E

Die Enigma ist eine Rotor-Schlüsselmaschine, die im Zweiten Weltkrieg zur Verschlüsselung des Nachrichtenverkehrs der Wehrmacht verwendet wurde. Entschuldigung... o Enigma é uma máquina cifradora com rotores que foi usada durante a Segunda Guerra Mundial para cifrar o tráfego de mensagens das Forças Armadas Alemãs. Ela foi uma grande dor de cabeça para os ingleses e gerou muitas estórias românticas. Existiram diversas versões. Basicamente uma para o Exército, outra para Aeronáutica e uma terceira para a Marinha. Durante a guerra, os ingleses criaram em Bletchley Park a GC&CS (*Government Code and Cypher School*) uma escola com grande capacidade de cripto-análise para decifrar as mensagens. Hoje, em Bletchley funciona um museu muito interessante (www.bletchleypark.org.uk) contando esta estória e ainda tem acervo da história da computação.

A intenção deste apêndice é usar a ideia dessa máquina Enigma para motivar diversos exercícios. Faremos uma breve descrição e proporemos algumas versões. Não é nossa intenção fazer um estudo fiel e aprofundado.

E.1. O Cifrador Enigma

O Enigma trabalha apenas com 26 letras maiúsculas: A, B, C, ..., Z. Não tem caracter de espaço, números ou qualquer outro símbolo. Assim, as mensagens são escritas sem espaço algum. Em alguns casos, usa-se a letra x, que é pouco frequente em alemão, para representar o espaço. A cifragem do Enigma faz a troca entre essas 26 letras. O segredo está na grande possibilidade de trocas.

A Figura E.1 apresenta a foto de uma máquina Enigma em uma de suas últimas versões. Devem ser destacados o teclado e o painel de lâmpadas. São 26 teclas e 26 lâmpadas. Cada tecla, ao ser pressionada, faz acender uma lâmpada indicando a letra para a cifragem. Normalmente, era operado em dupla. Um operador acionava a teclas, de acordo

com a mensagem a ser cifrada, enquanto o outro anotava as letras das lâmpadas que acendiam. Depois, a mensagem era enviada por Código Morse.

O Enigma foi projetado para ser uma máquina simétrica, ou seja, servia tanto para cifrar como para decifrar. Por exemplo, se o mecanismo de cifragem resultava na troca da letra A pela letra T, então:

- ao acionar a tecla A, a lâmpada T acendia e
- ao acionar a tecla T, a lâmpada A acendia.

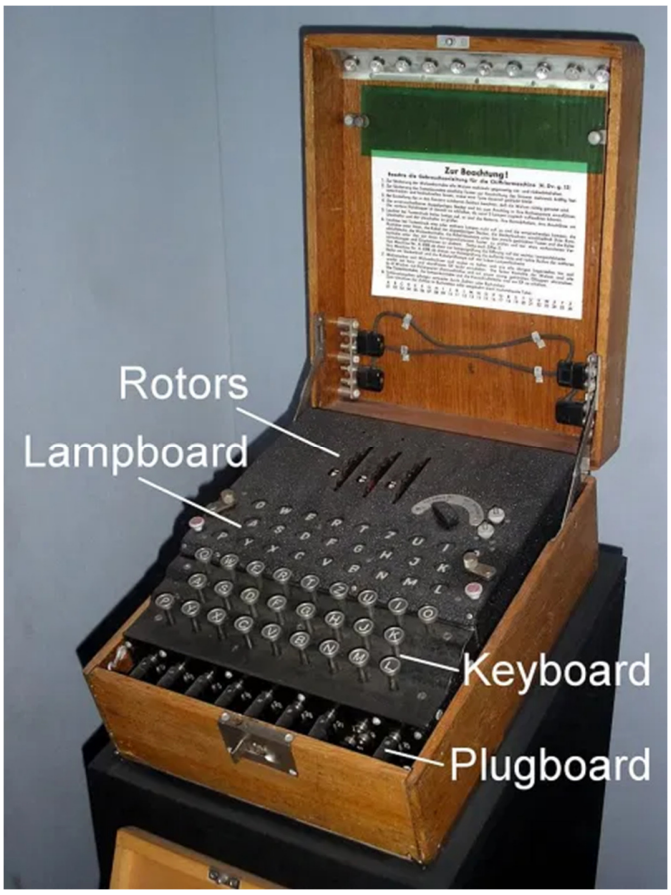


Figura E.1. Máquina Enigma em uma das versões mais sofisticadas.
(Fonte: Wikipedia)

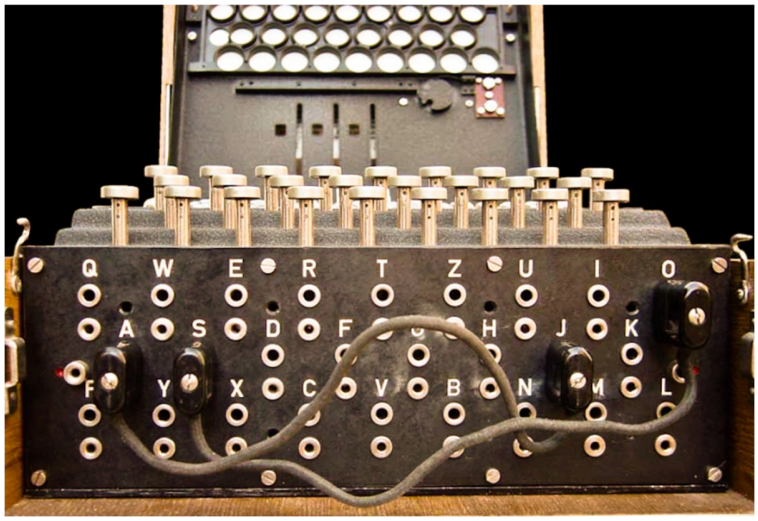
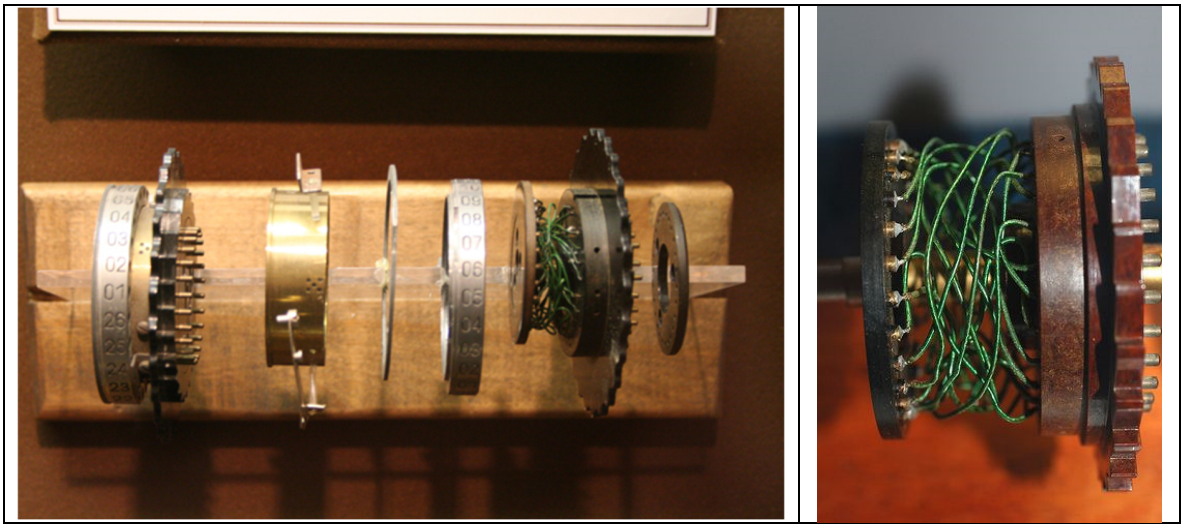


Figura E.2. Detalhe do Plugboard da Máquina Enigma.
(Fonte: https://hackaday.com)

Ainda na Figura E.1, podem-se ver os 3 Rotores. O painel de *plugs* (*Plugboard*) está mostrado em detalhe na Figura E.2. Vamos iniciar abordando os rotores (*Walzen*). Cada rotor é composto por dois anéis com 26 contatos, um para cada letra. A Figura E.3 apresenta à esquerda um rotor desmontado e à direita o detalhe da fiação do rotor. Essa conexão interna (elétrica) entre os 26 contatos é feita por fios, em uma ordem específica e faz o mapeamento de uma letra em uma outra qualquer.



