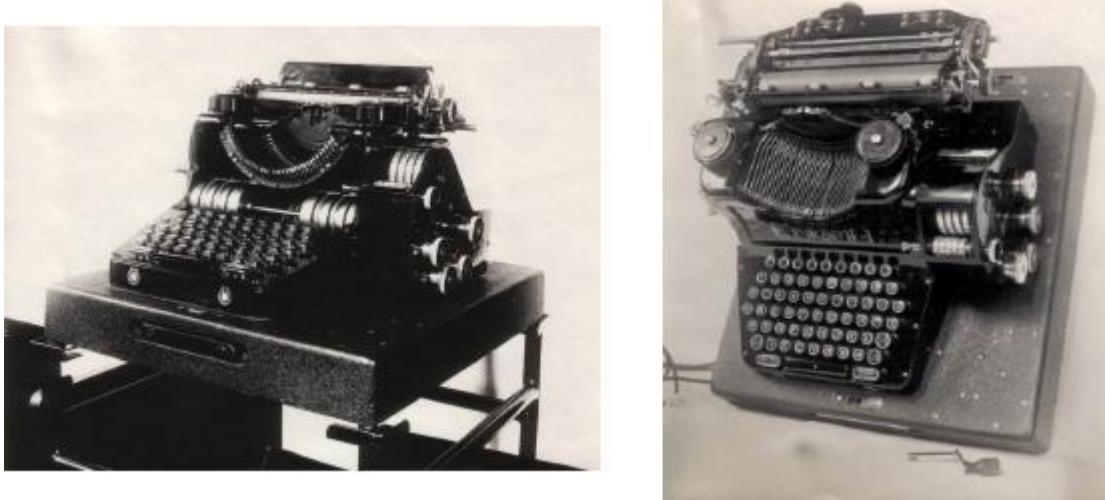


Figura 5.5: Modelo B da máquina Enigma (CRYPTO, 2012).

5.1.3 Enigma C

A Enigma C, de 1924, foi o primeiro modelo a usar lâmpadas para a saída de dados, o que era uma alternativa de baixo custo para os modelos baseados em máquinas de escrever. O modelo era muito menor que os anteriores, o que a tornava mais portátil, além de o preço ser cerca de 1/8 do preço da Enigma A.

Muitas versões da Enigma C foram construídas: o modelo padrão usava o alfabeto standard internacional e as letras no teclado e no painel de lâmpadas estavam organizadas em ordem alfabética. Havia um refletor fixo que podia ser montado em duas posições.



Figura 5.6: Modelo C da máquina Enigma (CRYPTO, 2012).

Uma variação da Enigma C, chamada *Funkschlüssel C* (ou cifra de rádio C), foi a primeira versão da Enigma a ser adotada pelas Forças Armadas. Ela foi posta em produção em 1925 e começou a ser usada pela Marinha alemã em 1926.

5.1.4 Enigma D

Também conhecida como Enigma comercial A26, foi desenvolvida em 1926 como sucessora da Enigma C, sendo substituída mais tarde pela família K de máquinas comerciais. Nela, a ordem das teclas e das lâmpadas era similar à ordem standard das letras de uma máquina de escrever alemã, e não mais em ordem alfabética.

Levando em consideração a árvore de máquinas Enigma (Figura 5.1), fica claro que era o produto mais importante do fabricante, uma vez que quase todas as máquinas Enigma construídas depois foram inicialmente baseadas nela.



Figura 5.7: Modelo D da máquina Enigma (CRYPTO, 2012).

Isso aconteceu após o primeiro ano da Enigma D, em 1927, quando muitas máquinas com melhorias passaram a ser desenvolvidas seguindo seu design. Entre as descendentes, seja por serem desenvolvidas diretamente a partir dela ou por terem design inspirado por ela, estão a *Reichswehr D* ou Enigma I (Ch. 11a), a Enigma K (A27, Ch. 11b), a *Zählwerk Enigma* ou Enigma G (A28, Ch. 15) e a Enigma Z (Z30, Ch. 16).

5.1.5 Enigma I ou Enigma *Reichswehr D*

O Exército alemão adotou a máquina Enigma em 1927, e ela entrou em uso em 1928 com uma importante alteração: um painel de plugues. A Enigma I ficou conhecida como Enigma de Serviço, com designador interno Ch. 11a. Todas as outras máquinas Enigma usadas pelo Exército alemão foram baseadas neste design.

A Enigma I foi a primeira máquina Enigma com lâmpadas usada exclusivamente pelo Exército alemão antes e durante a Segunda Guerra Mundial. Ela era baseada no chassi da Enigma D, mas tinha um refletor fixo e um único painel de plugues atrás da aba de madeira na frente da máquina.

Ela possuía inicialmente três rodas de códigos que podiam ser inseridas em 6 ordens diferentes. Em dezembro de 1938, surgiram duas novas rodas, o que fazia com que o número de ordens diferentes de configuração inicial passasse para 60. As duas rodas que não estavam sendo usadas no momento ficavam guardadas em uma pequena caixa

de madeira. O que aumentou de maneira mais dramática ainda o número de combinações possíveis foi o painel de plugues.



Figura 5.8: Modelo I da máquina Enigma (CRYPTO, 2012).

A Enigma I foi usada tanto pelo Exército quanto pela Força Aérea. Mais tarde, foi adotada também pela Marinha, quando ficou conhecida como M1, M2 e M3. A diferença mais óbvia entre as versões do Exército e da Marinha era que as rodas da segunda possuíam letras (A-Z) no lugar de números. Cerca de 20 mil máquinas desse tipo foram construídas.

5.1.6 Enigma II ou Enigma H

Desenvolvido em 1929, foi o último modelo que imprimia a saída diretamente no papel, e também tinha problemas de confiabilidade, como seu antecessor, o modelo B.

O número oficial dessa máquina Enigma era H29 (Ch. 14), e era usada principalmente pelas Forças Armadas alemãs (*Wehrmacht*), onde ficou conhecida como Enigma II. Algumas dessas máquinas foram vendidas para clientes estrangeiros, como a Hungria (modelo H-221), que as usou no Exército.

Existiam duas configurações possíveis na Enigma H: *Grosse Maschine* (máquina grande), usada quando a máquina funcionava como máquina de cifras, e *Kleine Maschine* (pequena máquina), que fazia com que o mecanismo de cifragem fosse solto, ignorando os rotores de codificação.

Na posição *Kleine Maschine*, a máquina podia ser usada como uma máquina de escrever elétrica ou, quando o modelo permitia, como dispositivo de impressão para uma máquina Enigma menor baseada em lâmpadas, como a Enigma I ou o modelo G31 da Enigma G (mesmo com a cifragem não sendo compatível).

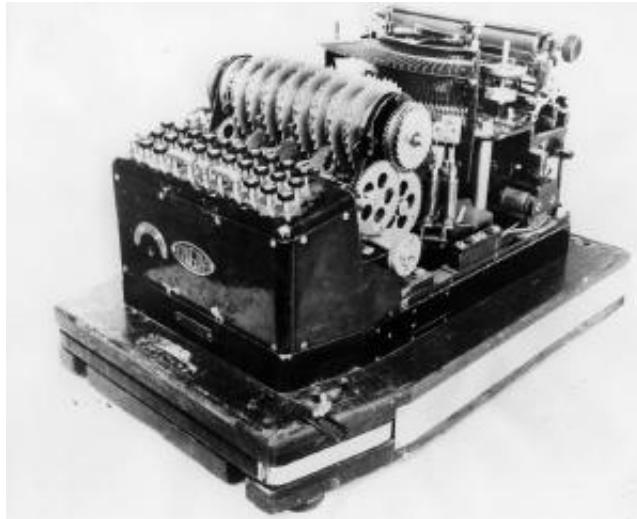


Figura 5.9: Modelo H da máquina Enigma (CRYPTO, 2012).

5.1.7 Enigma K

Por volta de 1927, o *Chiffriermaschinen AG*, fabricante das máquinas Enigma, iniciou o desenvolvimento de uma série de novas máquinas, todas derivadas da Enigma D comercial. Para o Exército (na época ainda *Reichswehr*), eles desenvolveram a Enigma I, e para vários outros clientes (civis e militares), foi introduzida a família K.



Figura 5.10: Detalhe do modelo K da máquina Enigma (CRYPTO, 2012).

A Enigma K pode ser considerada como uma série de máquinas especiais baseadas no design da Enigma D. O número oficial era A27 e o designador interno era Ch. 11b. Inicialmente, todas as máquinas tinham uma numeração de série começando com a letra A. Foi apenas em 1936 que a letra K passou a ser usada como número de série, provavelmente por causa da palavra alemã *Kommerziell* (comercial).

Muitas delas foram construídas para usuários como o *Reichsbahn* (a Ferroviária Imperial alemã), e também foram vendidas a estrangeiros, como o Exército suíço e a Marinha italiana (*Supermarina*), que usaram máquinas Enigma K ao longo da Segunda Guerra Mundial. Versões modificadas da Enigma K também foram utilizadas durante a Guerra Civil Espanhola (1936-1939).

Pertencem a esta família a Enigma K (1927), a variante suíça da Enigma K (1938), a Enigma T (Tirpitz) de 1942, a Enigma KD (1944) e a *Reichsbahn* Enigma.

Inicialmente, cada uma das rodas tinha um entalhe de rotação única (ou *stepping* regular), mas nas variantes posteriores, o número de entalhes foi aumentado. A Enigma T (1942), por exemplo, tinha cinco entalhes em cada roda, e as rodas da Enigma KD (1944), possuíam 9 entalhes, com *stepping* irregular.

5.1.8 Enigma *Zählwerk* ou Enigma G

Por volta da mesma época em 1927 em que era desenvolvida a série de máquinas derivadas da Enigma D comercial que deu origem à família K e à Enigma I, começou o desenvolvimento de uma máquina melhor e mais avançada, conhecida como *Glühlampen-Chiffriermaschine "Enigma" mit Zählwerk und der zwangsläufiger Kupplung Chiffrierwalzen*, ou traduzindo: máquina de cifragem Enigma de lâmpadas com contador e rodas de cifra acopladas.

Ela tinha um mecanismo de roda dentada com rotações irregulares, o que tornava a criptografia muito mais forte do que a da Enigma D. As rodas dentadas são vistas entre as rodas de codificação, e o contador pode ser visto à esquerda.



Figura 5.11: Modelo G da máquina Enigma (CRYPTO, 2012).

A máquina passou a ser chamada de Enigma G porque as que foram construídas mais tarde tinham números de série começando com a letra G. As máquinas Enigma *Zählwerk*, no entanto, tinham números de série começando com a letra “A”, e os criptoanalistas de Bletchley Park as chamavam de máquinas “11-15-17” por causa do número de entalhos em cada roda.

A máquina também era chamada de Enigma *Abwehr*, já que foi também usada pelo Serviço de Inteligência alemão durante Segunda Guerra Mundial, embora não tenha sido a única. Ela foi usada também por clientes civis e militares em vários países, como Hungria e Holanda.

Na prática, a máquina foi chamada principalmente de *Zählwerksmaschine* (Máquina com contador) ou de *Zählwerk* Enigma (Enigma com contador), e teve diferentes tipos construídos, sendo melhorada ainda algumas vezes. Além disso, uma variante menor (modelo G31) foi introduzida em 1931.

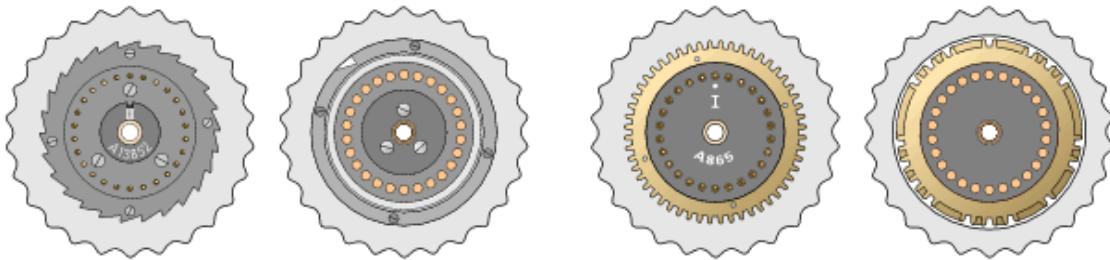


Figura 5.12: Rodas genéricas de Enigma e rodas da *Zählwerk* (CRYPTO, 2012).

A diferença mais marcante entre os outros modelos de Enigma e a Enigma *Zählwerk* era a maneira como as rodas se movimentavam: na Enigma D (e também na Enigma I utilizada pelo Exército alemão), as rodas eram movidas por meio de linguetas, catracas e chanfros. Como resultado, essas máquinas só podiam avançar.

Na Enigma *Zählwerk*, no entanto, as rodas eram movidas por um mecanismo como uma caixa de câmbio de engrenagens com rodas dentadas. Além disso, o número de entalhes de cada uma das rodas foi aumentado drasticamente, e era diferente para cada uma das rodas.

A Enigma *Zählwerk* usava o princípio de que o período mais longo de cifra é gerado quando números primos relativos são utilizados para o número de entalhes de cada roda. Outra diferença para a Enigma D era que o refletor (UKW) não só podia ser definido para cada uma das 26 posições, mas também era movido pelas outras rodas durante a codificação.

As três rodas codificadoras eram montadas sobre um eixo, tal como na maioria das máquinas Enigma, enquanto o refletor era montado de forma permanente. Cada roda de cifragem tinha uma roda dentada completa com 52 dentes anexada ao seu lado direito. No lado esquerdo havia outra roda dentada, com o mesmo espaçamento, mas com certo número de dentes faltando. A presença de um par de dentes era equivalente a um entalhe em uma roda comum. Quando as rodas estavam no lugar, entre elas ficavam 4 rodas dentadas com dentes de diferentes tamanhos.

Como resultado, era possível dar passos para frente e para trás, sem perder a relação entre a posição de uma das rodas. Uma manivela podia ser inserida num orifício no corpo da máquina para colocar o mecanismo na posição desejada. Isto era usado para corrigir erros, mas podia também atuar como parte da chave.

As rodas da máquina Enigma *Zählwerk* padrão tinham o mesmo diâmetro das rodas de outras máquinas Enigma, mas no modelo posterior G31, as rodas eram menores.

A Enigma *Zählwerk* teve as seguintes versões: *Zählwerk Enigma* (1927), *Zählwerk Enigma*, modelo A28 (1928) e *Zählwerk Enigma*, modelo G31 (1931).

5.1.9 Enigmas M1, M2 e M3

O Exército alemão começou o uso da máquina Enigma em 1928. Depois de várias experiências e melhorias com o painel de plugues, as máquinas Enigma I foram introduzidas para uso pelo Exército e pela Força Aérea em 1932. Em 1934 foi a vez de a Marinha seguir com a introdução da máquina Enigma M1 (Ch. 11g), que era compatível com o Enigma I (Ch. 11f). Mesmo assim, havia algumas diferenças de fabricação.

Por exemplo, os rotores das Enigma M1 tinham letras (A-Z) em suas circunferências, ao invés de números (01-26), e as máquinas tinham uma tomada de 4V que as tornava adequadas para utilização a bordo de um navio.

Cerca de 611 unidades da Enigma M1 foram construídas. A M1 foi seguida em 1938 pela M2, das quais 890 unidades foram feitas. Finalmente, em 1940, as máquinas foram substituídas pelas M3, das quais foram construídas aproximadamente 800 unidades. Todas as três máquinas, M1, M2 e M3 tiveram a mesma designação interna, Ch. 11g, e serão tratadas aqui em conjunto.

Inicialmente, o modelo M3 foi fornecido com cinco rodas de cifras que eram compatíveis com as rodas fornecidas com a Enigma I. Desta forma, todos os três departamentos das Forças Armadas alemãs poderiam trocar mensagens. Em 1939, mais três rodas foram adicionadas (VI, VII e VIII), sendo utilizadas exclusivamente pela Marinha.



Figura 5.13: Enigma M3 a bordo de um U-Boot U-124 alemão (CRYPTO, 2012).

No início da Segunda Guerra Mundial, a seção U-Boot da *Kriegsmarine* também usou a Enigma M3, até que ela foi substituída pela Enigma M4 em 1942.

5.1.10 Enigma M4

A Enigma M4 foi desenvolvida exclusivamente para a divisão U-Boot da *Kriegsmarine*. Era a sucessora da Enigma M3, que era baseada na Enigma I do Exército alemão. A Enigma M4 desempenhou papel fundamental na Batalha do Atlântico e foi introduzida de forma inesperada em fevereiro de 1942, causando grande assombro e transtorno para os criptoanalistas de Bletchley Park, que a chamaram de *Shark-key* (Chave-tubarão). Seu código permaneceu sem ser quebrado por nove meses, até outubro de 1942, quando livros de códigos novos foram capturados.



Figura 5.14: Modelo M4 da máquina Enigma (CRYPTO, 2012).

O projeto era baseado no da Enigma I, que já estava em uso pelo Exército e pela Força Aérea. Havia três rodas de código, um refletor fixo (UKW) e um painel de plugues (*Steckerbrett*). Eram fornecidas 8 rodas codificadoras diferentes, (I a VIII), das quais 3 ficavam na máquina. O cabeamento das rodas I a V era idêntico ao da Enigma I. Ao contrário do Exército, a Marinha optou por ter letras (A-Z) na circunferência da roda.

Pode-se dizer que a Enigma M4 dispunha de quatro rotoretes, colocados no espaço previsto para três: isso era conseguido à custa da substituição do refletor original por um refletor de espessura menor e adicionando o quarto rotor, fixo mas configurável, em qualquer uma das 26 posições.

Essa roda adicional (*Zusatzwalze*), à esquerda das outras três, fornecia uma fase adicional ao processo de codificação. A roda adicional não era movida durante a cifragem, e não podia ser trocada com as outras três rodas. Quando a roda adicional beta era colocada na posição A, a máquina ficava compatível com a Enigma I e a Enigma M3. Havia duas versões diferentes da roda extra: Beta e Gama.



Figura 5.15: Roda adicional (Zusatzwalze) da Enigma M4 (CRYPTO, 2012).

Nos submarinos, a máquina Enigma ficava geralmente localizada na sala de rádio, embora em alguns casos fosse levada para os aposentos do capitão para, por exemplo, uma dupla encriptação (*Sonderschlüssel M*). A maioria dos submarinos tinha ainda duas máquinas Enigma disponíveis, para lidar com as chaves diferentes do período anterior e posterior à meia-noite. Uma máquina ficava com as configurações do dia anterior, enquanto a outra era configurada com as configurações para o novo dia. Como algumas mensagens eram recebidas com atraso, poderiam ser rapidamente testadas com as duas chaves.

