

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.

A	1	4	A
B	2	5	B
C	3	10	C
D	4	1	D
E	5	11	E
F	6	15	F
G	7	2	G
H	8	6	H
I	9	17	I
J	10	20	J
K	11	16	K
L	12	8	L
M	13	21	M
N	14	7	N
O	15	23	O
P	16	25	P
Q	17	12	Q
R	18	22	R
S	19	13	S
T	20	24	T
U	21	9	U
V	22	18	V
W	23	3	W
X	24	19	X
Y	25	26	Y
Z	26	14	Z

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

A	1	4	1	23	1	20	A
B	2	5	2	4	2	17	B
C	3	10	3	14	3	15	C
D	4	1	4	17	4	3	D
E	5	11	5	6	5	5	E
F	6	15	6	3	6	4	F
G	7	2	7	2	7	13	G
H	8	6	8	21	8	18	H
I	9	17	9	24	9	22	I
J	10	20	10	8	10	24	J
K	11	16	11	20	11	6	K
L	12	8	12	9	12	9	L
M	13	21	13	13	13	12	M
N	14	7	14	10	14	8	N
O	15	23	15	11	15	1	O
P	16	25	16	18	16	25	P
Q	17	12	17	25	17	19	Q
R	18	22	18	1	18	11	R
S	19	13	19	16	19	2	S
T	20	24	20	19	20	16	T
U	21	9	21	15	21	10	U
V	22	18	22	22	22	21	V
W	23	3	23	7	23	14	W
X	24	19	24	5	24	26	X
Y	25	26	25	12	25	7	Y
Z	26	14	26	26	26	23	Z

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.