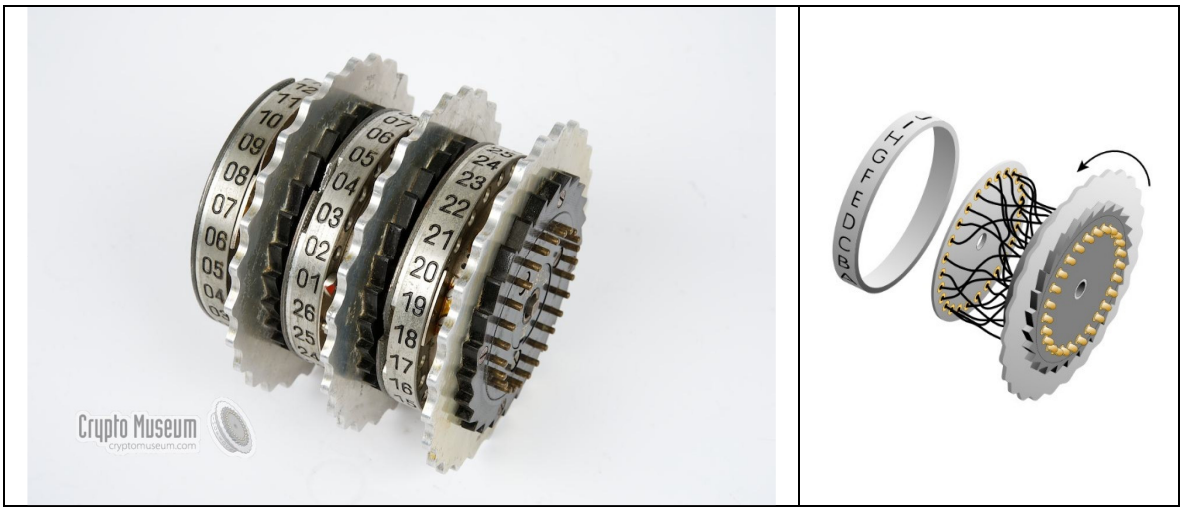


Figura E.3. Detalhe da montagem dos Rotores e à direita, ampliação mostrando a fiação que faz a troca entre as letras.
(Fontes: https://www.nsa.gov/about/cryptologic-heritage/museum e www.cryptomuseum.com)

A Figura E.4 apresenta a ilustração de um rotor. Neste caso, a letra A corresponde à letra G, a letra B à letra E e assim por diante. Os contatos externos dos rotores (os anéis com as letras) podiam ser girados, em relação à fiação interna, fazendo então uma nova correspondência.

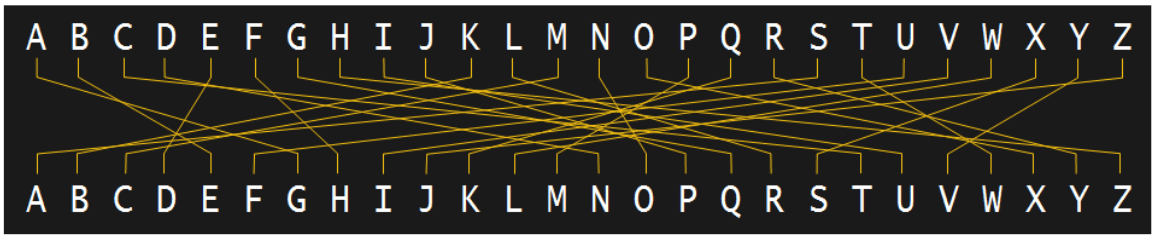


Figura E.4. Ilustração de um rotor e indicando a permuta (troca) entre as 26 letras realizada por uma série de condutores.
(Fonte: hackaday.com/2017/08/22/the-enigma-enigma-how-the-enigma-machine-worked)

E.2. Um Enigma Simplificado

Não é nosso objetivo um estudo da eficiência criptográfica do Enigma. Nosso único interesse é usá-lo como base para propor exercícios. Os autores avisam que são benvindas mensagens indicando erros neste apêndice).

Para um bom entendimento, vamos propor um Enigma mais simples (*die kleine Enigma*). Será uma máquina com apenas 6 letras: A, B, C, D, E e F. Como essas letras conseguiremos desenhar sem grandes dificuldades os principais esquemas. Iniciamos com os rotores.

E.2.1. Rotores Hipotéticos com 6 Letras (*Walzen*)

Para simplificar os esquemas, ao invés de desenharmos os rotores na sua forma circular, vamos representá-los por colunas. Entretanto, o leitor deve imaginar essas colunas ligadas de forma circular. A parte inferior está ligada ao topo.

Os rotores fazem permutas entre as letras. A permuta a ser feita é implementada com a conexão por fios entre os anéis internos, um de cada lado do rotor, como mostrado na Figura E.3. A Figura E.5.a apresenta um rotor simplificado, onde a letra A é trocada pela letra C, a letra B é trocada pela letra E, e assim por diante. Para facilitar a descrição, os dois anéis internos estão numerados. Do lado esquerdo, o rotor possui pontos para contato, indicados por pontos pretos. Do lado direito ele possui pequenas barras (com molas) que chamamos de hastes de contato. Esses contatos e essas hastes vão permitir que se usem diversos rotores, lado a lado.

Para simplificar os esquemas, deste ponto em diante, vamos representar o rotor pelo desenho da Figura E.5.b. Temos uma coluna com as letras e depois duas colunas numeradas indicando a troca realizada. Lembramos que o leitor deve imaginar tudo em forma de anéis. Este rotor pode ser descrito pelo **vetor = [3, 5, 2, 6, 4, 1]**.

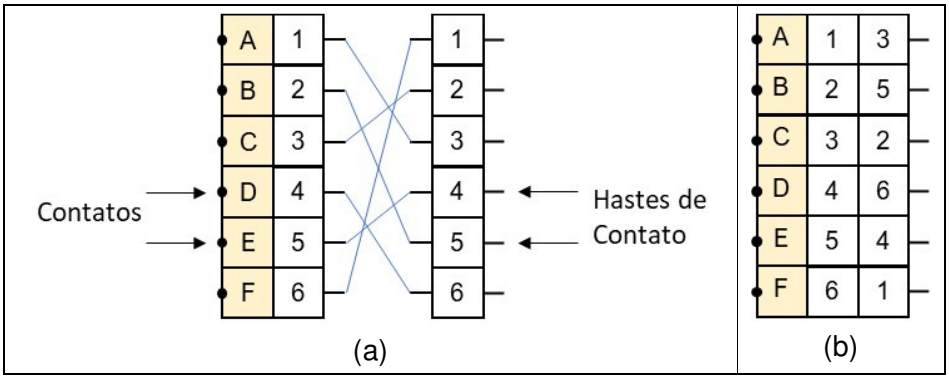


Figura E.5. Proposta de um rotor com apenas 6 letras. Representação deste rotor na forma do vetor = [3, 5, 2, 6, 4, 1].

O rotor oferecia ainda mais uma flexibilidade. O anel com as letras podia ser girado sobre o padrão de contados interno. Isso era chamado de configuração do rotor (*Ringstellung*). A Figura E.6 apresenta 5 das 6 possíveis configurações para um mesmo padrão de

contatos (faltou espaço para a sexta configuração). Vamos sempre tomar como referência a letra que corresponde ao contato 1. Temos então as configurações A (A → 1), B (B → 1) e assim por diante. De acordo com a configuração do rotor, a correspondência entre as letras é alterada. Vejamos os casos da Figura E.6.