Uma fraqueza do mecanismo de movimento das rodas era o movimento regular. Apenas depois de a roda da direita completar uma rotação completa é que a roda seguinte dará um passo. Como resultado, a segunda roda a partir da direita só dará um passo a cada 26 caracteres e a terceira roda dificilmente se moverá. Isso faz com que o período da cifra seja previsível e mais fácil de quebrar. A única máquina Enigma que não sofria desses passos regulares era a Enigma G (ou *Zählwerkmaschine*).

As três rodas extras (VI, VII e VIII) tinham dois entalhes cada, o que as fazia girar com mais frequência e ter passos menos regulares. No entanto, o número 2 de entalhes em cada roda não era primo relativo de 26 (26 pode ser dividido por 2), e os entalhes eram posicionados de maneira oposta um do outro. O resultado era o período da cifra ser reduzido pela metade, o que era mais uma fraqueza do sistema.

5.1.11 Enigma T (Tirpitz)

A Enigma T, codinome Tirpitz, era uma máquina Enigma desenvolvida durante a Segunda Guerra Mundial, em 1942, pelos alemães especialmente para o uso pelo exército japonês.

Ela era baseada na Enigma K comercial, mas tinha a fiação dos rotores diferente e múltiplos movimentos em cada rotor. Além disso, tinha uma roda de entrada (*Eintrittswalze*) moldada de forma diferente de todas as de outras máquinas Enigma.



Figura 5.16: Modelo T da máquina Enigma (CRYPTO, 2012).

A Enigma T deveria servir para a comunicação entre a Marinha alemã e a japonesa: toda a comunicação entre os países seria criptografada com a máquina, que era chamada de Tirpitz pelos alemães e de “Tirupitsu” pelos japoneses. A Marinha dos Estados Unidos se referia à máquina como OPAL, e o tráfego foi nomeado JN-18. O nome oficial para o sistema de máquina era Uso Conjunto Alemão-Japonês Código Nº 3.

O sistema consistia de um procedimento operacional chamado Tirpitz, e uma lista de chaves com o nome *Gartenzaun* (cerca de jardim). Os procedimentos operacionais funcionaram de agosto de 1943 até o final da guerra.

Como a máquina seria utilizada para a comunicação entre as Marinhas da Alemanha e do Japão, os alemães usaram como base a Enigma K modificada de diversas maneiras. A roda de entrada (ETW) foi ligada de forma aleatória, diferente de todas as outras máquinas. A máquina era fornecida com 8 rodas de codificação (3 na máquina).

A diferença mais importante entre a Enigma K e a Enigma T, porém, era a presença na segunda de cinco entalhes de rotação em cada uma das 8 rodas. Isso causava movimentos de roda muito mais frequentes, e estendeu o período de cifra (já que 5 é um primo relativo de 26). Em alguns casos, o procedimento operacional instruía o operador a avançar o UKW manualmente em uma posição depois de cada grupo de cinco cartas, adicionando complexidade extra.

Os japoneses encomendaram ao todo 800 máquinas (400 no primeiro pedido), mas por várias razões esse número nunca foi entregue. Verificaram-se atrasos no design e na fabricação, além da dificuldade provocada pela Guerra; como havia escassez de material, apenas pequenos lotes de máquinas foram fornecidos aos japoneses. Outro motivo para a não entrega de todas as unidades encomendadas foi a desconfiança dos alemães com relação à segurança da máquina.

Enquanto isso, os japoneses usaram dois sistemas manuais: Sumatra (mais tarde Sumatra 2) e TOGO (mais tarde TOGO 2).

5.1.12 Enigma KD

A Enigma KD era uma Enigma K comercial padrão com fiação diferente nas rodas de cifragem e um refletor recabeável chamado UKW-D.

Ela foi usada pelo Gabinete Militar (*Militärisches Amt, Mil Amt*) na conexão Berlim-Madrid-Lisboa, tendo aparecido pela primeira vez em dezembro de 1944 e permanecendo em uso até o final da guerra.

A Enigma KD fornecida para o *Mil Amt* tinham seis rodas de cifras diferentes, cada uma com nove entalhes. Três destas rodas ficavam na máquina durante o uso. A fiação usada pelo *Mil Amt* é desconhecida até hoje.

A origem do nome da máquina (KD) é desconhecida, mas existem duas explicações possíveis: o nome pode estar relacionado ao *Kommando des Meldegebietes* (KDM), que ficou no lugar dos *Abwehrstellen* (Ast) depois que estes foram incorporados ao *Reichssicherheitshauptamt* (RSHA) em junho de 1944, ou pode estar relacionado com a fusão do nome do modelo da máquina K com o nome do refletor recabeável D.

O Gabinete Militar alterava a ordem dos rotores (*Walzenlage*) e dos anéis (*Ringstellung*) diariamente, enquanto a posição inicial dos rotores (*Grundstellung*), e provavelmente também a fiação do UKW-D, era mudada a cada três semanas.



Figura 5.17: Modelo KD da máquina Enigma (CRYPTO, 2012).

5.1.13 Enigma Z

A Enigma Z possuía apenas 10 teclas e 10 lâmpadas, servindo para encriptar e desencriptar mensagens com números apenas (de 0 a 9). Pouco se sabe sobre este modelo, embora seja provável que tivesse duas versões: uma baseada na Enigma D e uma baseada na Enigma G.

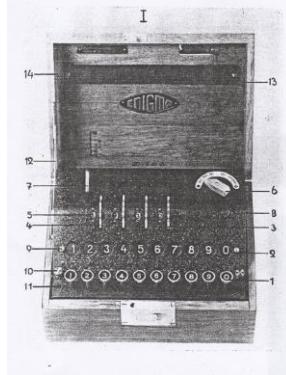


Figura 5.18: Modelo Z da máquina Enigma (CRYPTO, 2012).

5.2 Produção e distribuição das máquinas Enigma

Os dados mais completos sobre a produção e a distribuição das máquinas Enigma são do Crypto Musem (2012).

As máquinas eram inicialmente manufaturadas pela *Chiffriermaschinen AG* em Berlim. Depois que as patentes da Enigma foram adquiridas pelos alemães, o nome da companhia foi mudado para *Heimsoeth und Rinke*, e outras companhias foram designadas para fabricá-las sob licença. Abaixo está a lista completa dos fabricantes e de seus códigos, com exceção do fabricante original.

Código	Edição	Nome	Endereço
-	-	Chiffriermaschinen AG	Steglitzerstraße 2 Berlin W 35
aye	Oct 1940	Olympia Büromaschinenwerke AG	Mainzerhofplatz Erfurt
bac	Feb 1941	Ertel-Werk für Feinmechanik	Westendstr. 160 München
gvx	Jul 1941	Konski & Krüger Fabrik elektr. u. mechanischer Apparate	Chausseestr. 117 Berlin N 4
jla	Sep 1941	Chiffriermaschinengesellschaft Heimsoeth und Rinke	Uhlandstr. 136 Berlin-Wilmersdorf
j mz	Sep 1941	Atlas-Werke AG Maschinenfabrik	Steinhöft 11 Bremen

Figura 5.19: Produção e distribuição de máquinas Enigma (CRYPTO, 2012).

5.3 Outras máquinas usadas na Segunda Guerra Mundial

Além da máquina Enigma, que acabou se tornando a mais conhecida, outras máquinas foram usadas na Segunda Guerra Mundial. As principais foram a SIGABA (ou ECM Mark II ou ainda CSP-888/889), da Marinha norte americana e a Púrpura (ou 97-shiki-O-bun In-ji-ki), usada pelo serviço diplomático japonês.

6 SIMULANDO UMA MÁQUINA ENIGMA

Uma vez que existem poucos exemplares de máquinas Enigma em funcionamento e acessíveis para manuseio público, e que os próprios documentos oficiais descrevendo os pormenores das máquinas Enigma são escassos, torna-se interessante o uso de um simulador computacional para demonstrar seu funcionamento.

6.1 O que é necessário para criar um simulador

O mecanismo de funcionamento geral de uma máquina Enigma foi explicado anteriormente, e sua implementação em um computador atual não possui maior dificuldade.

Para simular uma máquina Enigma, são necessárias informações que podem variar de modelo para modelo, como a fiação interna dos rotores, o número de rotores disponíveis, a presença ou não dos rotores fixos finos, o tipo do refletor (qual letra, fixo, de duas posições ou de 26 posições), a presença ou não do painel de plugues usado pelas Forças Armadas, o tipo de teclado para entrada de dados (alfabético ou numérico) e o tipo de saída de dados (simulando o acendimento de lâmpadas ou direto na tela). A interface poderia ser simples ou emulando uma máquina Enigma real.

Supondo-se que se quisesse implementar um simulador da Enigma I, um dos modelos mais conhecidos e reportados, por exemplo, em uma linguagem qualquer e usando o que foi visto até agora sobre o funcionamento da máquina, teriam de ser levados ainda em consideração os dados a seguir.

A fiação teria de ser conforme a mostrada em Rijmenants (2012):

Entrada = ABCDEFGHIJKLMNOPQRSTUVWXYZ (ETW, rotor de entrada)

I = EKMFLGDQVZNTOWYHXUSPAIBRCJ

II = AJDKSIRUXBLHWHTMCQGZNPYFVOE

III = BDFHJLCPRTXVZNYEIWGAKMUSQO

IV = ESOVPZJAYQUIRHXLNFTGKDCMWB

V = VZBRGITYUPSDNHGXAWMJQOFEC

Os contatos do refletor teriam de ser conforme segue:

Contacts = ABCDEFGHIJKLMNOPQRSTUVWXYZ

Reflector B = YRUHQSLDPXNGOKMIEBFZCWVJAT

Reflector C = FVPJIAOYEDRZXWGCTKUQSBNMHL

Ainda seguindo os dados em Rijmenants (2012), os chanfros de cada rotor, que regulam as rotações dos rotores adjacentes, seguiriam a descrição a seguir: Rotor I, chanfro em Y, aparece na janela Q, próximo rotor esquerdo gira quando rotor passa de Q para R. Rotor II, chanfro em M, aparece na janela E, próximo rotor esquerdo gira quando rotor passa de E para F. Rotor III, chanfro em D, aparece na janela V, próximo rotor esquerdo gira quando rotor passa de V para W. Rotor IV, chanfro em R, aparece na janela J, próximo rotor esquerdo gira quando rotor passa de J para K. Rotor V, chanfro em H, aparece na janela Z, próximo rotor esquerdo gira quando rotor passa de Z para A.

O painel de plugues faria com que letras fossem trocadas por outras escolhidas pelo usuário antes de começar a cifragem ou decifragem.

O passo duplo (quando o rotor do meio avança no próximo passo do primeiro rotor uma segunda vez se o rotor do meio estiver em posição de girar), comum desse modelo, também deveria ser levado em consideração na hora da implementação.

Importante também seria o simulador ter uma interface que conseguisse mostrar de forma clara todos os elementos da máquina e facilitasse a escolha das configurações iniciais.

6.2 Escolhendo um simulador

Como implementar um simulador não fazia parte do escopo deste estudo, foram testados diversos simuladores de máquinas Enigma ao longo do segundo semestre de 2012, como forma de mostrar a máquina em operação.

A maioria simula a máquina Enigma I, usada pelo Exército, mas sem maiores opções de configuração ou de escolha de outras máquinas. Uma breve descrição dos melhores e do pior simuladores encontrados entre os pesquisados é dada a seguir.

O simulador online em Flash v4.3 disponível no site Enigma Simulator (SPIESSE, 2012) emula a máquina Enigma I, e é detalhado e completo, com visual atraente. Nele é possível acompanhar a direção da corrente e o caminho percorrido por ela nos rotores e no refletor. Um painel de plugues também está disponível, e nele podem-se conectar de zero a treze cabos. O simulador permite ainda trocar e escolher a ordem dos rotores e mandar configurações e cifragens por e-mail.

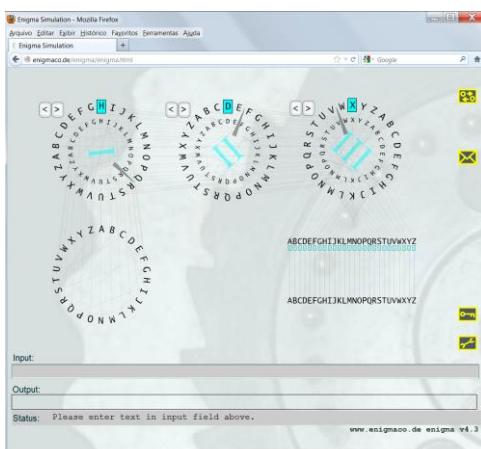


Figura 6.1: Enigma Simulator v4.3 (SPIESSE, 2012).

O simulador online em Java disponível no site Paper Enigma Machine (ROSS, 2012) simula uma Enigma I, e traz a possibilidade de serem configurados os rotores, os anéis, a posição inicial dos rotores e o painel de plugues, tudo isso com visual simples e entrada de dados em formato de texto, o que às vezes pode ser confuso. O site traz ainda um simulador Enigma para Android e um simulador que pode ser impresso em papel.

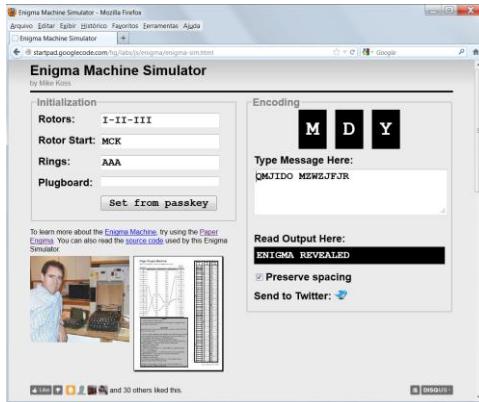


Figura 6.2: Enigma Machine Simulator (ROSS, 2012).

O site The Enigma Machine (SCHWAGER, 2005) foi o pior simulador encontrado na pesquisa. Ele simula online uma máquina Enigma genérica usando um *applet* Java. Um arquivo de ajuda sucinto poderia ajudar na operação deste simulador, que tem visual simples e confuso. Outros problemas encontrados foram a existência de 9 rotores disponíveis e a estranha possibilidade de escolha dos mesmos rotores para as três posições. O painel de plugues não funciona e a posição inicial não fica claramente mostrada, sendo que possivelmente esteja sendo confundida com a configuração dos anéis. É possível baixar o código fonte do programa no próprio site.

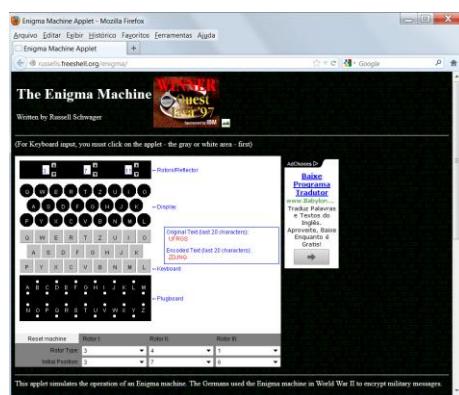


Figura 6.3: The Enigma Machine (SCHWAGER, 2012).

6.3 Simulação com Enigma Cipher Machine Simulator 7.0.5

A simulação de uma máquina Enigma mostrada a seguir usa o melhor simulador entre os pesquisados, e que pode ser considerado estado da arte: Enigma Cipher Machine Simulator 7.0.5, desenvolvido Rijmenants (2012). O simulador está disponível para download gratuito e é, entre os pesquisados, o mais completo, simulando máquinas

Enigma Wehrmacht (também conhecidas como Enigma I) com refletores B e C, Enigma M3 com refletores B e C e Enigma M4 com refletores B e C.

A interface emula as de máquinas Enigma com perfeição, com a máquina podendo ser “aberta” e “fechada” para a escolha das configurações. Um detalhe interessante é que, uma vez aberta, a máquina só pode ser fechada se todas as configurações tenham sido corretamente escolhidas. É possível ainda ouvir o barulho referente ao movimento dos rotores. Entre as opções do programa estão um bloco de notas para armazenagem dos textos cifrados e uma pequena galeria de fotos.

A seguir, pode ser visto no simulador uma máquina Enigma I, usada pelo Exército e pela Força Aérea alemães, em sua configuração original, primeiro aberta e depois fechada.



Figura 6.4: Máquina Enigma I (RIJMENANTS, 2012).



Figura 6.5: Painel de plugues, 10 pares de letras selecionados.



Figura 6.6: Enigma I com painel de plugues sendo usado.



Figura 6.7: Máquina Enigma I aberta.

A primeira simulação usa uma máquina Enigma I cifrando a palavra UFRGS. As configurações iniciais - ou chave criptográfica - escolhidas foram:

- Ordem dos rotores (*Walzenlage*): rotores I, III e V, colocados na seguinte ordem: V, III, I.
- Configuração dos anéis (*Ringstellung*): rotor V: I (indicado por I-09), rotor III: P (indicado por P-16) e rotor I: H (indicado por H-08).

- Posição inicial dos rotores (*Grundstellung*): rotor V: M (indicada pelo número 13), rotor III: B (indicada pelo número 02) e rotor I: G (indicada pelo número 07).
- Conexões dos plugues (*Steckerverbindungen*): foram suprimidas neste exemplo, por aparecem em tela separada.



Figura 6.8: Escolha dos rotores e ordem dos rotores: V, III, I.

