

**GUILHERME HAKIME ANDRADE  
PEDRO SANTOS OLIVEIRA  
RAFAEL OLIVEIRA**

**ENIGMA**

**FRANCA/SP  
SETEMBRO/2021**

## **Contexto histórico**

Em 1918, Arthur Scherbius desenvolveu uma máquina de cifra que utilizava rotores, mas no início a máquina não teve sucesso, já em 1923 uma empresa que tinha Scherbius trabalhando no conselho de administração, passou a comercializar a máquina. Em seguida a Enigma passou a ter diversas melhorias até que a Marinha começou a usar em 1926, o Exército em 1929, e a Força Aérea em 1935, a máquina então foi um sucesso entre os Alemães e foi melhorada até 1945, sendo de suma importância para o desenvolvimento da guerra por parte dos Alemães. As diversas versões da Enigma foram usadas por praticamente todas as comunicações de rádio alemãs.

## **Componentes da máquina enigma**

A Enigma em geral é bastante complexa e tinha diversas versões, mas uma máquina genérica compunha seis principais componentes: Teclado, que tinha um painel com lâmpadas distribuídas para cada letra, conjunto de rotores, um refletor, painel de plugs e uma bateria para alimentação do sistema que se resume a circuitos elétricos. As máquinas tinham três rotores, cada um com 26 posições diferentes que deveriam ser escolhidas manualmente seguindo o padrão estipulado por alguém para assim começar o código, esse sistema de mudar as posições era muito importante para dificultar que alguém pudesse decifrar os enigmas.

## **Funcionamento**

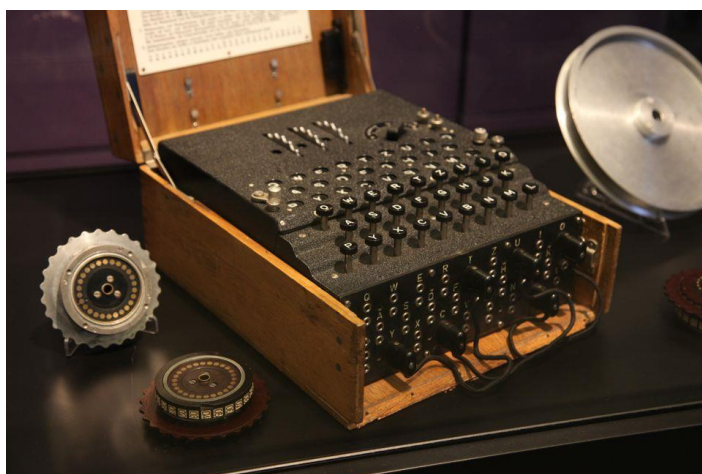
Cada letra do teclado ao ser pressionada, passavam por rodas rotativas onde eram misturados, cada vez a roda mais a direita era girada e resultava em códigos diferentes para cada letra pressionada no teclado. Todas as teclas eram conectadas a um rotor fixo chamado (ETW), após passar pelo ETW a corrente entrava no rotor mais à direita e o cabeamento interno traduzia para um dos contatos seu lado esquerdo, assim a corrente passava pelas rodas.

A máquina precisava ser configurada em ambos os lados envolvidos na comunicação para seu funcionamento, ou seja, a ordem dos rotores, o ajuste do anel, a

conexão inicial de cada um dos rotores e a conexão do plugues. No geral a máquina funcionava dessa maneira.

## Desafios para decifrar

A máquina Enigma ao contrário do que parece era bem simples, porém suas engrenagens geravam milhares de possibilidades, deixando assim a tarefa de decifrar esses enigmas quase que humanamente impossível. A Enigma era composta por cinco rotores nos quais apenas 3 eram selecionados de acordo com a tabela distribuída pelos nazistas mensalmente. Além disso, também era necessário as variáveis posições possíveis nos vinte e seis anéis de cada rotor, o operador precisava saber a posição inicial de uma sequência de três posições. No total as possibilidades chegavam a incríveis seis sextilhões de códigos.



<https://www.maisev.com/forum/off-topic/82401-o-enigma-nazista-e-bomba-de-turing.html>

Em resumo é uma máquina eletromecânica de criptografia com rotores, era usada para cifrar e decifrar mensagens, um excelente meio de comunicação durante a guerra, ela criada na Alemanha e aprimorada a partir de 1920. Foi bastante popularizada por conta da facilidade do uso e a suposta impossibilidade de decifrar os códigos.

### Referências

<https://www.infoescola.com/segunda-guerra/enigma/>

[https://pt.wikipedia.org/wiki/Enigma\\_\(m%C3%A1quina\)](https://pt.wikipedia.org/wiki/Enigma_(m%C3%A1quina))

<https://www.lume.ufrgs.br/bitstream/handle/10183/66106/000870987.pdf>

<https://cryptoid.com.br/banco-de-noticias/icone-da-criptografia-na-2a-guerra-mundial-maquina-enigma-tem-exemplar-no-brasil/>

### Perguntas:

- 1) No início a Enigma foi desenvolvida exclusivamente para a guerra ou tinha como finalidade a comercialização ?
- 2) Qual o procedimento necessário para mudar os formatos de códigos?
- 3) Por que a Enigma foi de suma importância para a nação Alemã durante a guerra?

### Respostas:

- 1) O uso da máquina Enigma na guerra foi uma adaptação, ela inicialmente não foi criada para essa finalidade.
- 2) A mudança da posição dos rotores da máquina.
- 3) A comunicação entre o exército, marinha e aeronáutica era muito importante e todas as informações precisavam ser sigilosas para a conclusão dos planos, a Enigma foi a ferramenta ideal para criptografar as mensagens.