- Configuração A: A → C, B → E, C → B, ...
- Configuração B: A → B, B → D, C → F, ...
- Configuração C: A → F, B → C, C → E, ...
- Configuração D: A → C, B → A, C → D, ...
- Configuração E: A → F, B → D, C → B, ...
- Configuração F: A → D, B → A, C → E, ... (não desenhada)

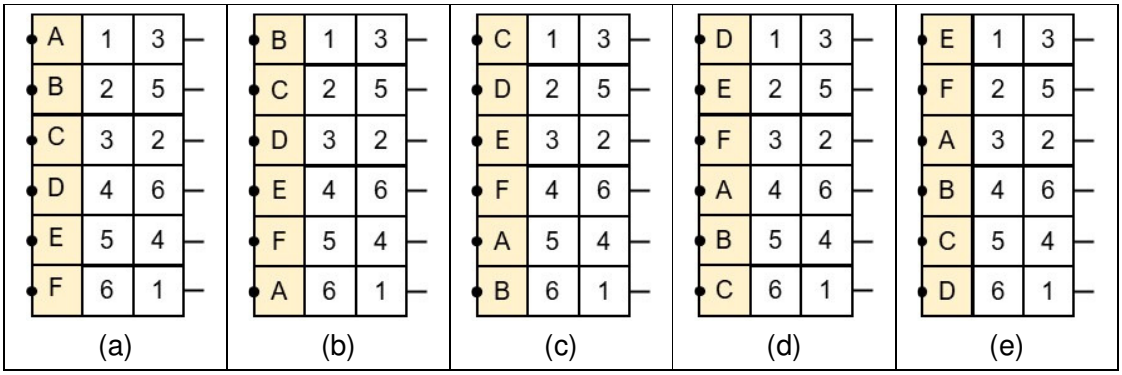


Figura E.6. Algumas possibilidades de configuração dos rotores (Ringstellung).

Na sua forma mais típica, o Enigma dispunha de 5 rotores diferentes, numerados em algarismos romanos, cada um com um distinto padrão de contatos. A cada dia, 3 rotores eram selecionados para serem usados no Enigma. A Figura E.7 apresenta 5 rotores que foram aqui inventados. O padrão dos contatos foi criado no momento desta escrita deste texto, sem qualquer cuidado especial. Por isso, é possível que apresente falhas. O ideal é usar um mecanismo aleatório para gerar o padrão de contatos.

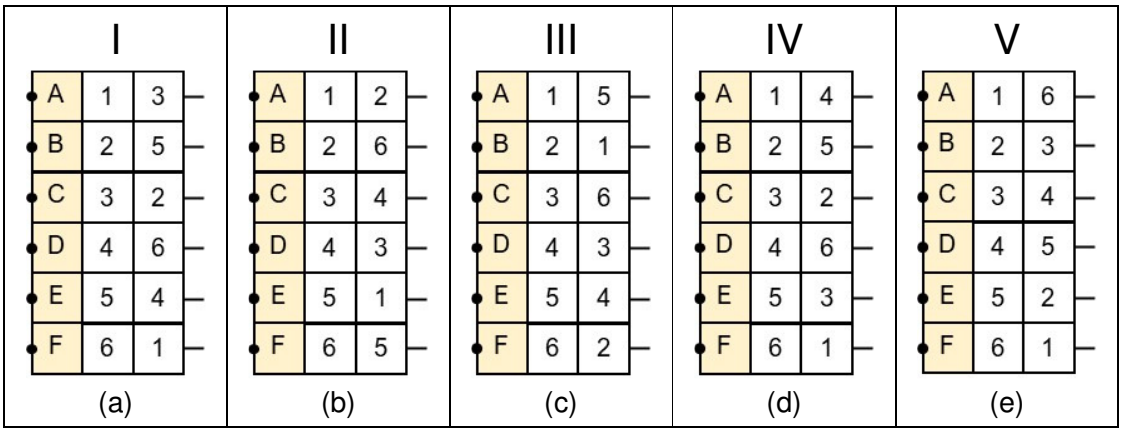


Figura E.7. Sugestão (invenção) de 5 rotores distintos.

Os rotores, ao serem colocados no Enigma, ficam lado a lado. Os vizinhos fazem contato entre os pontos e as hastes, como mostrado na Figura E.8. Temos, então contatos que vão desde o lado esquerdo até o lado direito. Aqui em nosso estudo, para facilitar o raciocínio, estamos organizando os rotores da esquerda para a direita. Temos, então, três permutações em sequência. Abaixo listamos exemplos com as letras A e B.

A → (1,3) → C	C → (3,4) → D	D → (4,3) → C
B → (2,5) → E	E → (5,1) → A	A → (1,5) → E
...	...	...

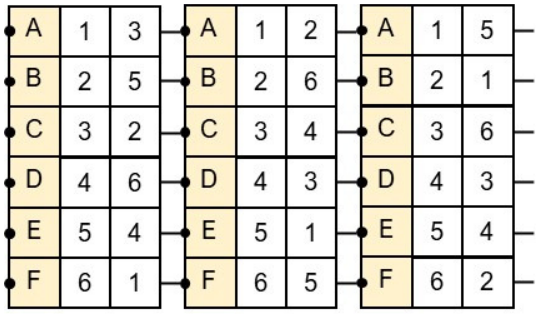


Figura E.8. Ilustração da justaposição dos rotores I, II e III sugeridos na figura anterior. Note que agora há três permutações sucessivas.

É importante lembrar da configuração dos rotores (*Ringstellung*), que permite que o anel de letras gire sobre o padrão de contatos. No exemplo da Figura E.8, todos os rotores estão na configuração A. A Figura E.9 apresenta o caso em que os rotores estão na configuração CBE (a referência é a letra ao lado do número 1). Agora as permutações são diferentes. O leitor é convidado a conferi-las.

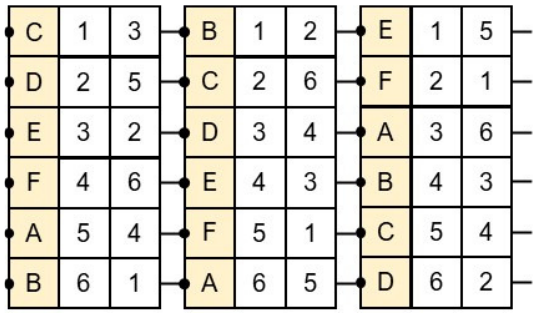


Figura E.9. Ilustração da justaposição dos rotores I, II e III da figura anterior, sendo que os rotores agora estão na configuração (Ringstellung) CBE.

É preciso ainda especificar a posição inicial (*Grundstellung*) dos rotores ao serem colocados no Enigma. Isso amarra a posição relativa entre eles. Foram usadas diferentes formas de especificar esta variável. Aqui neste texto vamos usar a forma mais simples que é a de especificar a letras que aparecem numa janela do Enigma, como mostrado na Figura E.10. Nesta figura, os rotores deveriam ser introduzidos de forma que nas janelas aparecesses as letras E, H e S. Existe um acionamento mecânico que facilita o giro do rotor dentro de seu receptáculo.

Figura E.10. Janelas para indicar a posição inicial (Grundstellung) de cada rotor.

Vamos agora definir (inventar) um método para garantir a posição inicial de cada rotor (*Grundstellung*). Por simplicidade, imaginamos que exista uma janela que mostre, de cada rotor, a letra que correspondente ao terceiro contato do corpo do Enigma (na vertical, de cima para baixo). Usando esta suposição, a posição inicial dos rotores na Figura E.9 é "EDA". A Figura E.11 desenhas as janelas em vermelho para indicar a configuração "EDA" e ainda mostra como seria a colocação dos rotores para a posição inicial "DEC".