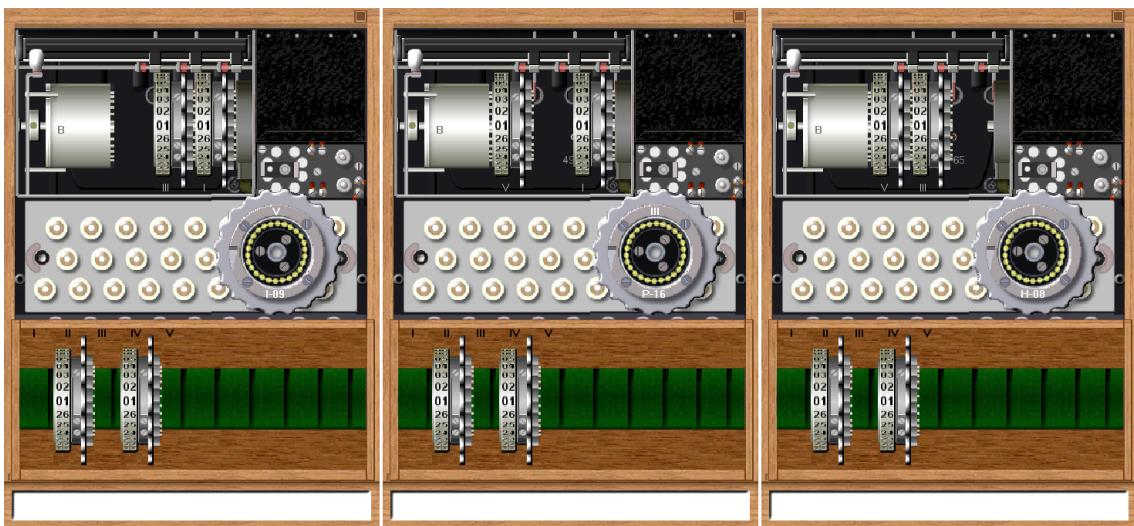


Figura 6.9: Configuração dos anéis.



Figura 6.10: Posição inicial dos rotores e início da cifragem com a letra U.

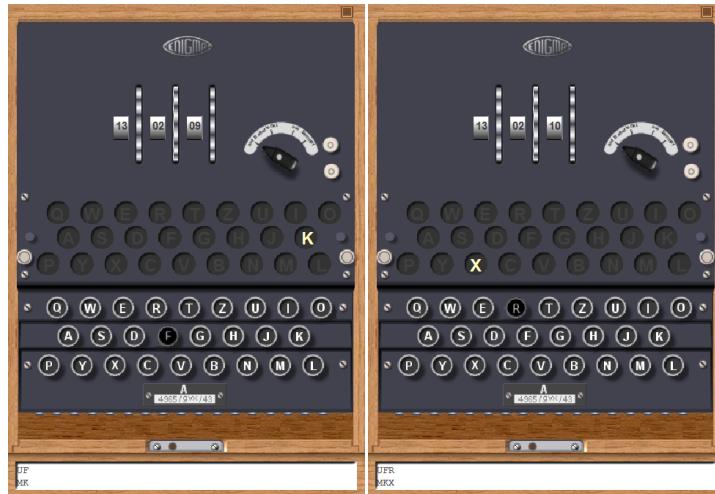


Figura 6.11: Cifrando F, R.



Figura 6.12: Cifrando G, S.

Após a cifragem, foi gerado MKXOU. É interessante notar que as máquinas Enigma não cifravam letras nelas mesmas, devido ao uso do refletor.

A segunda simulação usa uma máquina Enigma M4, da Marinha alemã. Considerada uma das máquinas mais difíceis de ter seus códigos decifrados, esta máquina podia ser usada para cifrar e decifrar mensagens das máquinas Enigma I e M3. Para isso, era necessária uma configuração especial, mostrada na simulação abaixo.

A entrada usada é MKXOU, resultado da simulação anterior. A palavra que se espera encontrar usando a Enigma M4 para decifrá-la é UFRGS. As configurações iniciais, ou chave criptográfica, escolhidas foram as mesmas usadas no exemplo acima, condição para que a compatibilidade ocorra:

- Ordem dos rotores: V, III, I.
- Configuração dos anéis: rotor V: I, rotor III: P e rotor I: H.
- Posição inicial dos rotores: rotor V: M, rotor III: B e rotor I: G.
- Conexões dos plugues: foram suprimidas.

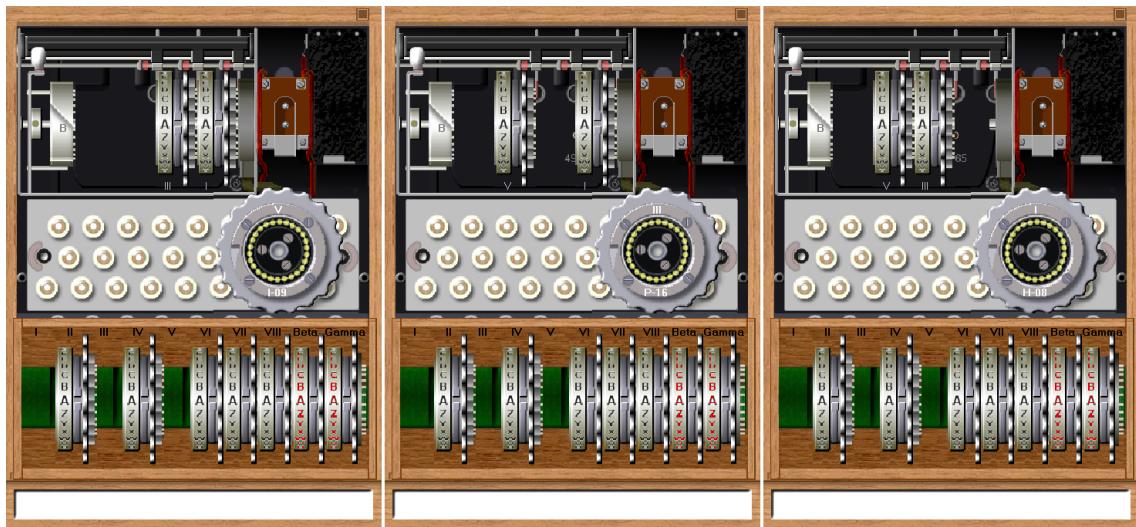


Figura 6.13: Configuração dos anéis.

Note-se que é necessária ainda uma configuração extra para tornar a compatibilidade entre a máquina Enigma I e a máquina Enigma M4 completa: a escolha do anel beta (não podendo ser usado o gama), colocado na configuração A-01.

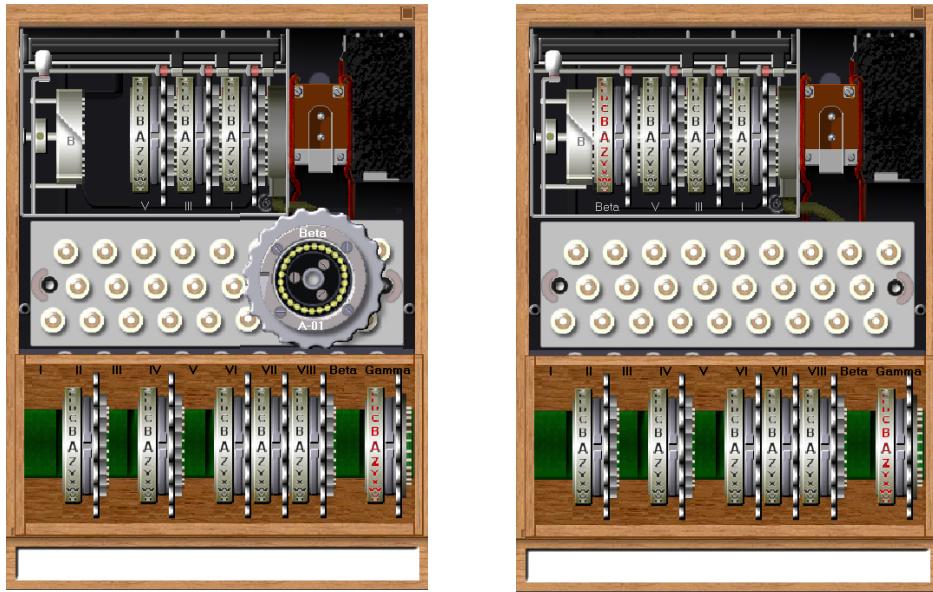


Figura 6.14: Anel beta na configuração A-01 e configuração interna completa.



Figura 6.15: Configuração externa completa e início da decifragem com a letra M.



Figura 6.16: Decifrado K, X.



Figura 6.17: Decifrado O, U.

O resultado esperado foi encontrado: a decifragem de MKXOU gerou a palavra UFRGS. Vale lembrar ainda que, por gerar um código simétrico, para uma máquina Enigma (excetuando-se os primeiros modelos) não havia diferença entre a cifragem e decifragem de um texto.

6.4 Um protótipo de máquina Enigma

Durante a pesquisa para este trabalho surgiu a ideia de implementar uma máquina Enigma. Uma implementação em software foi descartada porque uma breve pesquisa na internet mostrou que já existem diversas implementações como as mostradas aqui de boa qualidade disponíveis para download e para uso online, algumas inclusive destinadas a aparelhos móveis, como celulares e *tablets*.

O interesse de ainda assim construir uma máquina Enigma continuou, e assim surgiu a ideia de fazer um protótipo físico. Ele foi feito usando-se materiais de fácil acesso e materiais disponíveis em casas de produtos eletroeletrônicos.

O resultado foi um protótipo que funciona emulando o exemplo simplificado ilustrado no Livro dos Códigos (SINGH, 2011, p. 150) e reproduzido abaixo. Este exemplo com seis letras, ou variações dele, é normalmente utilizado quando se deseja mostrar o princípio de funcionamento da máquina Enigma de forma didática e simplificada.

Dado mais tempo e uma maior prática em trabalhos eletroeletrônicos, ele pode evoluir até um protótipo ainda mais completo, também funcional.

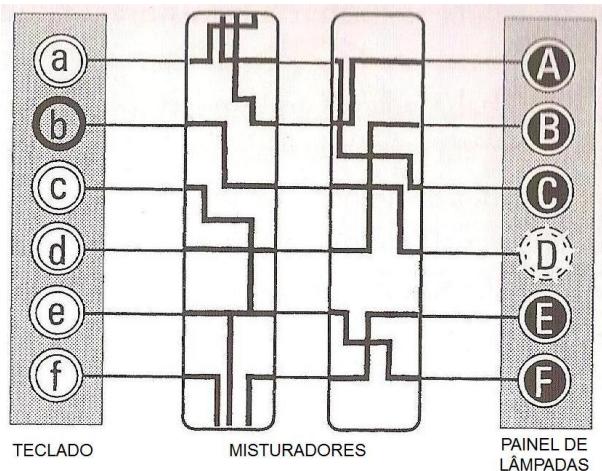


Figura 6.18: Diagrama de funcionamento da máquina Enigma (SINGH, 2011).

Material usado no protótipo: 12 teclas de dois teclados diferentes, diversos rolos de papel toalha, tesoura, alicate, 26 pedaços de cabo flexível de cobre de 20cm e um de 50cm, fita isolante, fita crepe, caneta permanente, corretivo, *stripboard*, porta-pilhas, 2 pilhas AA, resistor 100 ohms limitador de corrente para os LEDs, 6 LEDs brancos, 6 *tactile switches*, pistola de colagem, silicone e solda manual.

Nesta máquina Enigma simulada, existem apenas dois rotores (ou misturadores), representados pelos dois rolinhos do meio, e não há refletor. O rolinho de papel mais à direita serve como rotor de entrada (ETW) e, junto com o rolinho mais à esquerda, serve também para dar estabilidade aos cabos e facilitar a conexão.

Para emular a máquina Enigma simplificada do exemplo, a ordem dos rotores (*Walzenlage*) ficou I e II, a configuração dos anéis (*Ringstellung*) ficou sugerida pela fita crepe, com a posição da letra A sendo colocada nos anéis dos dois rotores. A posição inicial dos rotores (*Grundstellung*) ficou sendo as letras que são vistas na mesma linha do teclado e do painel de lâmpadas, ou seja, A e A. As conexões dos plugues (*Steckerverbindungen*) foram abstraídas.

Para simular o movimento dos misturadores a cada letra pressionada, é necessário desconectar os contatos do rotor ou dos rotores (dependendo do caso) em ambos os lados e refazê-los manualmente na posição seguinte.

A cada seis passos do primeiro misturador, o segundo misturador dá um passo. A cada seis passos do segundo misturador, a máquina volta para a posição original.

Os dois misturadores juntos fazem com que o padrão de cifragem não seja repetido até que o segundo misturador esteja de volta a seu ponto inicial, o que exige seis rotações completas do primeiro misturador, que equivale à cifragem de $6 \times 6 = 36$ letras. Ou seja, existem 36 ajustes diferentes de misturador, o que equivale a 36 alfabetos cifrados diferentes.



Figura 6.19: Visão geral do protótipo.

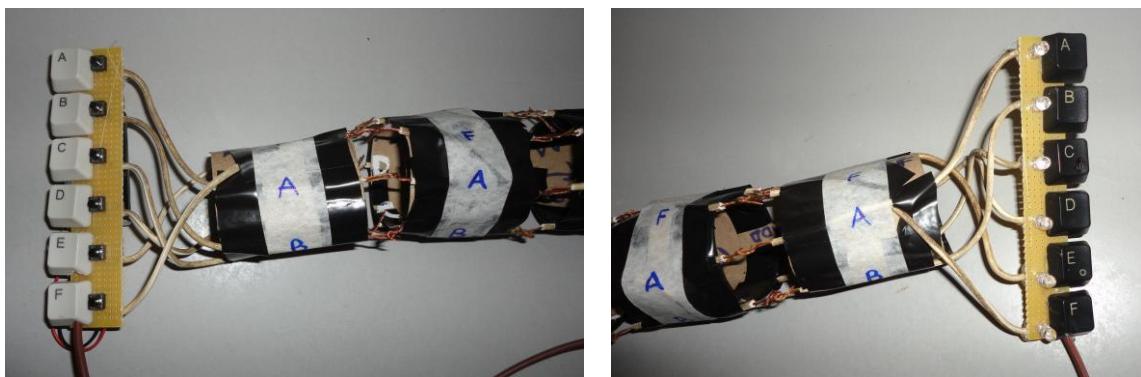


Figura 6.20: Teclado de entrada e teclado de saída com LEDs do protótipo.

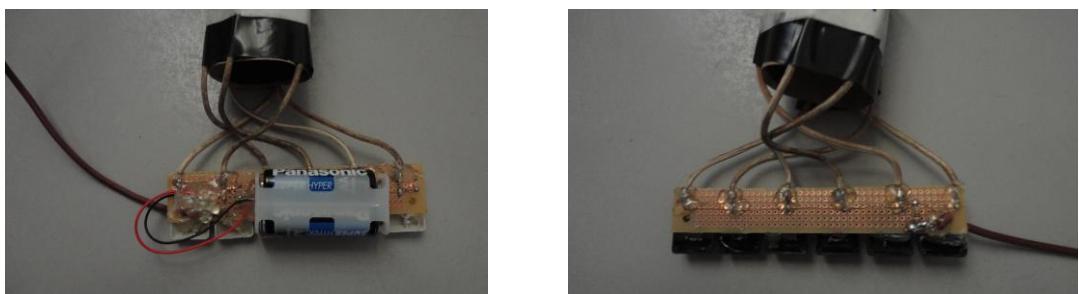


Figura 6.21: Verso do teclado de entrada e verso do teclado de saída com LEDs.



Figura 6.22: Detalhes da fiação do protótipo.

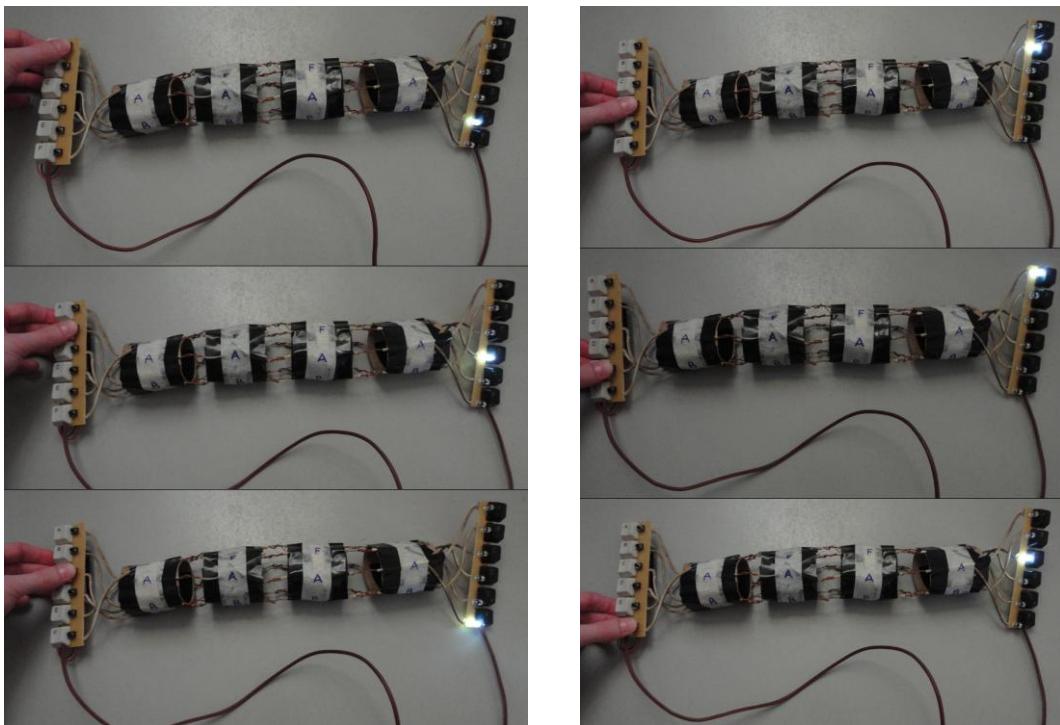


Figura 6.23: Cifragem (decifragem) das letras.

7 A FORÇA DA CIFRA ENIGMA

A força da segurança das cifras que foram produzidos pela máquina Enigma era um produto do grande número associado com o processo de cifragem (WIKIPEDIA, 2012).

Ao longo dos anos, novos procedimentos operacionais seguidos pelos alemães aumentaram a dificuldade de calcular as configurações possíveis da máquina Enigma. A cifra Enigma ganhava assim uma maior dificuldade de ser quebrada (CRYPTO, 2012).

Esse número total de configurações possíveis pode ser calculado de diversas formas. Um cálculo que leva em conta todas as variações possíveis de fiação em cada um dos rotores e o refletor aparece em Miller (2001), e resulta em 3×10^{114} . No entanto, esse número astronômico representa todas as variações enganosas teoricamente possíveis da máquina (RIJMENANTS, 2012).

Seguindo o Princípio de Kerkhoff, um sistema criptográfico (militar) deve ser seguro mesmo se tudo sobre o sistema, com exceção da chave, for de conhecimento público. Supondo que um possível atacante sabe a fiação das rodas, a roda de entrada (ETW) e o refletor (UKW), é possível fazer uma estimativa mais realista do número de configurações possíveis da Enigma (CRYPTO, 2012).

