Relatório da Atividade Sobre Cifra de Máquina de Rotação da Disciplina

Introdução à Criptografia

João Marcello Mendes Moreira

E-mail: joaomarcello.mm@gmail.com

Professor: Areolino de Almeida Neto

Resumo da Atividade. Implementar a cifra de máquina de rotação com três cilindros

considerando o alfabeto com 26 letras maiúsculas. O programa deve permitir ao usuário

a escolha entre a cifragem e a decifragem de uma mensagem armazenada em um arquivo

de texto.

Implementação

Utilizou-se a linguagem Python 3.7 para a realização da atividade. Logo no início, o

programa exibe um menu com as seguintes opções: (1) Cifrar, (2) Decifrar e (3) Sair. Se

o usuário digitar 1, o programa lerá o conteúdo do arquivo 'claro.txt' e aplicará a cifra de

máquina de rotação. O resultado é armazenado no arquivo 'cifrado.txt'. Caso a opção

informada seja 2, o programa irá descriptografar o conteúdo do arquivo 'cifrado.txt' e

armazenará o resultado no arquivo 'decifrado.txt'. O programa encerrará caso a opção

informada seja 3.

O programa utiliza duas classes para executar a lógica da máquina de rotação:

"Cilindro" e "MaquinaRotacao". A classe "Cilindro" possui os seguintes atributos

principais: left (vetor com os números do lado esquerdo do cilindro), right (vetor com os

números do lado direito do cilindro) e rotateCount (a quantidade de rotações que o

cilindro já fez. Inicia em 0 e o máximo é 25. Se ultrapassar o máximo, volta ao valor 0).

Entre as funções, vale ressaltar o funcionamento da função "press" que, dado um

caractere, retorna um outro caractere, como mostra a Figura 1 onde o resultado da função

para o caractere "G" é o caractere "N". Já na Figura 2, em que há três cilindros, o resultado

para o caractere "G" é o caractere "D".

Figura 1 - Funcionamento do cilindro.

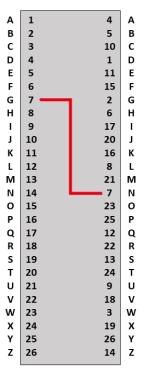
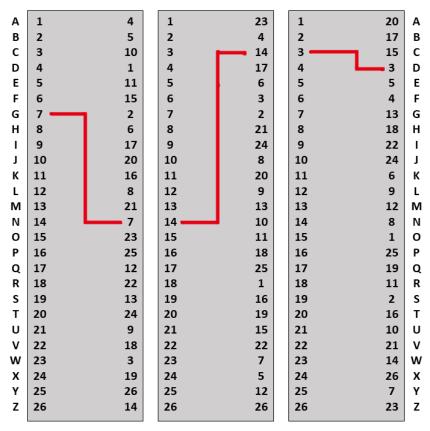


Figura 2 - Resultado da função press com três cilindro conectados.



A classe *MaquinaRotacao* é responsável por fazer o controle dos cilindros (executa uma rotação no primeiro cilindro a cada caractere pressionado), e os armazena como em uma lista duplamente encadeada, em que cada cilindro conhece o próximo cilindro e o anterior. Essa classe é responsável pela cifragem e decifragem da mensagem.

Para cifrar, cada caractere da mensagem é passado para a máquina (exclui-se os espaços em brancos do texto se houver). O resultado é armazenado no arquivo "cifrado.txt". Para decifrar, muda-se o "modo" da máquina. Ao fazer isso, o funcionamento da função *press* é alterado. Para exemplificar, voltemos à Figura 2. Caso o caractere atual seja "D" o resultado seria "G", ou seja, a máquina funciona de maneira invertida. Antes de começar a decifragem, fazemos a máquina voltar para a posição inicial. Em seguida, rotacionamos o cilindro a quantidade de caracteres que há na mensagem cifrada (isso é feito para deixar a máquina no mesmo estado que estava ao terminar a cifragem). Por fim, passamos cada caractere da mensagem cifrada para a máquina, que retornará o texto decifrado e armazenará no arquivo "decifrado.txt".

Problemas conhecidos

O programa não admite caracteres especiais no texto claro.