1	C	1	3	B	1	2	E	1	5	1	B	6	1	C	2	6	A	3	6
2	D	2	5	C	2	6	F	2	1	2	C	1	3	D	3	4	B	4	3
3	E	3	2	D	3	4	A	3	6	3	D	2	5	E	4	3	C	5	4
4	F	4	6	E	4	3	B	4	3	4	E	3	2	F	5	1	D	6	2
5	A	5	4	F	5	1	C	5	4	5	F	4	6	A	6	5	E	1	5
6	B	6	1	A	6	5	D	6	2	6	A	5	4	B	1	2	F	2	1

(a) Posição inicial “EDA”.	(b) Posição inicial “DEC”.

Figura E.11. Definição das janelas para indicar a posição inicial (Grundstellung) dos rotores I, II e III.

Bem, concluímos que o esquema dos rotores é bem sofisticado. Existe uma falha a ser tratada. Imagine que se descubra que a letra “G” é mapeada na letra “K”. Isso aconteceria em todas as mensagens. Uma análise estatística da frequência das letras no idioma alemão facilitaria a quebra do código. Para resolver isso, a cada tecla digitada, o rotor da extremidade gira (executa um passo). Como são 26 letras no caso original, então, a cada 26 acionamentos do teclado, este rotor dá uma volta completa e força um passo no seu vizinho. Assim, esse giro vai sendo transmitido para os três rotores. Isto significa que a cada letra um novo mapeamento é feito.

Em nosso caso simplificado, vamos considerar que o rotor da esquerda seja o primeiro a girar. Como temos apenas 6 letras, após 6 passos, o rotor vizinho à direita dá um passo. A cada 36 teclas, o rotor mais à direita executa um passo. Não temos claro em que exato instante o rotor do Enigma original girava. São duas possibilidades.

- A tecla, ao ser acionada fazia os contatos e acendia a lâmpada da letra cifrada, sendo que o rotor só girava se essa tecla for acionada até o final ou
- A tecla precisava ser acionada até o final para girar os rotores e só depois fazia os contatos para acender a lâmpada correspondente à cifra.

Como estamos propondo uma máquina simples, vamos adotar a seguinte solução. A máquina faz primeiro a cifragem e depois gira os rotores. Ou seja, a primeira letra é cifrada com a posição inicial (*Grundstellung*) dos três rotores. A Figura E.12 ilustra a cifragem das letras F e D, quando digitadas sequência sendo que a posição inicial é “DEC”. O resultado (se não erramos) é C e F, como mostrado abaixo. Bem esta não é a cifragem final. Estamos ainda na metade do caminho. A próxima etapa é o Refletor.

F → (4,6) → B	C → (2,6) → A	E → (1,5) → C
D → (2,5) → A	A → (6,5) → F	D → (6,2) → F
...	...	...

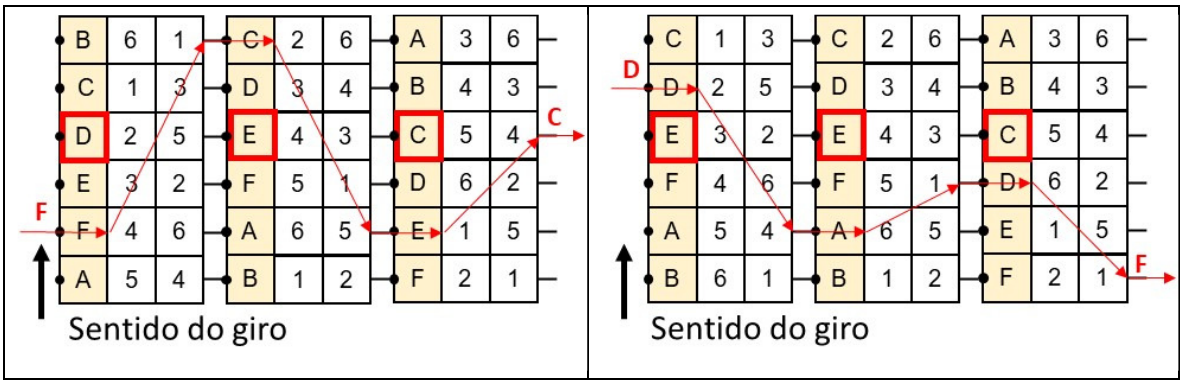


Figura E.12. Exemplo da cifragem das letras F e D, agora considerando a giro do rotor após cada letra cifrada.

Assim, finalmente terminamos a abordagem dos rotores. Imagine tudo isso acontecendo com rotores de 26 letras. Em resumo, temos a seguintes variantes:

- a conexão interna dos rotores;
- a seleção de 3 dos 5 rotores disponíveis;
- configuração *(Ringstellung)* dos 3 rotores selecionados e
- posição inicial (*Grundstellung*) dos 3 rotores dentro do Enigma.

E.2.2. Painel Refletor (*Reflektor*)

O painel refletor (*Reflektor*), como o próprio nome diz, reflete de volta para os rotores, o contato recebido. Ele simplesmente faz um cruzamento entre os contatos do rotor mais à direita, em nosso caso. Com isso, se consegue que a máquina cifradora fique simétrica, ou seja, se a letra F é codificada na letra C, então a letra C é codificada na letra F. De forma simples, se no teclado se aciona letra F, a lâmpada C acende. Por outro lado, se a tecla C é acionada, a lâmpada F acende.

A Figura E.13 apresenta um painel Refletor inventado para o caso do nosso Enigma de 6 letras. Este refletor é descrito pelo **vetor = [4, 6, 5, 1, 2, 3]**. Note que o Refletor devolveu o contato de volta para o rotor mais à direita, e com isso se forma um novo caminho, agora da direita para a esquerda. Nesta figura está ilustrada a cifragem da letra F, que resultou na letra D. Note que no refletor há um caminho ligando as letras F e D. Por esta forma de construção, nunca uma letra pode ser cifrada nela mesma. Esta característica era uma das vulnerabilidades do Enigma. Se a letra cifrada é D, então, tenho a certeza de que a original não é a letra D.

Algumas versões da máquina Enigma permitiam a troca do painel refletor e, como isso, inseriam um maior número de possibilidades.

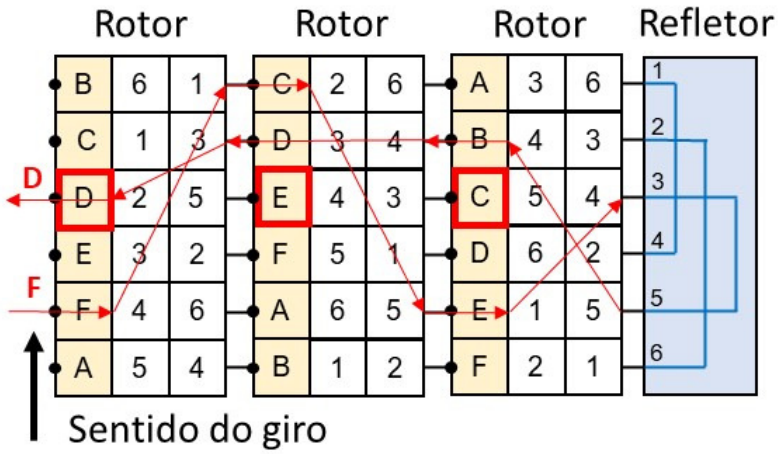


Figura E.13. Exemplo da cifragem da letra F com o uso do Refletor. Note que existe um caminho ligando as letras F e D. Representação deste refletor na forma do vetor = [4, 6, 5, 1, 2, 3].

Vamos agora a uma parte interessante que envolve o teclado e as lâmpadas. Como no exemplo acima, a letra F foi codificada na letra D, então o inverso deve acontecer, ou seja, a letra D deve ser codificada na letra F. Em temos mais simples:

- Tecla F → acende lâmpada D e
- Tecla D → acende lâmpada F

A Figura E.14 ilustra a conexão entre as lâmpadas e o teclado. As lâmpadas têm um terminal ligado à terra e o outro à sua tecla. Uma determinada tecla, quando solta, ela faz contato com sua lâmpada. Por outro lado, quando acionada, a tecla desfaz o contato com sua lâmpada e faz contato com a tensão da bateria. Assim, a tecla D acende a lâmpada F e vice-versa. É importante notar que os rotores e o refletor apenas construíram um "caminho elétrico" entre as letras F e D.