São consideradas então a seguir apenas as configurações possíveis do painel de plugues e dos rotores, e os cálculos usam como base uma Enigma I (Enigma de Serviço) e uma Enigma M4 naval.

7.1 Configurações possíveis do painel de plugues e dos rotores

Com 26 letras e 26 soquetes no painel de plugues, qualquer número de canos entre 0 e 13 podiam ser colocados para trocar pares de letras. O número máximo de combinações alcançáveis seria o uso de qualquer variação de 0 a 13 entre um dia e outro. No entanto, na prática, eram usados normalmente 10 cabos (CRYPTO, 2012).

Usando n para o número de cabos, o número total de combinações para cada número de cabos é calculado como mostrado a seguir.

$$n = \frac{26!}{n! \cdot (26 - 2n)! \cdot 2^n}$$

Figura 7.1: Cálculo das combinações usando cabos (CRYPTO, 2012).

Os números de combinações possíveis de cabos no painel de plugues (*Steckerbrett*) podem ser vistos na tabela abaixo. O valor total equivaleria à possibilidade de uso de qualquer variação entre 0 a 13 pares de cabos todos os dias.

Tabela 7.1: Combinações possíveis de cabos no painel de plugues

Cabos (n)	Combinações possíveis
0	1
1	325
2	44.850
3	3.453.450
4	164.038.875
5	5.019.589.575
6	100.391.791.500
7	1.305.093.290.000
8	10.767.019.640.000
9	53.835.098.190.000
10	150.738.274.900.000
11	205.552.193.100.000
12	102.776.096.500.000
13	7.905.853.580.550
Total	532.985.208.200.000

Fonte: CRYPTO, 2012.

As combinações possíveis dos rotores de uma Enigma I são mostradas a seguir.

Tabela 7.2: Combinações possíveis dos rotores da Enigma I

	Cálculo	Total
Ordem dos rotores (<i>Walzenlage</i>)	$5 \times 4 \times 3$	60
Ajuste dos anéis (<i>Ringstellung</i>)	26×26	676
Posição inicial dos rotores (<i>Grundstellung</i>)	$26 \times 26 \times 26$	17.576
Total		712.882.560

Fonte: CRYPTO, 2012.

A seguir, consideramos o cálculo do painel de plugues, assumindo que estavam sendo usados exatamente 10 cabos. Comparando-se com encriptações modernas, o uso da Enigma I seria equivalente a 76 bits, o que era bastante para a época.

$$\begin{array}{r}
 712,882,560 \\
 150,738,274,900,000 \times \\
 107,458,491,300,000,000,000 = 1.07 \times 10^{23} = 2^{76} = 76 \text{ bits}
 \end{array}$$

Figura 7.2: Chaves de mensagem cifradas Enigma I (CRYPTO, 2012).

Considera-se agora uma Enigma M4. Ela possuía 3 rotores normais em uso entre os 8 disponíveis e 1 rotor mais fino fixo, mas configurável, em uso entre dois disponíveis, num total de 4 rotores. O rotores mais finos não eram intercambiáveis com os rotores normais, e aqui não está sendo levado em consideração as duas possibilidades de escolha entre o rotor beta e o gama.

Tabela 7.3: Combinações possíveis dos rotores da Enigma M4

	Cálculo	Total
Ordem dos rotores (<i>Walzenlage</i>)	$8 \times 7 \times 6$	336
Ajuste dos anéis (<i>Ringstellung</i>)	26×26	676
Posição inicial dos rotores (<i>Grundstellung</i>)	$26 \times 26 \times 26 \times 26$	456.976
Total		103.795.700.700

Fonte: CRYPTO, 2012.

Considerando-se as seguir mais uma vez o uso de exatamente 10 cabos no painel de plugues, a comparação com encriptações modernas seria equivalente a 84 bits.

$$\begin{array}{r} 103,795,700,700 \\ 150,738,274,900,000 \times \\ \hline 15,645,956,330,000,000,000,000 = 1.56 \times 10^{25} = 2^{84} = 84 \text{ bits} \end{array}$$

Figura 7.3: Chaves de mensagem cifradas Enigma M4 (CRYPTO, 2012).

Isso mostra que a Enigma M4 era significativamente mais forte do que a Enigma I das Forças Armadas. Na prática, no entanto, o número total de combinações era menor do que o calculado, graças às várias restrições impostas à seleção dos rotores, como, por exemplo, a Marinha sempre utilizar, pelo menos, uma das rodas extras (VI, VII e VIII) e nunca usar uma roda na mesma posição em dias sucessivos.

A quebra da cifra Enigma era um enorme desafio, com um número de configurações de chave extraordinário para a era eletromecânica. Uma busca exaustiva era impossível, e a chave de 76 bits ainda hoje pode ser considerada grande (RIJMENANTS, 2012).

Ou seja, a força da cifra de 76 bits (ou 84 bits) era algo assombroso para as décadas de 1920 a 1940, quando não existiam ainda computadores como os conhecemos hoje. Mas exatamente graças à força da cifra Enigma, muitos dispositivos que serviriam como base para a computação moderna acabaram sendo criados pelas equipes de criptoanalistas, num esforço para quebrar códigos complexos que usavam um volume de informações que não seriam mais humanamente possíveis de serem trabalhados.

Entre esses dispositivos de propósito único e com funcionamento ainda simples, mas já demonstrando certo poder computacional, estavam o ciclômetro, as bombas criptológicas do *Biuro Szyfrów* e as bombas de Bletchley Park, que serão vistos a seguir.

8 A QUEBRA DO CÓDIGO

“A Enigma é uma máquina de cifragem muito complicada e decifrá-la exigiu um imenso poder intelectual” (SINGH, 2011, p. 176).

Quando a Primeira Guerra Mundial acabou, os criptoanalistas britânicos da Sala 40 continuaram monitorando as comunicações alemãs. Mas em 1926, com a entrada em funcionamento da máquina Enigma, começaram a surgir mensagens impossíveis de serem decifradas, tanto por eles quanto pelos norte-americanos e pelos franceses.

Logo eles perderam a esperança de decifrar as mensagens vindas do que podia ser chamado de “o sistema de comunicação mais seguro do mundo” (TKOTZ, 2005, p.250). O único país que insistiu nas tentativas de decifragem foi a Polônia, que tinha acabado de recuperar sua soberania após a Primeira Guerra Mundial e era ameaçada a leste pela Rússia, tentando expandir o comunismo, e a oeste pela Alemanha, determinada a reaver territórios perdidos para a Polônia na guerra.

8.1 Biuro Szyfrów

Como explica Singh (2011, p. 164), “Se a necessidade é a mãe das invenções, então a adversidade é a mãe da criptoanálise”. Foi criada então na Polônia uma agência de cífras em 1919, que chegou a decifrar 400 mensagens inimigas em agosto de 1920, durante a Guerra Polaco-Soviética (1919-1921). Os poloneses também monitoravam as comunicações alemãs, sendo também surpreendidos pelas mensagens encriptadas pelas máquinas Enigma em 1926. Em 1931, com a junção da agência de cífras polonesa a outra agência, foi formado o *Biuro Szyfrów*. Segundo Tkotz:

Nesta época, o responsável pela quebra das mensagens alemãs era o capitão Maksymilian Ciezki, que possuía um modelo comercial da Enigma. Essa máquina revelou os princípios da invenção de Scherbius, mas não a fiação correta dos rotores, pois a versão comercial era totalmente diferente da militar (2005, p. 251).

Do anedotário da época vem a história de que o capitão Ciezki teria chegado a recorrer aos préstimos de uma vidente, na tentativa de quebrar a cifra, mas sem sucesso. A ajuda viria, no entanto, de uma fonte mais próxima ao inimigo.

Hans-Thilo Schmidt, berlimense nascido em 1888, era filho de um professor e de uma aristocrata. Lutou na Primeira Guerra Mundial, mas foi desligado do Exército devido aos cortes de gastos impostos pelo Tratado de Versalhes. Quando sua tentativa nos negócios não deu certo, ele “acabou obrigado a fechar sua fábrica de sabão devido a hiperinflação e à depressão do pós-guerra. Sua família mergulhou na pobreza” (SINGH, 2005, p. 164). Hans-Thilo acabou obrigado a pedir ajuda a seu irmão, Rudolph.

Rudolph Schmidt também lutara na guerra e havia permanecido no Exército, chegando a ser promovido a chefe do Estado-Maior do Corpo de Sinaleiros. Ele era o responsável pelas comunicações seguras e, numa ironia histórica, quem aprovou oficialmente o uso da máquina Enigma pelo Exército. Rudolph arranjou um emprego para Hans-Thilo no *Chiffrierstelle* (ou Agência de Criptografia), escritório encarregado de administrar as comunicações cifradas da Alemanha. Hans-Thilo estava no “lar da Enigma”. Como explica Tkotz:

Morando sozinho, economizando cada centavo, invejando o sucesso do irmão e decepcionado com seu país, o resultado não poderia ser diferente. Sua vingança foi vender informações secretas da Enigma para potências estrangeiras (2005, p. 252).

Segundo Kahn (1991, p. 57-59), Hans-Thilo encontrou-se com um agente francês pela primeira vez em novembro de 1931, na Bélgica. Ele recebeu o codinome “Asche” e, por uma soma alta de dinheiro, deixou que o agente fotografasse dois documentos: *Gebrauchsanweisung für die Chiffriermaschine Enigma* (Manual de operação da máquina de cifragem Enigma) e *Schlüsselanleitung für die Chiffriermaschine Enigma* (Instruções de uso das chaves da máquina Enigma).

As informações contidas nos documentos permitiam deduzir o conjunto de conexões, embora não indicassem precisamente a fiação de cada um dos rotores (SINGH, 2011, p.166). Os documentos também explicavam em detalhes o esquema dos livros de códigos usados: a cada mês, os operadores da Enigma recebiam um novo livro-código com a chave para cada dia.

Uma réplica da máquina Enigma chegou a ser construída pelos aliados, mas sem bons resultados, uma vez que a força residia na chave utilizada. Convencidos de que a cifra era indecifrável, os franceses enviaram as fotografias obtidas dos documentos para a Polônia, graças a um acordo de cooperação entre os dois países.

Os criptoanalistas do *Biuro Szyfrów*, ao contrário dos criptólogos dos outros serviços de inteligência, seguiram adiante na tentativa de decifrar a máquina Enigma, uma vez que agora conheciam seu modo de funcionamento, a fiação dos três rotores e como as chaves eram gerenciadas. Os poloneses construíram sua primeira réplica da máquina Enigma em 1932.

Era sabido pelo *Biuro Szyfrów* que os operadores da Enigma recebiam todo mês um novo livro de códigos contendo as chaves diárias. O livro indicava a configuração do quadro de ligação, a sequência de rotores e a posição inicial deles. Todos os dias os operadores configuravam suas máquinas de maneira idêntica. As letras do texto claro eram digitadas na máquina e o resultado era anotado; a mensagem era enviada por telégrafo ou por rádio, e do outro lado o mesmo processo era repetido para decifrar a mensagem.

Embora seja um processo seguro, o uso da mesma chave diária para cifrar centenas de mensagens enfraquece sua segurança. Para aumentá-la, uma vez que havia um grande volume de dados sendo transmitido, os operadores passaram a escolher uma nova chave de três letras que indicasse a posição inicial dos rotores para cada mensagem que fossem transmitir.

Como precaução extra, os alemães usavam os ajustes da chave diária para transmitir uma nova chave de mensagem para cada mensagem. Explica Singh:

As chaves de mensagem teriam as mesmas disposições do quadro de tomadas e o mesmo arranjo de misturadores da chave do dia, mas diferentes orientações para os misturadores. E como as novas orientações dos misturadores não estariam no livro de códigos, o emissor da mensagem tinha que transmiti-las em segurança para o receptor [...] (2011, p. 168).

- 1) O emissor ajusta sua máquina Enigma com a chave do dia, com por exemplo, QCW como orientação para os misturadores.
- 2) Escolhe ao acaso uma nova orientação para os misturadores, por exemplo PGH.
- 3) Ele cifra PGH de acordo com a chave do dia. A chave da mensagem é datilografada duas vezes, para fornecer uma dupla verificação ao receptor. Por exemplo, cifrando a chave da mensagem PGHPGH como KIVBJE.
- 4) O emissor muda a máquina então para o ajuste PGH e cifra a mensagem de acordo com sua chave de mensagem.
- 5) No local onde a mensagem é recebida, a máquina é ajustada inicialmente com a chave do dia original, QCW.
- 6) As primeiras seis letras da mensagem, KIVBJE, são datilografadas e revelam PGHPGH.
- 7) O receptor deve então ajustar seus misturadores para a chave da mensagem PGH, e então pode passar a decifrar o resto da mensagem.

Ou seja, ao invés de usar a cifra principal para cifrar todas as mensagens, os operadores a usavam para cifrar a nova chave de cada mensagem, cifrando-a de acordo com a nova chave.

Embora esse sistema parecesse invencível, havia como combatê-lo. Para isso, o *Biuro Szyfrów* contratou matemáticos da Universidade de Poznán, localizada num território que fora da Alemanha até 1918, fluentes em alemão. Explica Singh:

“Durante séculos presumira-se que os melhores criptoanalistas seriam peritos na estrutura da linguagem, mas a chegada da Enigma levou os poloneses a mudarem sua política de recrutamento. [...] O Biuro organizou um curso de criptografia e convidou vinte matemáticos. [...] Três dos vinte demonstraram uma aptidão para solucionar cifras e foram recrutados (2011, p. 169).

A seção no *Biuro Szyfrów* encarregada das mensagens alemãs chamava-se BS-4.

8.1.1 Marian Rejewski

Os três matemáticos eram Marian Rejewski, Jerzy Rozycki e Henryk Zygalski. Rejewski (1905-1980) era um especialista em estatística (esperava fazer um carreira no ramo de seguros) que tinha grande habilidade com cifras tradicionais (KAHN, 1991, p. 54).

Trabalhando sozinho, inicialmente ele analisou os detalhes disponíveis da máquina Enigma e seus aspectos de operação, testando exaustivamente os efeitos provocados pelos rotores e pelo painel de ligação, procurando repetições. A repetição produz padrões, e os criptoanalistas usam padrões para quebrar cifras.



Figura 8.1: Marian Rejewski (WIKIPEDIA, 2012).

A repetição mais óbvia na cifragem da Enigma era a chave da mensagem, cifrada duas vezes no início de cada mensagem, que Rejewski isolava das mensagens interceptadas recebidas em lotes.

Para ilustrar como o código começou a ser quebrado, será usado o exemplo disponível em Singh (2011). Se o operador escolhesse, por exemplo, ULJ como chave de mensagem, então ela teria de ser cifrada duas vezes, de maneira que ULJULJ se tornaria, por exemplo, PEFNWZ, que seria enviada primeiro, antes da mensagem real. A repetição era necessária para evitar erros na transmissão ou dos operadores.

Uma nova remessa de mensagens interceptadas se tornava disponível todos os dias, todas elas começando com as seis letras da repetição da chave de mensagem, cifradas com a mesma chave do dia. Continuando com o exemplo de Singh (2011), seriam recebidas quatro mensagens que começariam com as chaves de mensagem cifradas mostradas a seguir.

Tabela 7.1: Chaves de mensagem cifradas

	1 ^a	2 ^a	3 ^a	4 ^a	5 ^a	6 ^a
Primeira mensagem	L	O	K	R	G	M
Segunda mensagem	M	V	T	X	Z	E
Terceira mensagem	J	K	T	M	P	E
Quarta mensagem	D	V	Y	P	Z	X

Fonte: SINGH, 2011, p. 170.

Apesar de restritas a apenas duas letras, há repetições nas duas chaves iniciais: no texto claro, a 1^a e a 4^a letras são iguais, a 2^a e a 5^a, a 3^a e a 6^a. Como todas as chaves eram cifradas de acordo com a mesma chave do dia, se o número de mensagens fosse suficientemente grande, seria possível obter-se um alfabeto cifrante completo.

Por exemplo, na primeira mensagem L e R eram as cifras de uma única letra do texto claro, e a cifra R foi obtida após um deslocamento de três posições do rotor. O fato de que L e R eram cifras da mesma letra permitiu que Rejewski deduzisse uma característica do ajuste inicial da máquina: o ajuste do primeiro misturador, que é desconhecido, cifrou a primeira letra, também desconhecida, como L e então, outra disposição, três casas a partir da disposição inicial, também desconhecida, cifrou a mesma letra da chave diária, desconhecida, como R. Isso mostra que, mesmo cheia de fatores desconhecidos, existe uma ligação entre as letras L e R criada pelo ajuste inicial da máquina, ou seja, criada pela chave do dia.

Segundo o exemplo, a segunda mensagem mostra que M e X estão relacionadas, a terceira mostra que J e M estão relacionadas e quarta mensagem mostra que D e P estão

relacionadas. Rejewski começou então a resumir essas ligações entre (L,R), (M,X), (J,M) e (D,P) em uma tabela de relacionamento. Mesmo não sendo possível ainda deduzir a posição inicial dos rotores, a posição dos cabos no painel de plugues e a letra a qual correspondiam L e R, era possível afirmar que essas letras estavam relacionadas com a chave do dia. Baseando-se no exemplo das chaves, era possível obter uma tabela incompleta de relacionamentos como a mostrada abaixo.

Tabela 7.2: Relacionamento parcial de uma chave do dia

1 ^a letra	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
4 ^a letra						P					M	R	X													

Fonte: SINGH, 2011, p. 171.

Se Rejewski tivesse acesso a um número suficiente de mensagens em um único dia, poderia completar o alfabeto de relacionamentos. A título de exemplo, imagine-se que foram encontrados os relacionamentos completos mostrados na tabela abaixo.

Tabela 7.3: Relacionamento completo de uma chave do dia

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

Fonte: SINGH, 2011, p. 171.

Embora a tabela de relacionamentos não mostrasse ainda qual era a chave do dia ou quais chaves de mensagem estavam sendo escolhidas, Rejewski sabia que elas resultavam dessa tabela de relacionamentos. A chave estaria lá, representada de alguma forma: se a tabela do dia fosse diferente, também seria a chave.

