Trabalho 02

Arquitetura e Organização de Computadores I

Prof. Roberto Cabral

30 de Maio de 2019

Introdução

Este trabalho consiste em implementar uma cifra criptográfica simples, a cifra de Vigenère.

A cifra de Vigenère é um método de criptografia que usa uma série de diferentes cifras de César baseadas em letras de uma senha. Esta cifra é muito conhecida porque é fácil pôr em prática e aparentar ser inquebrável, para quem tem pouca prática em criptoanalise. Durante mais de 300 anos esta cifra foi julgada inquebrável, mas Charles Babbage e Friedrich Kasiski, independentemente um do outro, encontraram um modo de resolvê-la em meados do século XIX.

Descrição

Numa cifra de César, cada letra do alfabeto é deslocada da sua posição um número fixo de vezes; por exemplo, se tiver um deslocamento de 3, "A" torna-se "D", "B" vira "E", etc. A cifra de Vigenère consiste no uso de várias cifras de César em sequência, com diferentes valores de deslocamento ditados por uma "palavra-chave".

Para cifrar, é usada uma tabela de alfabetos que consiste no alfabeto escrito 26 vezes em diferentes linhas, cada um deslocado ciclicamente do anterior por uma posição. As 26 linhas correspondem às 26 possíveis cifras de César. Uma palavra é escolhida como "palavra-chave", e cada letra desta palavra vai indicar a linha a ser utilizada para cifrar ou decifrar uma letra da mensagem.

Por exemplo, supondo que se quer criptografar o texto:

`ATACARBASESUL` ("atacar base Sul")

Escolhendo a chave e repetindo-a até ter o comprimento do texto a cifrar, por exemplo, se a chave for "`LIMAO`":

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

Tabela 1: Matriz de Vigenère

`LIMAOLIMAOLIM`

A primeira letra do texto, “A”, é cifrada usando o alfabeto na linha “L”, que é a primeira letra da chave. Basta olhar para a letra na linha “L” e coluna “A” na matriz de Vigenère (Tabela 1), e que é um “L”. Para a segunda letra do texto, ver a segunda letra da chave: linha “I” e coluna “T” , que é “B”, continuando sempre até obter:

Texto:	ATACARBASESUL
Chave:	LIMAOLIMAOLIM
Texto cifrado:	LBMCOCJMSSDCX

A decriptação é feita inversamente.

Trabalho

Como trabalho, deve-se implementar as funções de encriptação e decriptação da cifra de Vigenère. Como entrada para a função de encriptação, o programa deve ler um arquivo contendo a mensagem a ser encritada e um arquivo com a chave de encriptação e escrever um arquivo de saída contendo a mensagem encriptada. Como entrada para a função de decriptação, o programa deve ler um arquivo contendo a mensagem encritada e um arquivo com a chave e escrever um arquivo de saída contendo a mensagem decriptada. Deve-se usar a linguagem Assembly. O trabalho deverá ser entregue no dia 16 de junho e a apresentação será nos dias 17 e 18 de junho.

Obs1.: o trabalho é individual.

Obs2.: qualquer indício de plágio implicará em nota ZERO a todos os envolvidos.