Por esse esquema, é óbvio que uma tecla numa será cifrada nela mesma. Bem, ainda não acabou a descrição, falta ainda o painel de *plugs*.

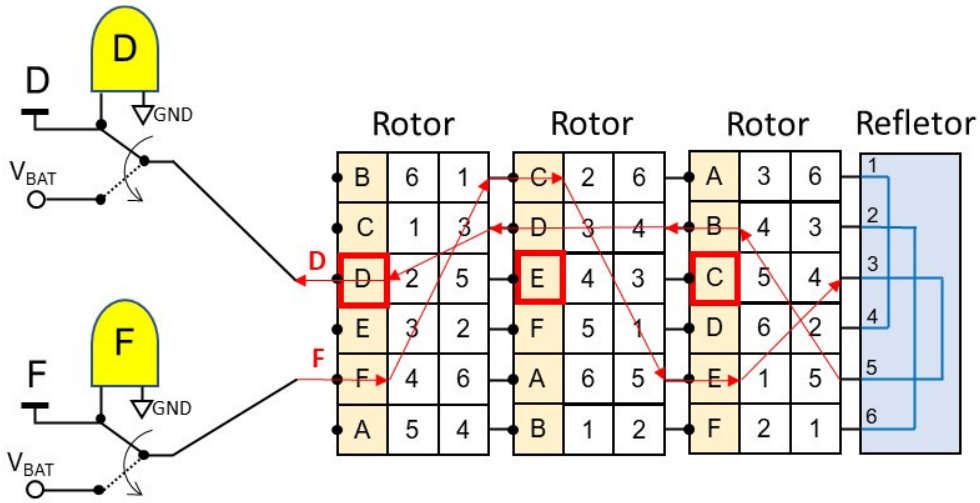


Figura E.14. Esquema para permitir a simetria no Enigma. A tecla F, quando acionada, acende a lâmpada D. Por sua vez, a tecla D acende a lâmpada F.

E.2.3. Painel de Plugs (*Steckerbrett*)

O painel de plugs é colocado entre o teclado e o primeiro rotor. Seu funcionamento é simples e apenas faz a troca entre duas letras. A Figura E.15 apresenta um exemplo para nosso Enigma simplificado para 6 letras.

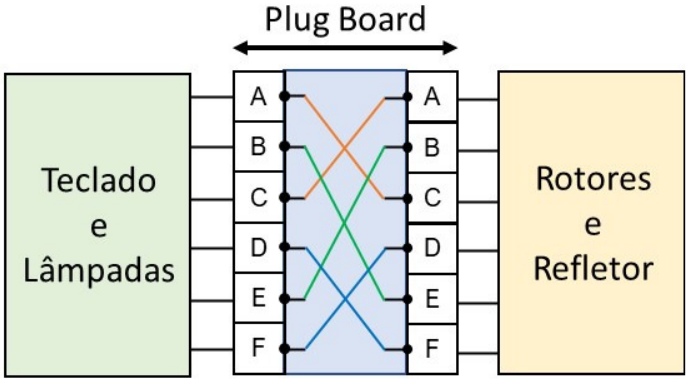


Figura E.15. Ilustração de um painel de plugs simplificado, a conexão feita realiza a troca entre as letras A↔C, B↔E e D↔F.

Na Figura E.2 se pode ver uma foto do painel de plugs. Nesta figura, note que existem dois cabos conectados. É um pouco difícil de ver, mas eles fazem a troca das letras A↔J e S↔O. Na Figura E.1, observe que na tampa da caixa do Enigma ainda existem dois cabos presos.

Como ilustrado na Figura E.16, esses cabos eram geminados e tinham dois contatos em cada extremidade, com diâmetros diferentes, para evitar conexão trocada. É preciso imaginar essa máquina era usada durante o combate. As informações coletadas indicam que havia o costume de se usar até 10 cabos, ou seja, 10 trocas de letras, o que deixa apenas 6 letras intactas.

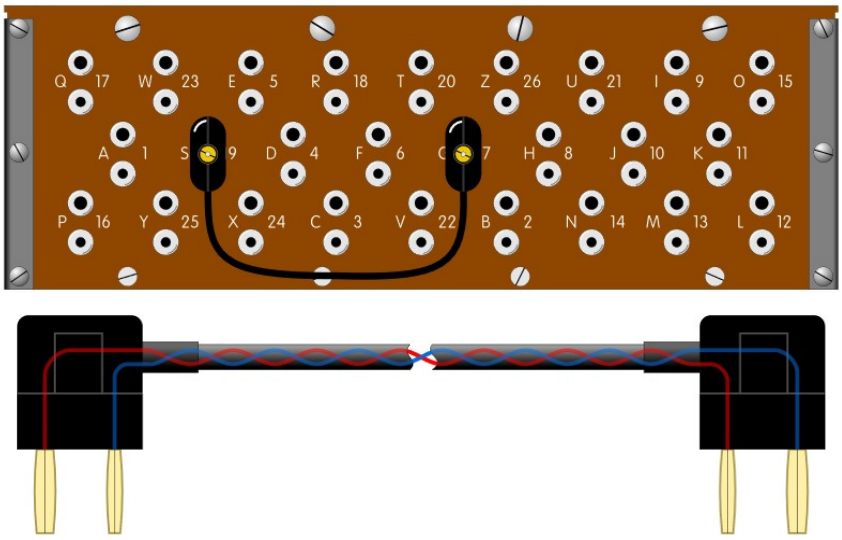


Figura E.16. Desenho de um Painel de Plugs e representação de um cabo de conexão. Note os contatos com diâmetros diferentes.
(fonte: https://www.cryptomuseum.com/crypto/enigma/i/sb.htm)

E.2.4. Esquema Completo

Finalmente, a Figura E.17 apresenta o esquema completo de nosso hipotético Enigma com apenas 6 letras. Nesta figura, o teclado e as lâmpadas estão representados de forma muito simplista. A conexão detalhada está na Figura E.14.

De forma simples, quando uma tecla é acionada, forma-se um caminho elétrico que sai da tecla, passa pelo painel de plugs, percorre os três rotores, é devolvido pelo refletor, percorre novamente os três rotores, volta para o painel de plugs e chega até uma das lâmpadas.

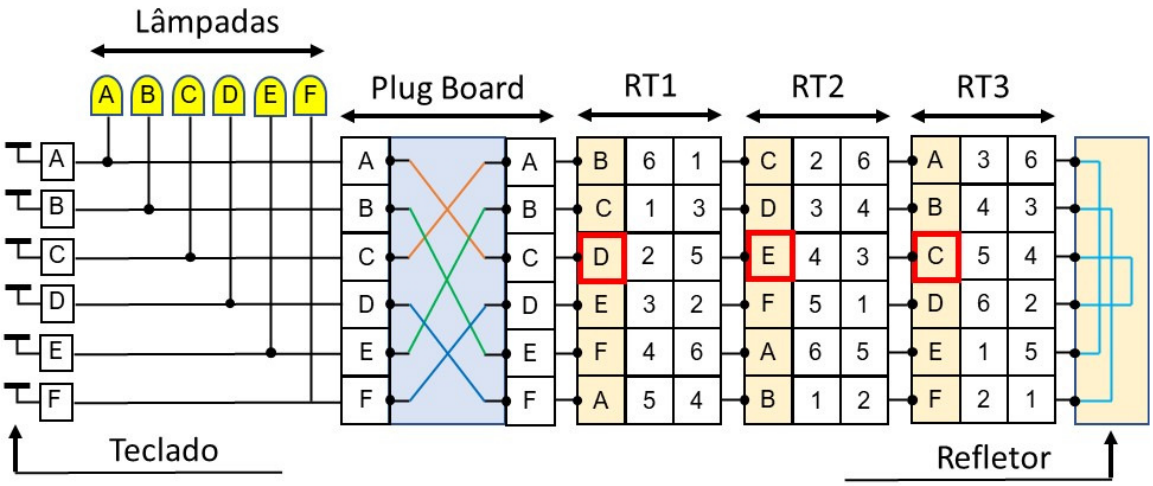


*Figura E.17. Ilustração do **Kleine Enigma** que cifra um alfabeto de apenas 6 letras.*