Rejewski começou a procurar padrões dentro da tabela, estruturas que indicassem a chave diária. Ele começou a estudar um tipo específico de padrão, que produzia correntes de letras. Na tabela do exemplo de Singh (2011) acima, o A na primeira fileira era ligado ao F na fileira de baixo. Procurando o F na fileira de cima, descobre-se que ele está ligado ao W. Procurando o W na fileira de cima, descobre-se que ele está ligado ao A. A corrente está completa.

Com o restante das letras do alfabeto, Rejewski podia gerar outras correntes. A seguir, uma lista de todas as correntes e número de ligações, ou elos, de cada uma (SINGH, 2011, p. 173).

A > F > W > A	3 ligações
B > Q > Z > K > V > E > L > R > I > B	9 ligações
C > H > G > O > Y > D > P > C	7 ligações
J > M > X > S > T > N > U > J	7 ligações

Até o momento, estão sendo consideradas as ligações apenas entre a primeira e quarta letras da chave repetida de seis letras. Rejewski repetiria ainda o processo para as relações entre a segunda e a quinta letras e para a terceira e a sexta letras, identificando as correntes e o número de elos em cada uma.

As correntes mudavam a cada dia, assim como seu tamanho e as letras dentro delas. Ficava claro que as características das correntes estavam relacionadas com o resultado

do ajuste da chave diária. A questão que permanecia era como seria possível determinar a chave diária a partir dessas correntes. Relata Singh:

Foi nesse ponto que Rejewski teve um *insight* profundo. Embora a disposição do quadro de tomadas e o ajuste dos misturadores afetassem os detalhes das correntes, suas contribuições poderiam ser separadas. [...] O número de elos nas correntes é puramente uma consequência do ajuste dos misturadores (2011, p. 173).

No exemplo de Singh (2011, p. 174), presumindo-se que a chave diária exigisse que as letras S e G fossem trocadas como parte da disposição do painel de plugues, caso se retirasse o cabo ligando S e G e colocando-o, por exemplo, entre as letras T e K, as correntes mudariam da seguinte maneira:

A > F > W > A	3 ligações
B > Q > Z > T > V > E > L > R > I > B	9 ligações
C > H > S > O > Y > D > P > C	7 ligações
J > M > X > G > K > N > U > J	7 ligações

Nota-se que algumas letras nas correntes mudaram, mas o número de elos em cada corrente permaneceu constante, reflexo unicamente do ajuste dos misturadores.

O lance de genialidade de Rejewski foi perceber que as configurações dos rotores e do painel de plugues não atuavam em bloco, embora ambas afetassem as cadeias, ou seja, podia-se separar a participação desses elementos. No caso dos cabos no painel de plugues, se todos os cabos fossem retirados (a máquina Enigma estaria funcionando sem painel de plugues) o número de elos na cadeia continuaria o mesmo, e a única alteração seriam as letras que compunham as cadeias.

Essa descoberta diminuía a ordem de grandeza do problema em bilhões de vezes. Com esse dado em mãos, Rejewski e uma equipe passaram a trabalhar com réplicas de máquinas Enigma. Um ano depois, as mais de 100 mil combinações possíveis haviam sido testadas, e as cadeias resultantes de cada uma das configurações tinham sido anotadas: o *Biuro Szyfrów* possuía um catálogo das sequências e dos comprimentos de cadeias associados a cada uma das possíveis configurações da máquina.

Cada dia, quando novas mensagens chegavam, Rejewski olhava as chaves de mensagem cifradas (as primeiras seis letras das mensagens interceptadas) e usava essa informação para construir uma tabela de relacionamentos, que permitiria rastrear as correntes e estabelecer o número de ligações em cada uma. Continuando com o exemplo em Singh (2011), a análise poderia achar os seguintes três conjuntos de correntes abaixo:

4 correntes da primeira e da quarta letras com	3, 9, 7 e 7 ligações
4 correntes da segunda e da quinta letras com	2, 3, 9 e 12 ligações
5 correntes da terceira e da sexta letras com	5, 5, 5 e 8 ligações

Os poloneses se dedicaram então à criação de um catálogo de cartões desses padrões de ciclo. Rejewski, por volta de 1935, inventou uma máquina para facilitar esta tarefa: o ciclômetro.

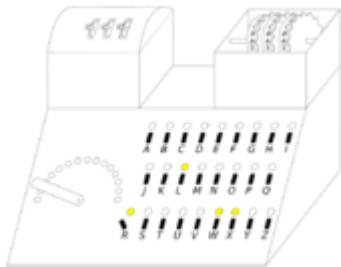


Figura 8.2: Ciclômetro de Rejewski (WIKIPEDIA, 2012).

Este dispositivo compreendia dois conjuntos de rotores conectados por cabos através dos quais a corrente eléctrica podia passar. O rotor N do segundo conjunto ficava três letras fora de fase com relação ao rotor N do primeiro conjunto, ao passo que os rotores L e M do segundo conjunto estavam definidos da mesma maneira que os rotores L e M no primeiro conjunto (WIKIPEDIA, 2012). A preparação do catálogo usando o ciclômetro durou mais de um ano, mas quando ficou pronto, fez com que obter as chaves diárias fosse questão de aproximadamente 15 minutos.

Mais detalhes podem ser vistos no artigo *An Application of the Theory of Permutations in Breaking the Enigma Cipher* (Uma aplicação da teoria das permutações na quebra da Cifra Enigma), a primeira publicação sobre a base matemática usada para quebrar a cifra (REJEWSKI, 1980).

O próximo passo era estabelecer a disposição dos cabos no painel de plugues. Embora houvesse centenas de bilhões de possibilidades, a tarefa não era difícil. Para isso, Rejewski começaria ajustando os misturadores na réplica da máquina Enigma de acordo com o resultado da análise da chave diária. Em seguida, eram retirados todos os cabos do painel de plugues. Um trecho de texto cifrado seria datilografado, resultando numa sequência de letras sem sentido, já que a configuração dos cabos era desconhecida e estava ausente (SINGH, 2011, p. 175).

Mesmo assim, explica Singh (2011, p. 175), frequentemente algumas frases vagamente reconhecíveis apareciam, como por exemplo “alliveinbelrin”, que poderia significar “arriveinberlin” (*arrive in Berlin*, ou chega em Berlim). Era então testada a troca das letras R e L no painel de plugues. Analisando mais partes do texto, logo seria possível identificar os outros cinco pares de letras trocadas.

Sabendo a disposição dos cabos no painel de plugues e o ajuste dos rotores, problemas que separados eram solucionáveis, a decifração da chave diária estava completa, e Rejewski poderia passar a decifrar todas as mensagens interceptadas daquele dia, mesmo que não fosse possível ler todas as mensagens regularmente (KAHN, 1991, p. 68).

Embora não estivesse em guerra com a Alemanha, ter acesso às comunicações do país vizinho era um importante trunfo para a Polônia. Os poloneses usaram durante muitos anos com sucesso, a partir de 1932, a técnica de Rejewski.

8.1.2 Bombas criptológicas

Quando os alemães alteraram a maneira como transmitiam as mensagens, logo Rejewski e sua equipe aposentaram o catálogo de comprimentos de correntes, que havia se tornado inútil, e projetaram uma versão mecanizada do sistema de catalogação que poderia procurar automaticamente os ajustes corretos dos misturadores (SINGH, 2011, p. 177).

Foi então construída em 1938 a primeira bomba criptológica, uma máquina semi-automática que foi usada para recuperar a chave. O nome vinha do barulho feito pelo dispositivo. De acordo com Rejewski, era capaz de recuperar as configurações-chave em menos de duas horas. Embora todas as bombas tenham sido destruídas em 1939, pouco antes de os alemães invadirem a Polônia, Rejewski fez um esboço muitos anos mais tarde, conforme mostrada abaixo (CRYPTO, 2012).

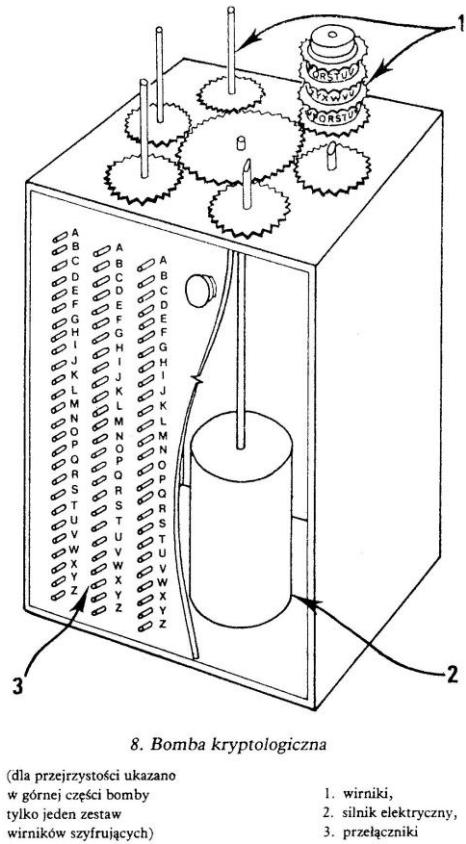


Figura 8.3: Bomba criptológica polonesa (CRYPTO, 2012).

A máquina era baseada no princípio de que as chaves de mensagem de 3 letras eram enviadas duas vezes, no início de cada mensagem, e que uma letra de texto claro em particular poderia ser a mesma três posições à frente, como por exemplo AWB e TWI. Essas coincidências eram chamadas de fêmeas. Como ambos os grupos de letras se originariam do mesmo texto claro, era possível procurar por uma combinação única.

Se as fêmeas suficientes fossem encontradas, a bomba podia ser utilizada para encontrar a posição dos anéis. As posições iniciais de rodas já eram dadas no começo da mensagem (CRYPTO, 2012).

Como os alemães usavam apenas 3 rotores na época (I, II e III), havia seis ordens possíveis a ser investigadas. Isso era feito através da execução 6 bombas em paralelo. Cada bomba tinha 6 conjuntos completos de rotores Enigma em sua superfície superior (mostrado como 1 na figura 7.3). Eles eram conectados em pares, e cada par era usado para resolver uma de três fêmeas.

Para descobrir a posição dos anéis, a configuração do painel de plugues não precisa ser levada em consideração, uma vez que não muda de posição durante a cifragem. O

que importava era que a mesma letra de entrada produzia o mesmo resultado duas vezes, com três passos de separação (CRYPTO, 2012).

Como explica Crypto (2012), “Ainda que a operação exata da bomba permaneça desconhecida, muito tentaram explicar seu princípio reconstruindo o modelo teórico”.

Rejewski e seus colegas passaram grande parte da década de 1930 trabalhando incansavelmente na descoberta das chaves da Enigma. No entanto, grande parte de seu trabalho era desnecessária, uma vez que o diretor do *Biuro Szyfrów*, major Gwido Langer, recebeu ao longo de sete anos 38 meses de chaves diárias, recebidas de Hans-Thilo Schmidt através dos franceses. Eram exatamente os mesmos livros de códigos “distribuídos a todos os operadores alemães de máquinas Enigma e continham toda a informação necessária para cifrar e decifrar mensagens” (SINGH, 2011, p. 177).

A motivação de Langer para não tornar conhecido o conteúdo dos documentos que possuía possivelmente era fazer com que Rejewski e seus colegas estivessem preparados para a eventual falta de informações privilegiadas que a iminente guerra causaria.

Contudo, em 1938, dois rotores extras foram incorporados à Enigma, fazendo com que o arranjo dos rotores pudesse ser qualquer conjunto de três dos cinco rotores. Se antes existiam seis modos de escolhê-los, agora o número passava para 60. Tornava-se necessário descobrir a fiação interna dos dois novos rotores e construir um número dez vezes maior de bombas. Explica Singh:

O custo de construir essa bateria de bombas era quinze vezes maior do que todo o orçamento anual do Biuro para gastos com equipamentos. E no mês seguinte a situação piorou, quando o número de fios no quadro de tomadas aumentou de seis para dez. No lugar de doze letras sendo trocadas [...] agora havia vinte (2011, p. 178).

Isso fez com que chegasse ao limite os esforços poloneses de decifragem da Enigma. Se em 1938 as interceptações e decifragens tinham chegado ao máximo, no começo de 1939 elas se tornaram virtualmente impossíveis para os recursos do *Biuro Szyfrów*. Para piorar, Schmidt havia rompido contato com os franceses e não havia novos documentos secretos sendo entregues (SINGH, 2011, p.180).

Ao mesmo tempo, crescia a tensão entre Polônia e Alemanha. Em abril de 1939 a Alemanha descumpriu o tratado de não-agressão firmado com o país, e ficou claro que uma guerra estava prestes a começar.

Disposto a não perder todos os avanços conseguidos pelos poloneses no caso de uma invasão alemã, o diretor do *Biuro Szyfrów* decidiu compartilhar o conhecimento oculto até então dos aliados com França e Grã-Bretanha. Em julho de 1939, Langer convidou criptoanalistas e militares franceses e britânicos ao quartel general do *Biuro Szyfrów*.

Após mostrar que os poloneses decifravam a Enigma há anos, Langer ofereceu aos aliados duas réplicas sobressalentes da Enigma e as plantas e diagramas das bombas. Duas semanas depois, a Polônia seria invadida pela Alemanha (SINGH, 2011, p.181).

8.2 Bletchley Park

Ao longo de treze anos, de 1926 a 1939, britânicos e franceses haviam acreditado que a cifra da máquina Enigma era indecifrável. Mas as revelações obtidas na Polônia mostravam que a cifra tinha falhas.

Também foi aprendido com os poloneses o uso do trabalho de matemáticos como decifradores de códigos. Se na Inglaterra, como diz Singh, “a Sala 40 sempre fora dominada por linguistas e especialistas nos clássicos, [...] agora havia um esforço concentrado para equilibrar a equipe com matemáticos e cientistas” (2011, p. 180). E eles foram contratados principalmente em Oxford e Cambridge, através das redes de contatos daqueles que trabalhavam na Sala 40.

Os novos contratados, a partir de 1939, eram levados direto para Bletchley Park, em Buckinghamshire, Inglaterra, onde ficava a sede da Escola de Cifras e Códigos do Governo (*General Code and Cipher School*, ou GC&CS), que substituiria a Sala 40.

Bletchley Park era uma propriedade rural construída na época da batalha de Hastings (1066) e que, em sua origem, foi apenas uma modesta casa de fazenda. Comprada em 1883 pelo financista londrino sir Herbert Leon, a casa foi transformada em uma mansão decorada com excessos. Entre os muitos acréscimos feitos, estavam uma biblioteca e um salão de baile, assim como uma fachada em tijolo e pedra.

Bletchley Park podia alojar uma equipe muito maior, o que era imprescindível devido à enorme quantidade de mensagens cifradas que era esperada assim que começasse a guerra. Explica Singh:

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 (2011, p. 182).

Ainda segundo Singh, se no começo a equipe era formada por apenas duzentas pessoas, em cinco anos a Bletchley Park estaria alojando sete mil homens e mulheres (2011).

A sua facilidade de acesso, sua grande amplitude e sua localização (uma vez que estava a meio caminho na estrada de ferro que à época ligava Oxford e Cambridge), levaram a propriedade a ser comprada pelo Almirante Hugh “Quex” Sinclair para servir de base para as atividades do GC&CS durante a Segunda Guerra Mundial. O comandante Alastair Denniston (1881-1961), diretor do GC&CS, tinha um escritório no andar térreo com vista para os jardins (NATIONAL, 2012).



Figura 8.4: Bletchley Park (WIKIPEDIA, 2012).

Mas a vista logo seria prejudicada pela construção de muitas casinhas de madeira, chamadas de *huts*, que alojavam as várias atividades de quebra de códigos e destoavam da imponência do prédio principal.

O *hut 8* e seus criptoanalistas eram especializados na Enigma naval, passando suas mensagens para o *hut 4*, próximo a eles, onde estavam os analistas de inteligência naval, que traduziam e anexavam comentários às mensagens interceptadas resolvidas. Os criptoanalistas do *hut 6* se dedicavam a decifrar as mensagens usando Enigma interceptadas do Exército e da Força Aérea alemães, passando as mensagens decifradas para o *hut 3*, onde eram traduzidas e analisadas para ser usadas.

Bletchley Park contava com uma equipe maior e mais recursos do que o *Biuro Szyfrów*: “Durante o outono de 1939 os cientistas e matemáticos de Bletchley aprenderam as minúcias da cifra Enigma e rapidamente dominaram as técnicas polonesas” (SINGH, 2011, p. 183). Por terem mais recursos e uma equipe maior, foram capazes de lidar com uma seleção maior de rotores e com o fato de a Enigma estar dez vezes mais difícil de decifrar.

Todos os dias os decifradores de códigos passavam pela mesma rotina: à meia noite os operadores alemães mudavam suas máquinas Enigma para novas chaves diárias, fazendo com que quaisquer avanços feitos no dia anterior não pudessem mais ser usados para decifrar as mensagens. A cada novo dia, o trabalho de identificação da chave do dia era recomeçado.

Assim que conseguiam descobrir a chave diária, a equipe de Bletchley Park passava a decifrar todas as mensagens daquele dia, tornando transparentes os planos alemães. Entre as informações conseguidas com a decifragem das comunicações estavam detalhes da operação alemã de invasão da Dinamarca e da Noruega em abril de 1940 e detalhes da Batalha da Inglaterra, que permitiram ser dado um alerta prévio com as horas e locais dos ataques dos bombardeiros, assim como dados atualizados da Força Aérea alemã.

8.2.1 Fraquezas nos procedimentos operacionais

Já dominando as técnicas polonesas, os criptoanalistas britânicos melhoraram seus próprios métodos: “por exemplo, eles aproveitavam o fato de que os operadores alemães da Enigma ocasionalmente escolhiam chaves de mensagem óbvias” (SINGH, 2011, p. 185). Para cada chave de mensagem deveriam ser escolhidas três letras aleatórias, conforme visto anteriormente.

O que acabava acontecendo rotineiramente, no entanto, era a escolha de três letras consecutivas no teclado, como QWE ou TZU (nos teclados alemães) ou as primeiras três letras do nome da namorada do operador. Também eram usadas palavras obscenas, posição em que os rotores estavam no final da cifragem da mensagem anterior e o JABJAB, quando as configurações do dia e da chave da mensagem eram idênticas. Essas chaves previsíveis, junto com o uso repetido da mesma chave de mensagem acabaram recebendo o nome de *cillies*, provavelmente numa referência a *sillies*, que poderia ser interpretado como tolices (KAHN, 1991, p. 112-113).

