

**EMC – Estruturas Matemáticas para Computação 195405**

**Trabalho final**

**{Enigma Machine}**

|  |  |  |
| --- | --- | --- |
| **Nome** | **Matrícula** | **Assinatura** |
| Gesiel dos Santos Freitas | 14/0082531 |  |
| Vinicius Pinheiro da Silva Corrêa | 14/0066543 |  |

Brasília 10 de julho de 2015

**Introdução**

A enigma é uma maquina de criptografia inventada pelo alemão Artur Scherbius no final da primeira guerra mundial. Seu uso se fez em grande escala pelos alemães na segunda guerra mundial. Por volta de 1920 passou a ser comercializada e vários países começaram a adotar em seus serviços militares governamentais. Existem varias versões da enigma a mais conhecida é a Wehrmacht que foi usada pelo poder militar alemão.

**Como funciona:**

A enigma usa um sistema de rotores, existem vários tipos de rotores no qual se tem uma sequência no ordenado do alfabeto. As variáveis que compõem a enigma são:

* Os rotores e sua ordem
* Posições iniciais dos rotores
* Posição do anel
* Ficha de tabuleiros e definições

**Rotores**

Os rotores são sistemas que mudam suas posições de acordo com seu entalhe assim uma letra não saíra criptografadas duas vezes com a mesma saída. Os rotores ainda podem assumir ordens tais como direita, centro e esquerda. O mais a esquerda embaralha as cartas primeiro e seu entalhe gira uma posição fazendo com que a letra digitada novamente saíra com outra codificação, depois vem o do centro e assim por diante até chegar no refletor e volta fazendo o caminho inverso.

Cada rotor tem 26 posições no qual o mesmo fica girando pra criptografar as palavras. Uma característica importante é o fato de que os rotores podem assumir posições iniciais diferentes essa característica é conhecida como (Ringstellung : ajuste do anel) que define a posição inicial do rotor veja como funciona: ajuste no anel do rotor I em ’A’(ou 1)¹

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

E K M F L G D Q V Z N T O W Y H X U S P A I B R C J¹

Com um ajuste do anel de 'B' (ou 2), rotor substituição do I parece com isso:

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

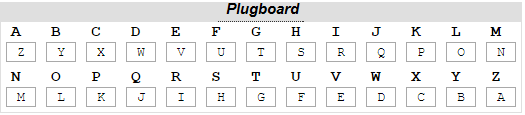
E K M F L G D Q V Z N T O W Y H X U S P A I B R C J¹

**Refletor**

Os refletores têm funções de refleti o sinal para a viagem de volta através dos rotores². Existem vários tipos de refletores o mais comum é o refletor ‘B’.

**PlugBoard**

O plugboard é o uma camada de segurança adicional que liga cada letra a outra existem treze matriz de contato que cada contato conecta duas letras, por exemplo, PO este par sofre substituição antes de ir para o primeiro rotor se você digitar a letra P irá para o rotor a letra O, se o rotor devolver a letra O passará pelo plugboard e devolvera a letra P. veja um exemplo de configuração do plugboard.



*1 .0 imagem plugboard.*

**Codificando uma letra.**

Definições dos rotores: vamos usar os rotores I, II, III nesta ordem.

Posição inicial: AAA

Refletor ‘B’

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

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

Rotores I, II, III

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

E K M F L G D Q V Z N T O W Y H X U S P A I B R C J¹

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

E K M F L G D Q V Z N T O W Y H X U S P A I B R C J¹

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

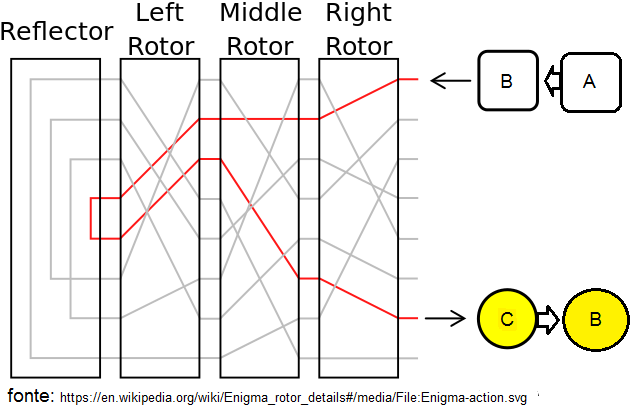
BDFHJLCPRTXVZNYEIWGAKMUSQO

Letra codificada A

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| plugboard | III | II | I | Refletor | Inv(I) | Inv(II) | Inv(III) | plugboard | saída |
| Mantém A | B=>D | C=>D | D=>F | F=>S | S=>S | S=>E | F=>C | B mantém | B |

Cada passagem de um Rotor para outro é feito um calculo de soma e subtração, esse calculo é feito levando em conta quanto o rotor que está passando a codificação pra frente andou e quanto o que está recebendo andou.

Entendendo: quando o A saiu do plugboard o rotor III rodou então a nova posição inicial ficou AAB, assim foi somado um índice no A que passou a ser B, o rotor então fez a codificação tornando D, como o rotor adicionou um índice para o próximo rotor deverá retirar essa soma então se faz a subtração de um índice passando a letra para C, o rotor II recebe e faz sua codificação tornando a em D, como o rotor II não andou não soma passa a letra normal para o rotor I que faz sua codificação e a transforma em F, passa para o refletor e troca para S, agora vamos fazer o caminho inverso , S chega no rotor I e codifica em S não mudou mera coincidência), passa para rotor II que codifica em E, como o rotor I andou e o rotor II não andou faz-se a soma de um índice então o rotor I receberá a letra F que a codifica em C para voltar ao normal tem que fazer uma subtração (veja que fizemos uma soma nessa passagem de ida de 1 no índice) a letra C passa a ser a letra B que chega no plugboard que a mantém e é a saída codificada. Note que o plugboard não foi configurado ele mantém o padrão cada letra está codificada com ela mesma. Veja agora o caminho por um gráfico.



**Conclusão**

Com a demonstração e o nosso software funcionando concluímos que o estudo e aprendizado sobre esse tema será de grande importância em nova vida tanto pessoal como profissional, se você quiser cifra uma palavra ou texto não deixe de usar nosso software que acompanha esse material e está junto.

**Bibliografia**

1. **PRATICAL CRYPTOGRAPHY - Enigma Cipher** <http://practicalcryptography.com

/ciphers/enigma-cipher/> acesso em 05/07/2015.

1. **ENIGMA – Enigma Mechanics** <http://enigma.louisedade.co.uk/howitworks.html> acesso em 05-07-2015.

**WIKIPEDIA – Enigma rotor details** <https://en.wikipedia.org/wiki/Enigma\_rotor\_details> acesso em 05-07-2015.

**ENIGMACO – Enigma** <http://www.enigmaco.de/enigma/enigma.swf> acesso em 05-07-2015.

**STARTPAD-GOOGLECODE – Enigma Machine Simulator** < http://startpad.googlecode.com/hg/

labs/js/enigma/enigma-sim.html> acesso em 05-07-2015.