Para que o Enigma pudesse ser usado, era preciso combinar antecipadamente toda a configuração. Os alemães trocavam essa configuração a cada 24 horas. Usualmente a troca era feita à meia-noite. Os cadernos com as configurações eram impressos mensalmente. A Figura E.18 apresenta a foto de uma tabela com as configurações usadas pela aeronáutica (Luftwaffe). Essa tabela possui 6 colunas:
1) Dia do mês (*Monat Tag*);
2) Ordem dos rotores selecionados (*Walzenlage*);
3) Configuração dos rotores (*Ringstellung*);
4) Refletor (*Reflektor*)
5) Painel de Plugs (*Steckerbrett*)
6) Grupos de teste? (*Kennengruppen*)


Geheime Kommandosache! Jede einzelne Tagesschlüssel ist geheim. Mitnehmen im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

Monats-tag	Walzenlage	Ringstellung	Steuerverbindungen an der Umkehrwalze	Steuerverbindungen am Steckerbrett	Kenngruppen	
649 31	I V III	14 09 24		SZ GT DV KU FO MY EW JN IX LQ	wny dgy	ekb rzg
649 30	IV III II	05 26 02		IS EV MX RW DT UZ JQ AO CH NY	ktl acw	zsi wao
649 29	III II I	12 24 03	KM AX PZ GO	DJ AT CV IO ER QS LW PZ FN BH	ioc acn	ovw wvd
649 28	II III V	06 08 16	DI CN BR PV	CR FV AI DK OT MQ EU BX LP GJ	lrb cld	ude rzh
649 27	III I IV	11 03 07	LT EQ HS UW	DY IN BV GR AM LO PP HT EX UW	woj fbh	vct uis
649 26	I IV V	17 22 19		VZ AL RT KO CG EI BJ DU FS HP	xle gbo	uev rxm
				OR PV AD IT PK HJ LZ NS EQ CW	ouc uhq	uew uit

Figura E.18. Foto de uma tabela de configuração do Enigma usado pela Força Aérea Alemão, a Luftwaffe. (https://hackaday.com)

E.3. Decifrar o Enigma?

Após estudarmos este Enigma simplificado, temos uma boa ideia de seu funcionamento. Os leitores devem estar curiosos sobre a quantidade de combinações possíveis. Esse cálculo é um bom exercício de análise combinacional. Deixamos para uma noite de insônia.

O vídeo da *Numberphile* (https://www.numberphile.com/) disponível no Youtube em (https://www.youtube.com/watch?v=G2_Q9FoD-oQ) é bastante interessante. Está legendado e apresenta com detalhes o cálculo da quantidade de possibilidades. O resultado apresentado é: 158.962.555.217.826.360.000 ou, aproximadamente, **$1,5 \times 10^{20}$**.

Problema: Você tem um computador extremamente rápido, capaz de checar 10^9 possibilidades por segundo. Quanto tempo você gastaria, no pior caso, para quebrar uma mensagem do Enigma?

Se você resolveu o problema acima, deve ter obtido um número proibitivo. Concluímos então que a força bruta não resolve. Como será que os ingleses quebravam o código das mensagens alemãs. Conta a estória que cada dia, à meia-noite iniciavam a interceptação das mensagens e começavam as tentativas. Depois de 24 horas, tendo conseguido ou não conseguido quebrar o código, tudo começava de novo, pois a configuração era trocada. Aí tem muita estória romanceada e a grande maioria passa por Bletchley. É interessante buscá-las na Internet e temos agora sugestão para uma segunda noite insone.

O Enigma tinha uma vulnerabilidade básica. Uma letra nunca era trocada por ela mesma. Uma das estórias conta que foi interceptada uma mensagem que não continha a letra U (se não me engano). A conclusão foi de que o operador, talvez para fazer um teste, teclou diversas vezes a letra U e depois transmitiu a mensagem cifrada. Essa foi fácil, conheciam a mensagem em claro e a mensagem cifrada. Durante aquele dia, decifraram todas as transmissões.

Também acontecia de capturarem um livro de códigos e, até que os alemães descobrissem, conseguiam decifrar várias mensagens. O trabalho com livros de códigos e mensagens antigas, permitia descobrir a configuração interna dos rotores e os tipos usados.

Uma outra vulnerabilidade estava no operador. Algumas vezes conseguiam identificar da pessoa que estava operando e transmitindo as mensagens. Essas mensagens eram enviadas por Código Morse. Quem trabalha com Código Morse não conta os traços e pontos e sim, acostuma-se a identificar o "som" de cada letra. Todo operador de transmissor, sempre tem um certo cacoete, como se fosse um sotaque em Morse. Assim, depois de algum tempo, os ingleses começaram a identificar determinados operadores e passaram a conhecer suas manias. Alguns sempre começavam suas mensagens por um bom dia (*Gutten Tag*). Conhecendo isso, já tinham as primeiras letras da mensagem e

começavam a tentar descobrir quais rotores foram usados e qual sua posição original. A letra “G”, de *Gutten*, é cifrada, talvez, sem o primeiro giro do rotor, o que reduz bastante a quantidade de possibilidades. Depois, a letra U, era cifrada só com um giro.

Foram construídas máquinas automáticas para testar possibilidades de cifragens. As primeiras eram chamadas de Bombs e se chegou até o Colossus que é tido como primeiro computador eletrônico programável, contrariando o que os americanos afirmam sobre o ENIAC. Vide Figura E.19.

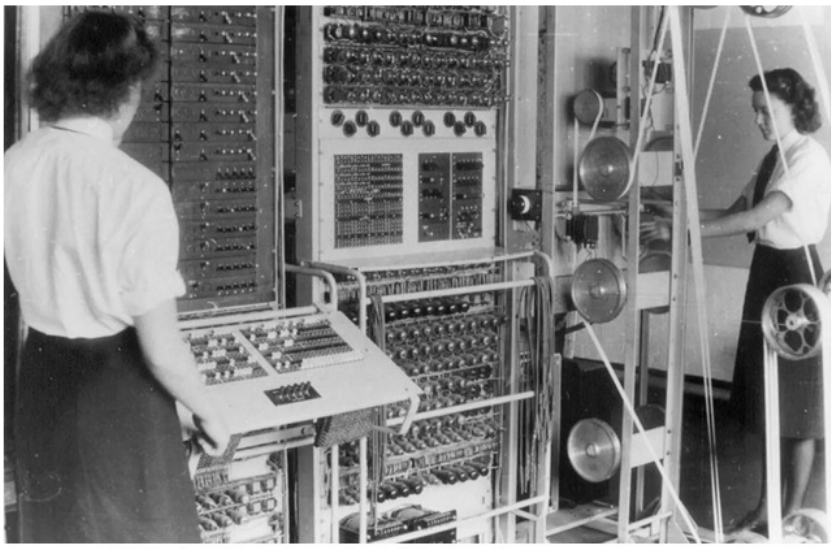


Figura E.19. Foto do computador Colossus.
(Fonte: https://www.telegraph.co.uk/technology/connecting-britain/colossus-bletchley-computer-broke-hitler-codes/)

E.4. Simuladores do Enigma

Na Internet existe a disponibilidade de vários simuladores. Listamos alguns deles. Ainda não tivemos tempo de testá-los. O leitor que o fizer, por favor envie seus comentários.