Outro método utilizado para decifrar as Enigma era o palpite de Herivel, criado por John Herivel, estudante de matemática que trabalhava no *hut 6*. Ele antecipou um hábito

dos operadores de máquinas Enigma: o uso das letras que apareciam para o operador depois de configurar os rotores e os anéis. A primeira mensagem depois de uma troca de chave frequentemente teria um indicador que daria a posição inicial dos rotores próxima à da configuração dos anéis para o período da chave (SULLIVAN, 2005, p. 211).

Segundo Singh, “os *cillies* não eram fraquezas da máquina Enigma, eles eram fraquezas do modo como a Enigma estava sendo usada”. Erros humanos, inclusive nos mais altos níveis da cadeia de comando, também comprometiam a cifra (2011, p. 185).

Mais ajuda veio de características dos procedimentos criptográficos alemães. A Força Aérea não usava o mesmo rotor na mesma posição em dias consecutivos (por exemplo, se a ordem dos rotores fosse I, III, IV, não poderia ser II, I, IV no dia seguinte), o que diminuía o número de ordens de rotores a serem testadas com as bombas pela metade.

Também não era permitido o uso de duas letras consecutivas serem ligadas no painel de plugues (por exemplo, S não podia estar ligada a R ou a T), o que permitiu que fosse adicionado às bombas um circuito chamado CSKO (*Consecutive stecker knock-out*) que também diminuía o número de chaves possíveis nos testes (KAHN, 1991, p. 113-114).

8.2.2 Fraquezas da máquina Enigma

Além dos procedimentos operacionais alemães que poderiam ter sido mais fortes mencionados anteriormente, o projeto básico de uma máquina Enigma tinha uma série de fraquezas que ajudaram os decifradores. Abaixo está uma lista desenvolvida por Crypto (2012).

8.2.2.1 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).

8.2.2.2 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.

8.2.2.3 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.

8.2.2.4 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.

8.2.2.5 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.

8.2.2.6 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.

8.2.2.7 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.

8.2.3 Alan Turing

O trabalho em Bletchley Park seguia a estratégia de passar um problema intratável para o *huts* seguinte, de maneira que chegasse a alguém com capacidade de resolvê-lo, ou resolvê-lo de maneira parcial antes de enviá-lo ao próximo *hut*. Era um esforço conjunto levando a avanços notáveis. Relata Singh:

A busca por novos atalhos criptoanalíticos era necessária porque a máquina Enigma continuou a evoluir ao longo da guerra. Os criptoanalistas eram continuamente forçados a inovar, a reprojetar e melhorar as bombas e a criar estratégias inteiramente novas. (2011, P. 186).

Entre os muito criptoanalistas notáveis desse esforço conjunto estava o matemático inglês Alan Turing (1912-1954), responsável por identificar a maior fraqueza da máquina Enigma, descrita a seguir.

Contratado em 1939, Turing chegou a Bletchley Park um dia depois de a Inglaterra declarar guerra à Alemanha, viajando sob o disfarce de membros do destacamento de tiro do Capitão Ridley. Segundo Singh, ele passava parte do tempo nos *huts* “contribuindo para o esforço rotineiro de quebra de códigos, e parte do tempo na sala de pesquisas teóricas de Bletchley” (2011, p. 190).

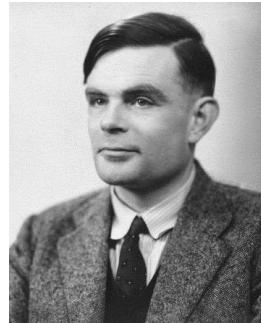


Figura 8.5: Alan Turing (WIKIPEDIA, 2012).

Antevendo que logo os operadores alemães abandonariam o procedimento de cifrar duas vezes cada chave de mensagem, Turing ficou responsável por encontrar um modo alternativo para decifrar a Enigma.

Percebendo que Bletchley Park estava acumulando uma vasta biblioteca de mensagens decifradas, e que muitas delas obedeciam a uma estrutura rígida, ele acreditava que poderia ser possível prever parte do conteúdo de mensagens ainda não decifradas baseando-se em quando e onde elas foram enviadas.

Singh (2011, p. 191) explica um exemplo: “a experiência mostrava que os alemães enviavam relatórios cifrados sobre a previsão do tempo logo depois das seis horas da manhã de cada dia”. Assim, uma mensagem interceptada pouco depois das 6hs quase que certamente conteria a palavra *Wetter* (tempo, em alemão).

O rigoroso protocolo militar alemão fazia com que as mensagens fossem muito parecidas em seu estilo, de modo que Turing podia até mesmo ter uma ideia da posição em que estaria a palavra *Wetter* dentro de uma mensagem cifrada.

Por exemplo, a experiência trazida de mensagens decifradas anteriormente poderia indicar que as primeiras seis letras de um certo texto cifrado correspondiam a *Wetter*. E a essa associação de um pedaço de texto original com um pedaço do texto cifrado se dava o nome de *crib*.

Turing acreditava que poderia usar os *cribs* para decifrar a Enigma. Um exemplo do uso dos *cribs* é o mostrado em Singh (2011) e visto a seguir. Se Turing tivesse um texto cifrado e conhecesse um trecho específico dele, como por exemplo ETJWPX representando *wetter*, o desafio seria identificar os ajustes da Enigma que transformariam *wetter* em ETJWPX. Normalmente o que seria feito era a datilografar *wetter* em uma Enigma e descobrir se sairia o texto cifrado. Caso não saísse, o criptoanalista mudaria as configurações da máquina (como visto anteriormente) e tentaria novamente até conseguir.

O problema com essa abordagem de tentativa e erro era o fato de existirem aproximadamente $1,07 \times 10^{23}$ possibilidades, no caso das máquinas usadas pelo Exército e pela Força Aérea, e $1,56 \times 10^{25}$ possibilidades, no caso da Enigma M4 naval, a serem testadas, tarefa aparentemente impossível.

8.2.4 Dividindo o problema e as bombas britânicas

Para simplificar o problema, Turing tentou seguir a estratégia de Marian Rejewski de separar os ajustes: separando o problema de encontrar os ajustes dos rotores do

problema encontrar as ligações no painel de plugues, ele poderia primeiro encontrar um, depois o outro. Ele passou então a estudar um tipo especial de *crib* com ligações internas semelhantes às correntes exploradas por Rejewski.

Segundo Singh, “as correntes de Rejewski ligavam letras dentro da chave de mensagem repetida. Contudo, os elos de Turing [...] conectavam letras do texto original e do texto cifrado dentro de uma cola” (2011, p. 192-193). Seguindo com o exemplo de Singh, o *crib* mostrado na figura a seguir possui um elo (ou laço).

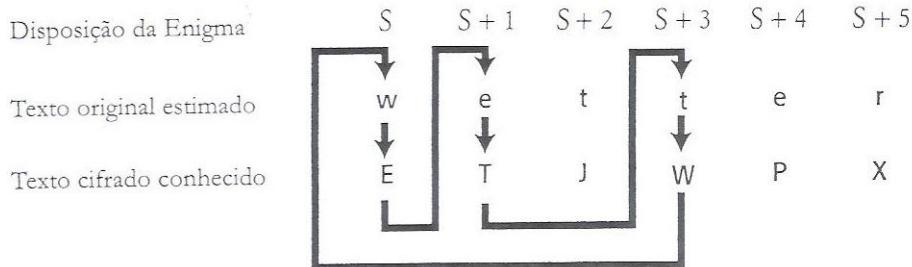


Figura 8.6: Um *crib* mostrado como elo (SINGH, 2011, p. 192).

Embora sejam apenas suposições, se for assumido que o *crib* está correto, é possível ligar as letras $w > E$, $e > T$, $t > W$ como parte de um elo. Sem saber ainda quais eram os ajustes da Enigma, era possível rotular o primeiro ajuste como S , e nele w é cifrado como E . Depois da primeira cifragem, o primeiro rotor move-se uma casa, para a posição $S + 1$, e a letra e é cifrada como T . O rotor avança outra casa e cifra uma letra que não está no elo – essa cifragem será ignorada. O rotor gira e chega-se a uma letra que está no elo. No ajuste $S + 3$ é sabido que a letra t é cifrada em W . Abaixo, um resumo:

No ajuste S	a Enigma cifra w como E .
No ajuste $S + 1$	a Enigma cifra e como T .
No ajuste $S + 3$	a Enigma cifra t como W .

Turing viu que os relacionamentos dentro do elo davam o atalho de que precisava. No lugar de trabalhar com uma máquina Enigma para testar cada ajuste possível, ele imaginou três máquinas separadas, cada uma lidando com a cifragem de um elemento do elo: a primeira tentaria cifrar w em E , a segunda e em T e a terceira t em W . As três máquinas teriam ajustes iguais exceto pela segunda ter as orientações de seus rotores deslocadas de uma casa em relação à primeira (ajuste $S + 1$) e a terceira tendo as orientações deslocadas em três casas com relação à primeira (ajuste $S + 3$).

O passo seguinte da ideia de Turing, como relata Singh (2011, p 194), foi ligar as três máquinas, conectando as entradas e as saídas de dados de cada máquina, conforme mostrado no diagrama abaixo, onde o elo no *crib* é reproduzido pelo elo no circuito elétrico.

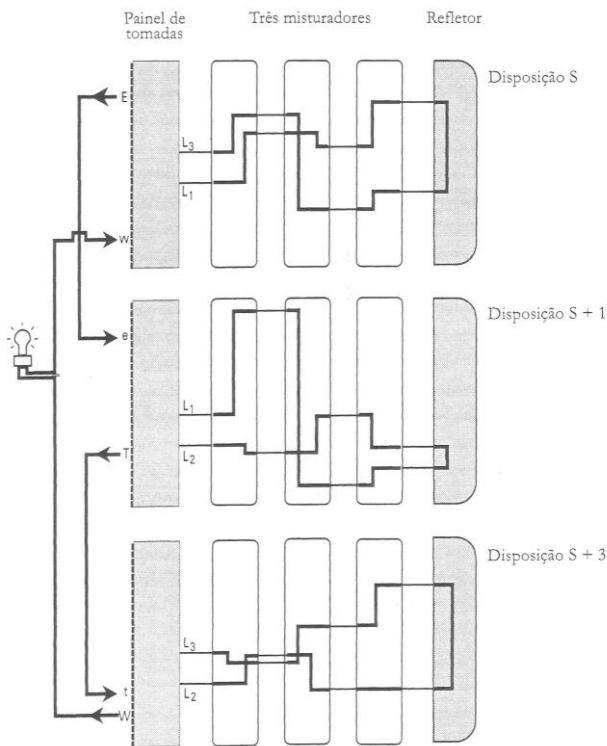


Figura 8.7: Circuito completo com 3 máquinas Enigma (SINGH, 2011, p. 196).

Turing imaginou o dispositivo de tal maneira que, segundo Singh, apenas “quando todos os ajustes estivessem corretos, para todas as três máquinas, é que o circuito se completaria, permitindo que a corrente fluísse entre todas as máquinas”. Caso fosse acrescentada “uma lâmpada ao circuito, a passagem de corrente faria com que ela se acendesse, sinalizando que o ajuste correto fora encontrado” (2011, p 194).

O salto lógico seguinte de Turing foi o que simplificou em diversas ordens de grandeza a tarefa de testar todas as possibilidades de ajustes. “Turing tinha montado o seu circuito elétrico de tal modo a anular o efeito do quadro de tomadas, de modo que pudesse ignorar os bilhões de ajustes possíveis na disposição dos fios” (Singh, 2011, p. 194): os quadros de tomadas cancelavam-se mutuamente ao longo do circuito inteiro, aos pares.

Agora Turing só precisava ligar a saída do primeiro conjunto de rotores L₁ na entrada do segundo conjunto de rotores L₁, e assim por diante. Como o valor da letra L₁ não era conhecido, era necessário conectar todas as 26 saídas do primeiro conjunto de rotores a todas as 26 entradas correspondentes no segundo conjunto de rotores, e assim por diante, num total de 26 circuitos elétricos, cada um com uma lâmpada para sinalizar quando um circuito fosse completado. Como relata Singh:

Os três conjuntos de misturadores então simplesmente verificariam cada um das 17.576 orientações [...]. Quando as orientações corretas [...] fossem encontradas, um dos circuitos se completaria e uma lâmpada acenderia (2011, p. 195).

O projeto seguiu adiante e os dispositivos receberam o nome de bombas, tal como as bombas criptológicas polonesas. Cada uma das bombas de Turing consistia em doze

conjuntos de rotores conectados eletricamente capazes de lidar com elos mais longos. Explica Singh:

A unidade completa teria dois metros de altura, por dois de comprimento e um metro de largura. Turing finalizou o projeto no início de 1940, e o trabalho de construção foi entregue à fábrica British Tabulating Machinery, em Letchworth (2011, p. 197).

A bomba ajudava a identificar a ordem dos rotores nas Enigma, as posições iniciais dos rotores e o par da letra sendo trocada. Isso era conseguido testando todos as possíveis 17.576 posições para um conjunto de ordens de rotores em uma comparação entre um *crib* e um texto cifrado, de modo a eliminar possibilidades que contradiziam características conhecidas do Enigma (WIKIPEDIA, 2012). A tarefa da bomba era simplesmente reduzir as supostas possibilidades para um número gerenciável.

Os rotores desmontáveis na frente da bomba eram ligados de forma idêntica às ligações feitas por diferentes rotores Enigma. Ao contrário deles, no entanto, os contatos de entrada e de saída para o lado esquerdo e os lados direitos eram separados, fazendo 104 contatos entre cada cilindro e o resto da máquina. Isso permitia um conjunto de rotores serem ligados em série por meio de 26 cabos. Conexões elétricas entre os cabos dos rotores rotativos e o painel traseiro de plugues eram feitas por escovas de metal; Quando a bomba detectava uma posição dos rotores sem contradições, ela parava e o operador observava a posição antes de reiniciá-la (WIKIPEDIA, 2012).

Existia uma melhoria no design da bomba chamada quadro diagonal que explorava a reciprocidade das conexões no painel de plugues, reduzindo consideravelmente o número de configurações dos rotores que precisariam ser consideradas.

A imagem abaixo mostra a parte de trás de uma das bombas, reconstruída em Bletchley Park.



Figura 8.8: Bomba britânica reconstruída (DAY, 2012).

Mas antes que as bombas pudessesem começar a procurar uma chave, no entanto, era necessário encontrar *cribs*. Os criptoanalistas os dariam aos operadores das bombas, mas não havia garantias do significado correto do texto cifrado nem da posição correta (SINGH, 2011, p. 198).

Havia, no entanto, um truque para verificar se a posição do *crib* estava correta. Conforme o exemplo em Singh (2011, p. 199), o *crib* não poderia estar na posição mostrada abaixo, uma vez que a máquina Enigma não cifrava uma letra nela mesma.

Texto original estimado	w e t t e r n u l l s e c h s
Texto cifrado conhecido	I P R E N L W K M J J S X C P L E J W Q

Figura 8.9: Teste de posição de um *crib* (SINGH, 2011, p. 199).

Para achar o alinhamento correto, era necessário apenas “deslizar” o texto original e o texto cifrado até que nenhuma letra igual apareça em ambos simultaneamente. Abaixo, o texto original foi deslizado uma casa para a direita.

Texto original estimado	w e t t e r n u l l s e c h s
Texto cifrado conhecido	I P R E N L W K M J J S X C P L E J W Q

Figura 8.10: Posição correta de um *crib* (SINGH, 2011, p. 199).

Bem como escolher um *crib*, era necessária uma decisão quanto a qual das muitas possíveis ordens de rotores poderia ser omitida. O bamburismo de Turing (método que tentava prever os rotores mais à direita e do meio da Enigma) era usado para fazer essa economia. O criptoanalista, então, elaborava um cardápio que especificava as conexões dos cabos dos painéis na parte de trás da máquina, e uma letra cujo par era procurado. O menu refletia as relações entre as letras do *crib* e as do texto cifrado. Algumas dessas letras formavam loops, de forma similar às correntes que os poloneses haviam explorado (WIKIPEDIA, 2012).

Ainda segundo a Wikipedia (2012), a natureza recíproca do painel de plugues significava que nenhuma letra podia ser conectada a mais de uma letra. Quando havia uma contradição entre duas letras diferentes que aparentemente eram um par no painel com a letra no menu, a bomba detectaria e seguiria em frente. Se, no entanto, isso aconteceu com uma letra que não fazia parte do menu, uma falsa parada ocorria. Refinando o conjunto de paradas para um exame aprofundado, o criptoanalista eliminaria paradas que continham tal contradição.

As paradas restantes decifrariam os *cribs* corretamente, mas apenas a parada verdadeira iria produzir o texto claro correto de toda a mensagem (WIKIPEDIA, 2012).

Turing e os demais criptoanalistas continuaram seu trabalho, e tudo que se referia à Escola de Códigos e Cifras do Governo continuou altamente secreto. Ninguém fora de Bletchley Park sabia dos códigos serem decifrados (SINGH, 2011, p.197).

O protótipo da primeira bomba foi apelidado de *Victory*, mas seus resultados não foram satisfatórios. Enquanto esperavam pela construção do segundo protótipo, os criptoanalistas se depararam com o desafio que já haviam previsto: em 10 de maio de 1940 os alemães mudaram o protocolo de troca de chaves: a chave de mensagem não era mais repetida. O número de mensagens decifradas caiu drasticamente (SINGH, 2011, p.198).

O blecaute nas informações durou até 08 de agosto de 1940, quando a nova bomba chegou. Batizada de *Agnus Dei* e apelidada *Agnes*, a máquina funcionou satisfatoriamente. Nos dezoito meses seguintes, havia outras 15 bombas em funcionamento. Segundo Singh:

Uma bomba podia encontrar uma chave da Enigma em uma hora. E depois que a disposição dos fios [...] e o ajuste dos misturadores (a chave da mensagem) foram estabelecidos para uma mensagem [...], era fácil deduzir a chave daquele dia. E todas as mensagens enviadas naquele mesmo dia poderiam ser decifradas" (2011, p. 198).

Para detalhamento matemático dos métodos usados por Alan Turing e uma descrição do embasamento teórico por trás das bombas, sugere-se a leitura da série de documentos apelidada de Prof's Book, o Tratado de Turing sobre a Enigma (TURING, 2012).

O esforço de criptoanálise, com a ajuda das bombas, continuava. Bombas chegaram a ser construídas pela Marinha e pelo Exército norte americanos quando a guerra já se aproximava de seu final.

8.2.5 A procura e o uso das informações

As informações obtidas em Bletchley Park eram passadas apenas às mais altas patentes militares e a membros selecionados do gabinete de guerra. O primeiro ministro britânico Winston Churchill chegou a chamar a grande e heterogênea equipe de Bletchley Park de "os gansos que botam ovos de ouro e jamais grasnam" (SINGH, 2011, p. 199-200).

Ao final de 1942, havia 49 bombas em funcionamento em Bletchley Park e arredores. Mais gente foi recrutada para trabalhar no local, algumas através de desafios anônimos de palavras cruzadas de jornal. Mas as diversas redes de máquinas Enigma em funcionamento, como a do Exército alemão no norte da África ou a da Força Aérea, faziam com que o esforço de decifragem não se resumisse ao uso das bombas.

Algumas redes eram mais difíceis de decifrar que outras. A rede da Marinha alemã (*Kriegsmarine*) era a mais difícil de todas, graças às diferenças de projeto e de procedimentos operacionais já discutidas.

O fracasso de Bletchley em decifrar a Enigma naval significava que a *Kriegsmarine* começava a levar vantagem na Batalha do Atlântico. Em uma das estratégias de guerra naval altamente eficiente, que envolvia a localização de um alvo e o posterior ataque coordenado de outros submarinos chamados ao local, era essencial o uso de comunicações seguras. Explica Singh:

A Enigma naval fornecia esse tipo de comunicações e os ataques dos submarinos tiveram um impacto devastador sobre o transporte marítimo aliado, que fornecia à Grã-Bretanha a comida e os armamentos [...]. Enquanto as comunicações com os submarinos permanecessem secretas, os aliados não teriam ideia da localização dos submarinos, não podendo traçar rotas seguras para os comboios (2011, p. 204).

Entre junho de 1940 e junho de 1941, os aliados chegaram a perder em média 50 navios por mês, com imensurável custo humano (50 mil marinheiros aliados morreram durante a guerra). Havia o risco real de os britânicos perderem a Batalha do Atlântico, e com ela, a guerra.

Neste ambiente de ansiedade e medo, o esforço intelectual dos criptoanalistas de Bletchley Park recebeu a ajuda de espionagem, roubo e infiltração, na tentativa de obter as chaves inimigas.

Entre as estratégias usadas, estava a de lançar minas em um local escolhido, obrigando os navios alemães a enviar mensagens de aviso para as outras embarcações. As advertências, cifradas com a Enigma, conteriam um mapa de referência já conhecido pelos britânicos, podendo ser usado como *kisses*. Esse processo era conhecido como *gardening*, mas exigia missões especiais da Força Aérea Real britânica que não podiam ser feitas regularmente (KAHN, 1991, p.144).

Uma operação, chamada *Ruthless* e nunca levada a cabo, chegou a ser pensada em 1940 por Ian Fleming (o escritor que criou o espião James Bond), membro do Serviço Secreto Naval durante a guerra. No plano, um bombardeiro alemão capturado, pilotado por ingleses fingindo ser alemães, faria um pouso de emergência próximo a um navio alemão. Os marinheiros se aproximariam para resgatar os sobreviventes, mas estes entrariam no navio e capturariam os livros de códigos (KAHN, 1991, p. 125-126).

Livros de código alemães acabaram sendo capturados em uma série de ataques a navios meteorológicos e submarinos. Esses “furtos” acabaram dando a Bletchley Park os documentos necessários para acabar com o blecaute de informações de 1940. “Com a Enigma naval transparente, [...] a Batalha do Atlântico começou a mudar em favor dos aliados” (SINGH, 2011, p. 206).

No entanto, se os alemães desconfiassem que suas comunicações não eram mais seguras, as Enigma seriam reforçadas e Bletchley Park estaria de volta ao ponto de partida. Explica Singh:

Como no caso do telegrama Zimmermann, os britânicos tomaram várias precauções para evitar despertar suspeitas, tais como afundar a embarcação alemã depois de roubar seus livros de códigos. Isso faria [...] acreditar que o material cifrado fora para o fundo do oceano e não caíra em mãos aliadas (2011, p. 206).

Depois de capturado, o material secreto era usado estrategicamente. Um súbito aumento no número de ataques certeiros denunciaria a origem dos dados. Em batalhas, os aliados permitiam que alguns submarinos escapassesem, e só atacavam os demais depois que um avião de observação era enviado. Outra estratégia segundo Singh era o envio de “mensagens falsas, descrevendo avistamentos de submarinos que forneciam explicações suficientes para o ataque” (2011, p. 206).

Embora alguns incidentes tenham causado suspeita por parte dos alemães, no geral eles continuaram acreditando que a quebra da Enigma era impossível.

8.2.6 Ultra

Além de decifrar a Enigma, Bletchley Park também teve sucesso com mensagens italianas e japonesas. As informações oriundas dessas três fontes receberam o nome de Ultra, e os dados recolhidos foram responsáveis por dar aos aliados uma vantagem clara.

Um dos criptoanalistas do *hut 6*, Stuart Milner-Barry, certa vez escreveu: “Eu não imagino que já houvesse acontecido uma guerra, desde a era clássica, na qual um dos lados pudesse ler todas as informações militares e navais do outro lado” (SINGH, 2011, p. 207). O conteúdo de muitas mensagens decifradas, no entanto, permanecia secreto e não utilizado para não alertar os inimigos de que o código estava sendo quebrado.

Já o general Alexander, na Tunísia, declarou em 1943: “O conhecimento não só do dispositivo inimigo e do seu efetivo exato, mas também de como, onde e quando ele pretende executar a operação introduziu uma nova dimensão na conduta de guerra” (WINTERBOTHAM, 1978, p. 214).

8.2.7 O fim do segredo

Embora as conquistas de Bletchley Park tenham sido um fator decisivo para a vitória aliada (embora haja controvérsias a respeito) e tenham encortado a guerra de modo significativo, ao longo da guerra os criptoanalistas não recebiam quaisquer detalhes operacionais, nem eram informados de como as mensagens decifradas estavam sendo usadas.

Singh traz o resumo de David Kahn sobre o impacto da quebra da Enigma:

Ela salvou vidas. Não apenas vidas aliadas e russas, ao encurtar a guerra, mas vidas alemãs, italianas e japonesas também. Algumas das pessoas que estavam vivas depois da Segunda Guerra Mundial não teriam sobrevivido se não fossem essas soluções. Esta é a dúvida que o mundo tem para com os quebradores de códigos, este é o valor humano de seus triunfos (2011, p. 209).

Depois da guerra, as conquistas de Bletchley Park permaneceram em segredo, em parte devido ao fato de os britânicos terem distribuído para suas ex-colônias muitas das milhares de máquinas Enigma apreendidas durante a guerra. Eles ainda acreditavam que a cifra era segura, e os britânicos não os avisaram. Pelo contrário, “decifraram, rotineiramente, suas comunicações secretas durante os anos seguintes” (SINGH, 2011, p. 209).

Quando a Escola de Códigos e Cifras de Bletchley Park foi fechada, tornando-se *Government Communications Headquarters* (GCHQ) em Londres em 1946, as bombas foram desmontadas e cada pedaço de papel relacionado com decifrações foi queimado ou trancado em cofres. A grande maioria dos milhares de homens e mulheres que trabalharam no local foram dispensados. Muitos deles voltaram à vida civil, presos a um juramento de sigilo que os impedia de revelar seu papel do esforço de guerra.

O segredo em torno de Bletchley Park terminou em 1974 com o lançamento do livro *The Ultra Secret*, de F. W. Winterbotham. Aqueles que tinham contribuído para o esforço de guerra podiam receber então o reconhecimento merecido. Entre eles, Marian Rejewski, que havia sido “relegado ao trabalho de lidar com cifras rotineiras, numa pequena unidade do serviço de informações” (SINGH, 2011, p. 211).

Singh relata que não ficou claro até hoje porque Rejewski não fora convidado a fazer parte da equipe de criptoanalistas de Bletchley Park, “mas, em consequência disso, ele ignorava completamente as atividades da Escola de Códigos e Cifras do Governo”, não sabendo até a publicação do livro *The Ultra Secret* que “suas ideias tinham fornecido o fundamento para a decifragem rotineira da Enigma durante a guerra” (2011, p. 211).

Entre os que não sobreviveram ao fim do segredo, estão Alastair Denniston, o primeiro diretor de Bletchley Park, e Alan Turing.

No fim das contas, a máquina Enigma, com suas cifras aparentemente perfeitas, e os criptoanalistas, determinados a conseguir quebrá-la como pudessem, disputaram uma

guerra secreta dentro da Segunda Guerra Mundial. Essa guerra estimulou a criação de aparelhos computacionais que viriam a servir como uma das diversas bases da computação moderna.

Infelizmente, muitos dos detalhes sobre os processos e os dispositivos empregados na criptoanálise, tanto os bem sucedidos quanto os rotineiros, permanecem perdidos, alguns ainda como segredo militar, outros à espera de reconstruções históricas como as bombas de Bletchley Park.

O que é seguro dizer é que o conhecimento adquirido graças à máquina Enigma e ao esforço de quebrar sua cifra foram de enorme valor para a Ciência da Computação. Ficou clara a necessidade de poder computacional para suprir o que já era humanamente impossível de ser calculado. Os ancestrais dos computadores puderam evoluir a partir de uma demanda não somente para quebrar cifras, mas para desenvolver novas cifras e decifrá-las, de maneira a manter o sigilo garantido.

9 CONCLUSÃO

Pode-se dizer que durante a Segunda Guerra Mundial houve também uma guerra sendo travada entre a máquina Enigma, com sua cifra extremamente forte para a época, e os criptoanalistas determinados a quebrá-la. Infelizmente, muitos dos detalhes dos processos empregados nessa guerra particular permaneceram – e permanecem – segredo militar.

Se por um lado a máquina Enigma deu uma enorme frente de comunicações seguras aos alemães, por outro a quebra de seu código conseguiu fazer com que a Segunda Guerra Mundial acabasse pelo menos um ano antes.

Inicialmente uma máquina de cifragem com rotores construída por um engenheiro para aplicações comerciais e diplomáticas, a máquina Enigma passou a ser usada principalmente pelas Forças Armadas alemãs antes e durante a Segunda Guerra Mundial como uma alternativa para gerar comunicações sigilosas seguras. Sua entrada no cenário fez com que criptoanalistas do mundo todo chegassem a pensar que finalmente teria sido inventado um método de cifragem inquebrável.

Pelos motivos expostos ao longo deste trabalho, fica claro o trabalho árduo dos criptoanalistas: a decifragem não era definitiva, a quebra do código de um dia não significava que todo o trabalho para dali adiante estava completo. Ou seja, cada dia era um dia. Mesmo assim, eles acabaram provando que mais essa ferramenta, virtualmente invencível, não produzia códigos inquebráveis.

Uma série de fatores ajudou na quebra da máquina Enigma, entre eles o grande volume diário de informações cifradas interceptadas, espionagem, falhas humanas que poderiam ter sido evitadas, falhas de projeto, a aquisição de livros de códigos e outros documentos sigilosos durante incursões militares e a perseverança dos criptoanalistas do *Biuro Szyfrów* e de Bletchley Park.

Mas tudo isso junto não foi suficiente: o grande volume e complexidade dos dados sendo analisados e a impossibilidade humana de testar todas as combinações possíveis para a quebra da cifra fizeram com que a máquina Enigma servisse como elemento motivador para a criação de dispositivos, como as bombas criptológicas e as bombas de Bletchley Park, que podem ser considerados ancestrais dos computadores modernos. Ou seja, mais uma vez a guerra impulsionou a Ciência: neste caso em especial, a máquina Enigma foi responsável por trazer grandes avanços para a Ciência da Computação.

REFERÊNCIAS

- DAY, Colin. **Bletchley Park – Britain's Best-kept WWII Secret.** Disponível em: <http://www.angelfire.com/oz/colinday/bletchley/>. Acesso em: dez. 2012.
- CRYPTO Museum. **Crypto Museum website by Paul Reuvers and Marc Simons.** Disponível em: <http://cryptomuseum.com/mission.htm>. Acesso em: set. 2012.
- CRYPTOOL Project. **CrypTool-Online.** Disponível em: <http://www.cryptool-online.org/>. Acesso em: dez. 2012.
- HAMER, David H. **Enigma cipher machines.** Disponível em: <http://w1tp.com/enigma>. Acesso em: set. 2012.
- KAHN, David. **Seizing the Enigma: Race to Break the German U-Boat Codes, 1939-43.** Houghton Mifflin Harcourt Publishing Company, 1991.
- KRUH, Louis; DEAVOURS, Cipher A. The Commercial Enigma: Beginnings of Machine Cryptography. **Cryptologia**, [S.l.], volume 26, number 1, January 2002. Disponível em: <http://www.dean.usma.edu/math/pubs/cryptologia/ClassicArticleReprints/V26N1PP1-16KruhDeavours.PDF>. Acesso em: nov. 2012.
- MAGALHÃES, Marcelo Vicente Vianna. **Segurança de sistemas.** 2002. Disponível em: http://www.gta.ufrj.br/grad/02_1/seguranca/. Acesso em: dez. 2012.
- MENEZES, Alfred; OORSCHOT, Paul van; VANSTONE, Scott. **Handbook of Applied Cryptography.** Boca Raton, FL: CRC Press, 1997. p. 237-250 e 271-276.
- LEAVITT, David. **O Homem que Sabia Demais:** Alan Turing e a Invenção do Computador. São Paulo: Novo Conceito Editora, 2007.
- MILLER, A. Ray. **The Cryptographic Mathematics of Enigma.** 2001. Disponível em: http://www.nsa.gov/about_files/cryptologic_heritage/publications/wwii/engima_cryptographic_mathematics.pdf. Acesso em: jan. 2013.
- REJEWSKI, Marian. **Breaking the Enigma Cipher.** Applicaciones Mathematicae. 16, No. 4, Warsau 1980. Institute of Mathematics, Polish Academy of Sciences. Disponível em: <http://cryptocellar.web.cern.ch/cryptocellar/Enigma/rew80.pdf>. Acesso em: dez. 2012.
- RIJMENANTS, Dirk. **Cipher Machines and Cryptology.** Disponível em: <http://users.telenet.be/d.rijmenants/index.htm>. Acesso em: set. 2012.
- ROSS, Mike. Mike Koss' Home Page: **Paper Enigma Machine.** Disponível em: <http://mckoss.com/Crypto/Enigma.htm>. Acesso em: set. 2012.

- SCHWAGER, Russel. **Enigma Machine.** Disponível em:
<http://russells.freeshell.org/enigma/>. Acesso em: out. 2012.
- SINGH, Simon. **O livro dos códigos:** A ciência do sigilo – do antigo Egito à criptografia quântica. 9.ed. Rio de Janeiro: Editora Record, 2011.
- SPIESSE, Frank. **Enigma Simulator.** Düsseldorf, Alemanha. Disponível em:
<http://enigmaco.de/enigma/enigma.html>. Acesso em: set. 2012.
- SULLIVAN, Geoff; WEIERUD, Frode. Breaking German Army Ciphers. **Cryptologia**, [S.l.], volume 29, number 3, July 2005, pp. 193-232. Disponível em:
http://www.tandf.co.uk/journals/pdf/papers/ucry_06.pdf. Acesso em: dez. 2012.
- TKOTZ, Viktoria. **Criptografia:** Segredos Embalados para Viagem. 1.ed. São Paulo: Novatec Editora, 2005. p. 246-262.
- TURING, Alan M. **Turing's Treatise on Enigma (The Prof's Book).** Disponível em:
<http://cryptocellar.web.cern.ch/cryptocellar/Turing/index.html>. Acesso em: dez. 2012.
- WIKIPEDIA. **Wikipedia, the free encyclopedia.** Wikimedia Foundation, Inc. Disponível em: <http://en.wikipedia.org/>. Acesso em: set. 2012.
- WINTERBOTHAM, F. W. **Enigma – O segredo de Hitler.** 1.ed. Rio de Janeiro: Biblioteca do Exército - Editora, 1978.

GLOSSÁRIO

Abwehr: Serviço de Inteligência alemão (1921-44). Foi substituído em 1944 pelo *Reichssicherheitshauptamt (RSHA)*. O nome *Abwehr* (Defesa, em alemão) foi dado porque as atividades alemãs de inteligência após a Primeira Guerra Mundial deveriam seguir propósitos defensivos apenas.

Abwehrstellen (Ast): agências de Inteligência locais do *Abwehr*.

Abreviação: forma reduzida da palavra e compreende a redução da palavra até um limite, de modo que não haja prejuízo ao entendimento.

Abreviatura: representação de uma palavra através de suas sílabas.

Almirantado: responsável pela Marinha Real Britânica.

Aktiengesellschaft (AG): Sociedade Anônima (S.A.).

Archery: kisses meteorológicos, nomeados em homenagem a Philip E. Archer.

Äussere Einstellung: configurações externas.

Bamburismo: *bamburismus*, processo criptoanalítico desenvolvido por Alan Turing que usava probabilidade condicional sequencial.

Biuro Szyfrów: Birô de Cifras polonês. Criado em 1919, ficou até 1937 localizado na sede do Estado-Maior Geral polonês em Varsóvia. Foi transferido em 1937 para instalações especialmente construídas perto da aldeia de Pyry, ao sul de Varsóvia.

Bundeswehr: Forças Armadas alemãs, a partir de 1955.

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

Consecutive stecker knock-out (CSKO): termo para o fato de que os alemães não conectavam duas letras consecutivas no painel de plugues das máquinas Enigma.

Crab: passo simultâneo de dois rotoretes.

Crash: quando a mesma letra aparecia na mesma posição em um crib e em um criptograma.

*Crib*s: partes do texto claro que sabidamente correspondem a uma parte do código. Alguns autores traduzem *crib* para cola.

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): 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 semear minas 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.

Notch: entalhe ou chanfro.

Números primos relativos: conjunto de números onde o único divisor comum a todos eles for o número 1, também chamados de números primos entre si ou coprimos.

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 envolvida com uma lingueta que permite que ele se mova em uma única direção.

Reichsbahn: Ferroviária Imperial alemã.

Reichsmarine: Marinha alemã de 1919-35, quando se tornou *Kriegsmarine*.

Reichswehr: Forças Armadas alemãs (1921-35). Passou a ser *Wehrmacht* em 1935.

Reichssicherheitshauptamt (RSHA): Escritório Central de Segurança do Reich, 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: inglês para 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.