1) https://www.101computing.net/enigma-machine-emulator/ (on-line)

2) https://play.google.com/store/apps/details?id=uk.co.franklinheath.enigmasim&hl=pt_BR

3) https://www.enigmaworldcodegroup.com/download-enigma-simulator

4) http://users.telenet.be/d.rijmenants/en/enigmasim.htm

5) https://cryptii.com/pipes/enigma-machine

E.5. Propostas de Versões do Enigma para Exercícios

Aqui neste tópico vamos inventar algumas versões simplificadas do Enigma, com a intenção de usá-las em exercícios. A listagem mais adiante apresenta o *script* Matlab "**Enigma.m**" usado para gerar as tabelas dos rotores e dos refletores.

Este *script* apenas pergunta pela quantidade de letras e sorteia as conexões para 5 rotores e 3 refletores. Estas quantidades de rotores e refletores podem ser facilmente alteradas no corpo do *script*. Logo no início, o script usa o comando `rng(1)` para inicializar o gerador aleatório do Matlab e assim sempre gerar os mesmos padrões. O leitor pode alterar essa linha para gerar novas sequências.

Além de imprimir o resultado na área de trabalho do Matlab, o *script* "**Enigma.m**" gera um arquivo de texto para facilitar a declaração dos rotores e refletores em *assembly* e em C. Ao final, ainda apresenta um texto que pode ser usado para criar uma planilha no formato ".csv". Veja um exemplo deste arquivo logo após listagem do *script*. O arquivo é nomeado como "Enigma_xx.txt", onde xx é um número. O *script* sempre procura por um número (xxx) não usado.

E.4.1. Rotores Propostos

Vamos criar 3 tipos de rotores e refletores, cada tipo de rotor tem 5 versões e cada tipo de refletor também tem 5 versões.
Tipo 1: com as 6 primeiras letras do alfabeto (A, B, C, D, E, F);
Tipo 2: com os 8 dígitos para numeração octal (0, 1, 2, ..., 7);
Tipo 3: com os 10 dígitos para numeração decimal (0, 1, 2, ..., 9);
Tipo 4: com os 16 dígitos para numeração hexadecimal (0, 1, 2, ..., 9, A, ..., F);
Tipo 5: com as 26 letras do alfabeto (A, B, ..., Z).

Tabela E.1. Rotores e refletores do tipo 1 (Enigma_01.txt)

Letras	Ordem	Rotores					Refletores		
		I	II	II	IV	V	I	II	III
A	01	03	01	02	05	01	04	05	04
B	02	05	05	05	02	04	05	06	03
C	03	01	03	06	06	05	06	04	02
D	04	02	04	01	01	03	01	03	01

E	05	04	02	03	03	06	02	01	06
F	06	06	06	04	04	02	03	02	05

Tabela E.2. Rotores e refletores do tipo 2 (Enigma_02.txt)

Letras	**Ordem**	**Rotores**					**Refletores**		
		I	**II**	**II**	**IV**	**V**	**I**	**II**	**III**
0	01	04	08	01	02	07	03	08	02
1	02	06	03	07	05	06	06	05	01
2	03	01	06	08	06	08	01	04	04
3	04	03	01	06	01	05	07	03	03
4	05	02	02	03	04	03	08	02	07
5	06	05	04	04	08	04	02	07	08
6	07	08	05	02	07	01	04	06	05
7	08	07	07	05	03	02	05	01	06

Tabela E.3. Rotores e refletores do tipo 3 (Enigma_03.txt)

Letras	**Ordem**	**Rotores**					**Refletores**		
		I	**II**	**II**	**IV**	**V**	**I**	**II**	**III**
0	01	05	04	08	02	07	02	04	02
1	02	08	07	02	10	04	01	06	01
2	03	01	09	05	04	06	08	07	08
3	04	04	01	10	08	09	10	01	10
4	05	02	02	03	09	10	06	10	09
5	06	06	05	01	07	01	05	02	07
6	07	07	10	07	03	02	09	03	06
7	08	03	06	06	05	08	03	09	03
8	09	09	08	09	06	03	07	08	05
9	10	10	03	04	01	05	04	05	04

Tabela E.4. Rotores e refletores do tipo 4 (Enigma_04.txt)

Letras	**Ordem**	**Rotores**					**Refletores**		
		I	**II**	**II**	**IV**	**V**	**I**	**II**	**III**

0	01	07	03	09	05	03	11	13	08
1	02	12	10	14	02	13	07	11	07
2	03	01	12	02	12	06	16	15	14
3	04	05	02	05	13	16	05	07	05
4	05	03	07	10	15	10	04	08	04
5	06	02	01	16	01	15	08	14	11
6	07	06	09	01	04	14	02	04	02
7	08	09	11	13	10	08	06	05	01
8	09	11	16	04	16	09	15	16	12
9	10	04	15	07	09	05	12	12	15
A	11	15	13	12	11	01	01	02	06
B	12	13	06	03	07	07	10	10	09
C	13	16	05	08	08	11	14	01	16
D	14	14	08	06	03	12	13	06	03
E	15	08	04	11	14	04	09	03	10
F	16	10	14	15	06	02	03	09	13

Tabela E.5. Rotores e refletores do tipo 5 (Enigma_05.txt)

Letras	**Ordem**	**Rotores**					**Refletores**		
		I	**II**	**II**	**IV**	**V**	**I**	**II**	**III**
A	01	11	20	17	26	14	08	03	23
B	02	19	10	22	05	06	18	14	06
C	03	01	08	05	22	21	06	01	10
D	04	08	24	01	23	08	20	09	13
E	05	04	12	02	18	01	16	11	15
F	06	03	26	13	15	16	03	20	02
G	07	05	18	16	13	22	10	24	14
H	08	09	17	15	09	10	01	15	11
I	09	15	03	09	06	20	15	04	24
J	10	18	25	26	16	15	07	23	03
K	11	06	16	10	24	25	19	05	08
L	12	23	11	20	07	19	17	21	22
M	13	21	07	18	03	13	26	26	04

N	14	26	15	07	19	07	24	02	07
O	15	24	01	06	11	03	09	08	05
P	16	02	09	21	17	12	05	18	25
Q	17	25	14	14	14	17	12	22	18
R	18	14	05	25	04	09	02	16	17
S	19	22	04	24	20	04	11	25	20
T	20	20	19	11	21	02	04	06	19
U	21	12	02	04	01	11	23	12	26
V	22	07	23	23	25	24	25	17	12
W	23	13	22	12	12	05	21	10	01
X	24	16	21	08	08	26	14	07	09
Y	25	10	06	19	10	23	22	19	16
Z	26	17	13	03	02	18	13	13	21

Tabela E.6. Configuração de rotores usados pela Marinha Alemã (Kriegsmarine). Não foi possível localizar o Painel Refletor.
(https://www.cryptomuseum.com/crypto/enigma/m3/index.htm)

Letras	**Ordem**	**Rotores**				
		I	**II**	**II**	**IV**	**V**
A	01	05	01	02	05	22
B	02	11	10	04	19	26
C	03	13	04	06	15	02
D	04	06	11	08	22	18
E	05	12	19	10	16	07
F	06	07	09	12	26	09
G	07	04	18	03	10	20
H	08	17	21	16	01	25
I	09	22	24	18	25	21
J	10	26	02	20	17	16
K	11	14	12	24	21	19
L	12	20	08	22	09	04
M	13	15	23	26	18	14
N	14	23	20	14	08	08

O	15	25	13	25	24	12
P	16	08	03	05	12	24
Q	17	24	17	09	14	01
R	18	21	07	23	06	23
S	19	19	26	07	20	13
T	20	16	14	01	07	10
U	21	01	16	11	11	17
V	22	09	25	13	04	15
W	23	02	06	21	03	06
X	24	18	22	19	13	05
Y	25	03	15	17	23	03
Z	26	10	05	15	02	11