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-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). Passou a ser *Bundeswehr* em 1955.

Wetter: tempo, no sentido usado para previsão do tempo. A grafia correta é com W maiúsculo.

Wetterkurzschlüssel: chaves curtas de previsão do tempo.

Zählwerk: contador.

Zusatzwalze: roda adicional.

Zuteilungsliste: lista de alocação.

ANEXO A LEITURAS RECOMENDADAS

Este estudo baseia-se em diversos trabalhos, todos de grande valor. A lista a seguir traz comentadas as principais fontes usadas e outras sugeridas para leitura e aprofundamento no assunto, com uma breve descrição do material.

O Livro dos Códigos, de Simon Singh, é referência obrigatória para qualquer trabalho sobre criptografia e é muito citado por outros autores. O autor mescla aspectos técnicos das principais cifras com sua história.

Criptografia: Segredos Embalados para Viagem, de Viktoria Tkotz traz uma versão condensada do que é mostrado em O Livro dos Códigos. Com uma linguagem leve e tom didático, serve como um primeiro contato do leitor com cifras e a máquina Enigma.

O Homem que Sabia Demais, de David Leavitt é uma biografia breve de Alan Turing, e mostra aspectos interessantes de seus anos de atividade em Betchley Park, quando fez parte do time que ajudou a decifrar a máquina Enigma.

Handbook of Applied Cryptography, de Menezes, Oorschot e Vanstone, é uma leitura técnica sobre o tema. Embora por vezes denso, o texto traz ainda muitas sugestões bibliográficas de trabalhos já feitos sobre o tema.

Enigma – O segredo de Hitler, de F. W. Winterbotham, é a tradução do livro norte-americano The Ultra Secret, e foi publicado em uma coleção lançada pela Biblioteca do Exército brasileiro em 1978. Ele traz jargão militar pesado e pode ser uma leitura difícil para aqueles não acostumados com o estilo detalhista usado. Atenta-se também o fato de o livro omitir o real valor do trabalho dos criptoanalistas do *Biuro Szyfrów* polonês.

Seizing the Enigma, de David Khan, é o livro primordial no estudo do tema, e é a referência indireta mais usada neste trabalho, já que muitas das fontes citadas aqui o citam. Infelizmente, o livro atualmente não está sendo editado no Brasil, e o acesso a ele é difícil.

O Crypto Museum, de Paul Reuvers e de Frode Weierud, é um dos sites mais completos sobre a máquina Enigma disponíveis na internet. Entre os pontos altos estão seu enorme acervo de fotos e de explicações técnicas de funcionamento e uma listagem de patentes, assim como o detalhamento dos diversos modelos da máquina Enigma criados. O site pode ser acessado em <http://www.cryptomuseum.com/>.

O site Cipher Machines and Cryptology, de Dirk Rijmenants, é um dos mais completos sobre o tema, com extenso material e um excelente simulador da máquina Enigma para download. O site pode ser acessado em <http://users.telenet.be/d.rijmenants/index.htm>. Um guia dos complexos procedimentos operacionais necessários para cifrar as

mensagens usados nas diferentes máquinas Enigma na Segunda Guerra Mundial pode ser acessado em <http://users.telenet.be/d.rijmenants/en/enigmaproc.htm>.

O site da Wikipedia é um excelente ponto de partida no estudo da máquina Enigma, oferecendo uma leitura resumida em sua versão em português e uma versão mais completa em inglês. O material em português pode ser acessado principalmente em [http://pt.wikipedia.org/wiki/Enigma_\(m%C3%A1quina\)](http://pt.wikipedia.org/wiki/Enigma_(m%C3%A1quina)), e o material em inglês pode ser acessado, entre outros artigos, em http://en.wikipedia.org/wiki/Enigma_machine e http://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma.

O artigo The Commercial Enigma: Beginnings os Machine Cryptography, de Louis Kruh e Cipher Deavours, foi publicado no periódico Cryptologia, do qual os autores são editores, e traz material sobre as máquinas Enigma de uso comercial. O artigo traz ainda reproduções de material informativo publicado na época e pode ser acessado em <http://www.dean.usma.edu/math/pubs/cryptologia/ClassicArticleReprints/V26N1PP1-16KruhDeavours.PDF>.

O artigo Enigma: Actions Involved in the “Double Stepping” of the Middle Rotor, de David Hamer, descreve o problema de a roda do meio da máquina Enigma girar duplamente quando completa uma rotação completa. O artigo pode ser acessado em <http://home.comcast.net/~dhamer/downloads/rotors1.pdf>.

O artigo An Application of the Theory of Permutations in Breaking the Enigma Cipher, escrito por Marian Rejewski, tem grande valor histórico. Nele, Rejewski descreve como conseguiu quebrar a cifra das primeiras máquinas Enigma. A tradução e a edição (foram mantidos erros estruturais e gramaticais) são de Enrico Grigolon e de Frode Weierud. Disponível em <http://cryptocellar.web.cern.ch/cryptocellar/Enigma/rew80.pdf>.

O Tratado de Alan Turing sobre Enigma (ou The Prof’s Book) é um documento de enorme valor histórico, e foi escrito enquanto Turing trabalhava como criptoanalistas em Bletchley Park. Pode ser acessado em versão não definitiva em <http://cryptocellar.web.cern.ch/cryptocellar/Turing/version.html>.

A versão atualizada do artigo Enigma Variations: An Extended Family of Machines, de David H. Hamer, Geoff Sullivan e Frode Weierud, trata de modelos de máquinas Enigma que haviam sido pouco documentados, trazendo detalhes técnicos e de uso. Disponível em: <http://cryptocellar.web.cern.ch/cryptocellar/pubs/enigvar.pdf>.

O artigo Breaking Army Ciphers, de Geoff Sullivan e Frode Weierud é um relatório sobre um projeto de criptoanálise que busca catalogar e decifrar mensagens de rádio do Exército alemão que permaneceram encriptadas depois da guerra. Disponível em: http://www.tandf.co.uk/journals/pdf/papers/ucry_06.pdf. Acesso em: dez. 2012.

O site CryptoCellar - Cryptology and Its History, de Frode Weierud, traz alguns dos artigos citados acima, entre muitos outros. Além de uma extensa lista de documentos históricos, tem também diversos links sobre o tema. O site está disponível no endereço <http://cryptocellar.org>.

O site oficial de Bletchley Park – National Codes Center oferece material extenso sobre o tema e pode ser acessado em <http://www.bletchleypark.org.uk/content/machines.rhtm>.

O site Enigma Cipher Machines, de David Hamer, tem material extenso sobre os diversos modelos de máquinas Enigma, com centenas de fotos. O site possui ainda peças e máquinas Enigma completas para venda. O site está disponível em <http://w1tp.com/enigma>.

O site Paper Enigma Machine, de Mike Ross, traz explicações sobre o tema e simuladores online e para Android da máquina Enigma. Um dos principais atrativos do site é um simulador da máquina Enigma que pode ser impresso e feito em papel. O site pode ser acessado em <http://mckoss.com/Crypto/Enigma.htm>.

O site CrypTool-Online, do CrypTool Project, traz um interessante diagrama simplificado da máquina Enigma e muito material sobre o tema. O site está disponível no endereço <http://www.cryptool-online.org/>.

ANEXO B CURIOSIDADES, PERGUNTAS E RESPOSTAS

O que é a máquina Enigma?

É uma máquina eletromecânica de criptografia com rotores, utilizada tanto para cifrar como para decifrar mensagens secretas, criada na Alemanha nos anos 1920.

A sua fama vem de ter sido usada pela maior parte das forças militares alemãs a partir de cerca de 1930. A facilidade de uso e a suposta indecifrabilidade do código foram as principais razões para a sua popularidade.

Onde e em que ano foi criada a primeira máquina Enigma?

A primeira máquina Enigma foi construída pela *Gewerkschaft Securitas* em Berlim, Alemanha, em 1923. O uso militar começou com a Marinha, em 1926.

Seus códigos foram decifrados?

O código da máquina Enigma foi decifrado, em diferentes estágios, em um esforço conjunto de, principalmente, poloneses, britânicos e americanos. É aceito hoje que a quebra do código teria sido responsável pela Segunda Guerra Mundial ter terminado pelo menos um ano antes do esperado.

Existe uma máquina Enigma apenas?

Não existe “a” máquina Enigma; na verdade, Enigma é a marca de uma série de mais de 50 modelos diferentes de máquinas de cifragem, desenvolvidas e construídas antes e durante a Segunda Guerra Mundial, que acabaram inspirando outras máquinas de cifragem de rotores criadas em outros países, como a Typex britânica e a SIGABA norte americana.

Mesmo depois da guerra, houve máquinas de cifragem inspiradas no mesmo princípio da Enigma, como a norte americana KL-7, a russa Fialke e a suíça Nema.

Uma curiosidade é que, ao longo dos anos, o logotipo da marca Enigma permaneceu o mesmo, conforme mostrado abaixo.



Figura 2: Logotipo da máquina Enigma (CRYPTO, 2012).

Qualquer máquina Enigma decifrava o que outra máquina Enigma cifrava?

Quase sempre não, com raríssimas exceções. Apenas as máquinas Enigma que fossem do mesmo modelo e estivessem com as mesmas configurações iniciais poderiam decifrar o que foi cifrado. Um exemplo dessa rara compatibilidade pode ser visto no capítulo 5, nas simulações envolvendo a Enigma M4 e a Enigma I.

Como as mensagens eram enviadas e recebidas após a encriptação e a desencriptação?

As mensagens eram enviadas e recebidas por telégrafo ou por rádio usando código Morse.

As máquinas Enigma podiam ser usadas como máquinas de escrever?

Alguns modelos, principalmente os primeiros, sim. Mas a maior parte dos modelos, não.

Como eram os teclados das máquinas Enigma?

O teclado, a entrada de dados de uma máquina Enigma, dependia do modelo. Alguns modelos possuíam teclado em ordem alfabética com adição das letras tremadas Ä, Ö e Ü, outros possuíam formato alemão standard (QWERTZU). Havia também um modelo que cifrava apenas números.

Como era a fonte de alimentação das máquinas Enigma?

Normalmente, elas possuíam baterias internas, mas alguns modelos podiam ser ligados diretamente na tomada de energia.

Como era a saída das mensagens depois de cifradas?

A maior parte das máquinas Enigma mostrava o texto sendo cifrado na forma de lâmpadas que se acendiam próximas a letras em um painel alfabético acima do teclado. Alguns modelos, no entanto, imprimiam o texto de saída diretamente em papel.

E como se cifravam os números?

Normalmente, os operadores das máquinas Enigma eram orientados a escrever por extenso os números. Por exemplo, “2012” seria escrito “dois mil e doze”. Havia também a possibilidade de serem usadas as teclas mais acima do teclado, responsáveis também pelas letras da fileira de cima.

É importante lembrar, no entanto, que nem todas as máquinas Enigma possuíam os números desenhados no painel acima da primeira fileira de letras, e que chegou a existir uma máquina Enigma que possuía apenas números, a Enigma Z.

Nos textos de saída, as palavras sendo cifradas refletiam o tamanho das palavras em texto claro?

Não. As mensagens eram normalmente divididas em grupos de letras: cinco, no caso do Exército e da Força Aérea, e quatro, no caso da Marinha. As mensagens também não podiam ter mais de 250 caracteres.

Ainda existem máquinas Enigma em funcionamento?

Sim, mas para uso pacífico e educacional. Museus ao redor do mundo têm máquinas Enigma em exposição. Em Bletchley Park, por exemplo, existem máquinas Enigma que podem ser manuseadas pelo público.

Há também um bom número de hobbistas que tem máquinas antigas em funcionamento. Alguns chegam a construir suas próprias máquinas. Até hoje são feitos eventos, convenções e reuniões abertas ao público sobre o tema.

Posso comprar uma máquina Enigma?

Pode, mas o preço é altíssimo e é difícil encontrar alguém que queira vender a sua. Um bom lugar para começar a busca é no site de David Hamer (<http://w1tp.com/4sale/>), que tem máquina Enigma completas e peças para venda.

Existe como construir minha própria máquina Enigma?

Sim, e há extenso material sobre como fazer isso na internet. O site model enigma machine (<http://enigmamachine.co.uk/index.html>), por exemplo, mostra todos os passos de construção de uma Enigma.

Existem também kits com o material necessário para a construção de réplicas, como a Enigma E, vendidos em sites que arrecadam fundos para museus, como o de Bletchley Park (http://www.bletchleypark.org.uk/shop/view_product.rhtm/-1/238531/detail.html) e o de Jan Corver Museum (<http://www.jancorver.org/en/price/>).

Uma alternativa mais simples é fazer sua própria máquina Enigma em papel (<http://mckoss.com/Crypto/Enigma.htm>) ou implementar uma em software, como as disponíveis para download em (<http://users.telenet.be/d.rijmenants/en/enigmasim.htm>) e para uso online em (<http://enigmaco.de/enigma/enigma.swf>)

É possível ainda ser criativo e criar máquinas Enigma usando brinquedos de criança (<http://www.youtube.com/watch?v=STRc6xCTAIC>), peças digitais no lugar de rotores (<http://www.youtube.com/watch?v=5EUYbIIqly4>) ou até mesmo rolinhos de papel toalha e fita crepe.

Existem produtos a venda sobre a máquina Enigma?

Sim, e uma listagem de excelentes livros sobre o tema está disponível nas Referências deste trabalho.

É também possível adquirir canecas, camisetas e vários outros produtos com o tema em sites como (<http://www.cafepress.com/ilord>) e Ebay (www.ebay.com).

ANEXO C MODELOS COM MAIS DE UM NOME

Alguns modelos de máquina Enigma possuíam mais de um nome de fato. A tabela abaixo traz os nomes, os designadores oficiais e outras denominações pelas quais alguns modelos passaram a ser chamados.

Tabela 1: Diferentes nomenclaturas de máquinas Enigma

<i>Nome</i>	<i>Designador oficial</i>	<i>Outras denominações</i>
Enigma C	-	<i>Funkschlüssel C</i> (variação da C)
Enigma D	Ch. 8	A26, Enigma Comercial
Enigma <i>Reichswehr D</i> e Enigma I	Ch. 11a e Ch. 11f	Enigma de Serviço, <i>Wehrmacht Enigma</i> , <i>Heeres Enigma</i> , 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, <i>Reichsbahn Enigma</i>
Enigma T	-	Tirpitz, “Tirupitsu”
Enigma II	Ch. 14	Enigma H, H29
Enigma <i>Zählwerk</i>	Ch. 15	Enigma G, <i>Zählwerksmaschine</i> , <i>Abwehr Enigma</i> , A28

Fonte: CRYPTO, 2012.

ANEXO D O TELEGRAMA ZIMMERMANN

O telegrama Zimmermann foi um telegrama codificado despachado pelo ministro do exterior do Império Alemão, Arthur Zimmermann, em 16 de janeiro de 1917, para o embaixador alemão no México, Heinrich von Eckardt, no auge da Primeira Guerra Mundial.

O embaixador era instruído a se aproximar do governo mexicano, com a proposta de formar uma aliança militar contra os Estados Unidos. A proposta prometia ao México terras dos Estados Unidos caso o país aceitasse o acordo.

O telegrama foi interceptado e decodificado por britânicos e seu conteúdo apressou a entrada dos Estados Unidos na Primeira Guerra Mundial (WIKIPEDIA, 2012).

Abaixo, a íntegra traduzida do telegrama, segundo Singh:

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 (2011, p. 128).

O incidente do telegrama Zimmermann foi um dos responsáveis pela busca na Alemanha de novos métodos de criptografia que reforçassem a segurança na comunicação de dados sigilosos. Entre eles, estava a máquina Enigma.

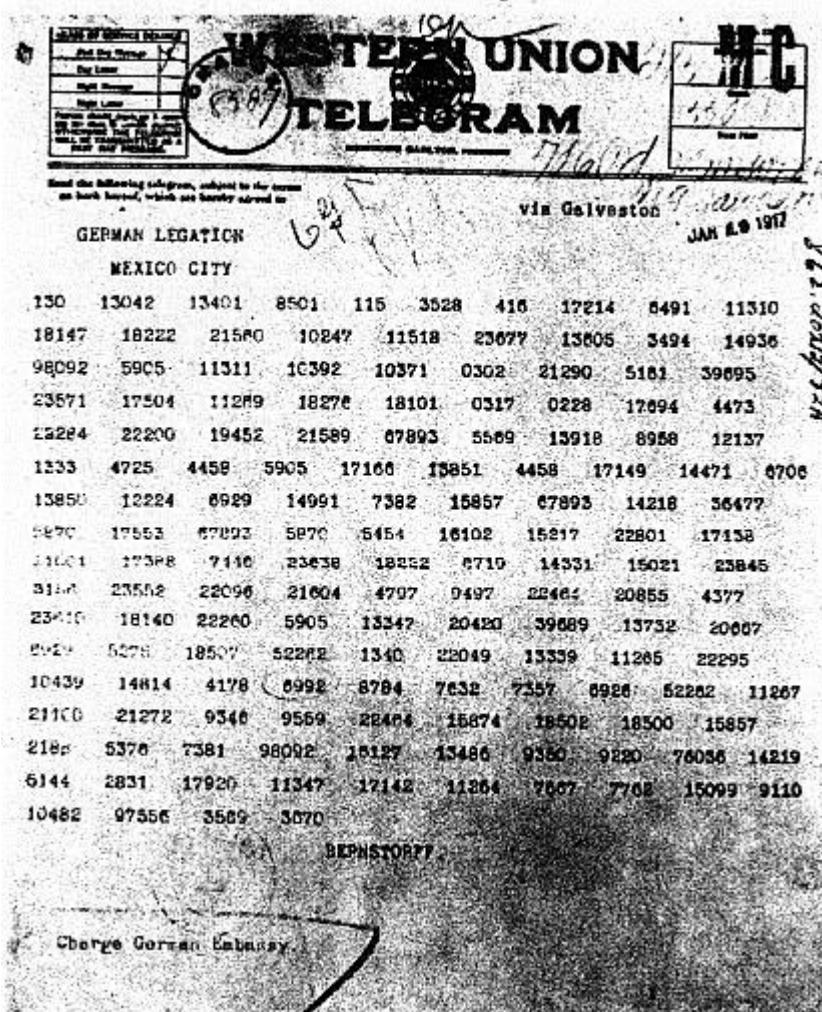


Figura x: Telegrama Zimmermann.