Listagem de um script Matlab para facilitar a criação de Rotores e Refletores.

```
% Enigma
% Gerar cruzamento para e refletores

rng(1);     % Inicializar gerador
qtd_rotor=5;    %5 Rotores
qtd_reflet=3;   %3 Refletores

p=input('Quantidade (par) de posições do rotor ? ');
p = 2*floor(p/2);   %Garantir p = par, arredonda para baixo

% Sortear Rotores
rt=zeros(qtd_rotor,p);
for lin=1:qtd_rotor
    base=ones(1,p); %Marcar os sorteados
    for col=1:p
        x=floor(1+p*rand);
        while base(1,x) == 0
            x=floor(1+p*rand);
        end
        base(1,x)=0;
        rt(lin,col)=x;
```

```
    end
end

% Sortear Refletores
rf=zeros(qtd_reflet,p);
for lin=1:qtd_reflet
    base=ones(1,p); %Marcar os sorteados
    for col=1:p/2
        x1=floor(1+p*rand);
        while base(1,x1) == 0
            x1=floor(1+p*rand);
        end
        base(1,x1)=0;
        %
        x2=floor(1+p*rand);
        while base(1,x2) == 0
            x2=floor(1+p*rand);
        end
        base(1,x2)=0;
        rf(lin,x1)=x2;
        rf(lin,x2)=x1;
    end
end

for lin=1:qtd_rotor
    fprintf(1,'\nRotor %d: ',lin);
    for col=1:p
        fprintf(1,'%02d ',rt(lin,col));
    end

end

for lin=1:qtd_reflet
    fprintf(1,'\nRefletor %d: ',lin-1);
    for col=1:p
        fprintf(1,'%02d ',rf(lin,col));
    end
end

% Gerar arquivo txt para facilitar inserir em programas

% Escolher um arquivo ainda não usado
fp=1;
ct=0;
while fp > 0
    ct = ct + 1;
    nome=sprintf('Enigma_%02d.txt',ct);
    fp=fopen(nome,'r');
    if fp>0
        fclose(fp);
```

```
    end
end
fp=fopen(nome,'w');

if fp < 0;
    fprintf(1,'\n\nRRO.\n');
    fprintf(1,'Não conseguiu criar o arquivo [%s].',nome);
    exit;
end

fprintf(1,'\n\nCriado o arquivo [%s].',nome);

fprintf(fp,nome);
fprintf(fp,'\n\n');

% ASM
fprintf(fp,'------ ASM ------\n\n');
fprintf(fp,'RT_QTD:\t.equ\t%02d\t\t;Quantidade de Rotores\n',qtd_rotor);
fprintf(fp,'RF_QTD:\t.equ\t%02d\t\t;Quantidade                          de
Refletores\n',qtd_reflet);

fprintf(fp,'\n;Rotores com %d posições\n',p);
for lin=1:qtd_rotor
    fprintf(fp,'RT%d:\t.byte\t',lin);
    for col=1:p-1
        fprintf(fp,'%02d, ',rt(lin,col));
    end
    fprintf(fp,'%02d\n',rt(lin,col+1));
end

fprintf(fp,'\n;Refletores com %d posições\n',p);
for lin=1:qtd_reflet
    fprintf(fp,'RF%d:\t.byte\t',lin);
    for col=1:p-1
        fprintf(fp,'%02d, ',rf(lin,col));
    end
    fprintf(fp,'%02d\n',rf(lin,col+1));
end

% C
fprintf(fp,'\n\n------ C ------\n\n');
fprintf(fp,'#define RT_QTD\t%d\t\t//Quantidade de Rotores\n',qtd_rotor);
fprintf(fp,'#define             RF_QTD\t%d\t\t//Quantidade             de
Refletores\n',qtd_reflet);

fprintf(fp,'\n//Rotores com %d posições\n',p);
for lin=1:qtd_rotor
    fprintf(fp,'rt%d[] = {',lin);
    for col=1:p-1
        fprintf(fp,'%d, ',rt(lin,col));
```

```
    end
    fprintf(fp,'%d};\n',rt(lin,col+1));
end

fprintf(fp,'\n//Refletores com %d posições\n',p);
for lin=1:qtd_reflet
    fprintf(fp,'rf%d[] = {',lin);
    for col=1:p-1
        fprintf(fp,'%d, ',rf(lin,col));
    end
    fprintf(fp,'%d};\n',rf(lin,col+1));
end

fprintf(fp,'\n//Matriz [%d,%d] com todos os Rotores\n',qtd_rotor,p);
fprintf(fp,'rt_mat[] = {\n');
for lin=1:qtd_rotor
    fprintf(fp,'\t\t{',lin);
    for col=1:p-1
        fprintf(fp,'%d, ',rt(lin,col));
    end
    fprintf(fp,'%d}\n',rt(lin,col+1));
end
fprintf(fp,' };\n');

fprintf(fp,'\n//Matriz [%d,%d] com todos os Refletores\n',qtd_reflet,p);
fprintf(fp,'rf_mat[] = {\n');
for lin=1:qtd_reflet
    fprintf(fp,'\t\t{',lin);
    for col=1:p-1
        fprintf(fp,'%d, ',rf(lin,col));
    end
    fprintf(fp,'%d}\n',rf(lin,col+1));
end
fprintf(fp,' };\n');

fclose(fp);

fprintf(1,'\nFim.\n');
```

Arquivo texto gerado pelo script "Enigma.m" para o caso de rotores e refletores com 6 letras.

```
Enigma_01.txt

------ ASM ------

RT_QTD:     .equ  05          ;Quantidade de Rotores
RF_QTD:     .equ  03          ;Quantidade de Refletores
```

```
;Rotores com 6 posições
RT1:  .byte 03, 05, 01, 02, 04, 06
RT2:  .byte 01, 05, 03, 04, 02, 06
RT3:  .byte 02, 05, 06, 01, 03, 04
RT4:  .byte 05, 02, 06, 01, 03, 04
RT5:  .byte 01, 04, 05, 03, 06, 02

;Refletores com 6 posições
RF1:  .byte 04, 05, 06, 01, 02, 03
RF2:  .byte 05, 06, 04, 03, 01, 02
RF3:  .byte 04, 03, 02, 01, 06, 05


------ C ------

#define RT_QTD    5           //Quantidade de Rotores
#define RF_QTD    3           //Quantidade de Refletores

//Rotores com 6 posições
rt1[] = {3, 5, 1, 2, 4, 6};
rt2[] = {1, 5, 3, 4, 2, 6};
rt3[] = {2, 5, 6, 1, 3, 4};
rt4[] = {5, 2, 6, 1, 3, 4};
rt5[] = {1, 4, 5, 3, 6, 2};

//Refletores com 6 posições
rf1[] = {4, 5, 6, 1, 2, 3};
rf2[] = {5, 6, 4, 3, 1, 2};
rf3[] = {4, 3, 2, 1, 6, 5};

//Matriz [5,6] com todos os Rotores
rt_mat[] = {
            {3, 5, 1, 2, 4, 6}
            {1, 5, 3, 4, 2, 6}
            {2, 5, 6, 1, 3, 4}
            {5, 2, 6, 1, 3, 4}
            {1, 4, 5, 3, 6, 2}
 };

//Matriz [3,6] com todos os Refletores
rf_mat[] = {
            {4, 5, 6, 1, 2, 3}
            {5, 6, 4, 3, 1, 2}
            {4, 3, 2, 1, 6, 5}
 };


------ Tabelas .csv ------
```

```
01; 03; 01; 02; 05; 01; 04; 05; 04
02; 05; 05; 05; 02; 04; 05; 06; 03
03; 01; 03; 06; 06; 05; 06; 04; 02
04; 02; 04; 01; 01; 03; 01; 03; 01
05; 04; 02; 03; 03; 06; 02; 01; 06
06; 06; 06; 04; 04; 02; 03; 02; 05
```

E.6. Links Interessantes sobre o Enigma

https://www.cryptomuseum.com/crypto/enigma/working.htm

https://hackaday.com/2017/08/22/the-enigma-enigma-how-the-enigma-machine-worked/

https://www.youtube.com/watch?v=ASfAPOiq_eQ (Simon Singh)

https://www.youtube.com/watch?v=G2_Q9FoD-oQ (legendado)

https://www.youtube.com/watch?v=G2_Q9FoD-oQ