Projeto 1
Cifra de Vigenère

Nathália Oliveira Pereira, 180042980
Victor Manuel Brito Santos, 200044184

[1]Dep. Ciência da Computação – Universidade de Brasília (UnB)
CIC0201 - Segurança Computacional

180042980@aluno.unb.br, 200044184@aluno.unb.br

1. Introdução

A cifra de Vigenère é uma cifra simples e ainda assim mais segura do que a famosa cifra de César, que consiste em mover cada letra do alfabeto um determinado número de passos para a frente para criar um texto cifrado. Já a cifra de Vigenère precisa de uma chave, cada letra dessa chave é usada para cifrar uma letra do texto, fazendo com que a cifra de Vigenère possua diversos ”shifts” de alfabeto originados na cifra de César.

2. Tratamento do texto

Todos as letras acentuados ou grafadas de forma especial, assim como letras maiúsculas, foram substituídas por suas respectivas letras minúsculas e não acentuadas. Todos os caracteres que não são letras, como espaços e pontuação foram removidos antes de criptografar/descriptografar o texto.

3. Interação com o usuário

O programa permite que o usuário criptografe um texto com uma chave ou descriptografe o texto (com ou sem chave), tanto para textos em inglês quanto para textos em português. Caso o usuário queira descriptografar um texto sem saber qual chave foi usada, o usuário receberá uma lista dos tamanhos chaves mais prováveis com base no índice de coincidência (que será explicado na seção 6.1 e poderá escolher qual será usado para tentar descriptografar o texto, sendo que o tamanho de chave mais provável já é sugerido. Após isso, o usuário será apresentado com as frequências de cada letra do alfabeto, com a frequência do alfabeto do idioma utilizado (português ou inglês) à esquerda e a frequência do texto a ser decifrado à direita e deverá informar duas letras correspondentes para que o texto será decifrado, sendo que novamente a correspondência mais provável já é realizada por padrão. Por fim, o usuário recebe o texto descriptografado e pode tentar novamente com outros tamanhos de chave ou correspondências entre os alfabetos.

4. Cifrando o texto

Para cifrar o texto com uma determinada chave, primeiro repetimos a chave até que ela seja do tamanho do texto a ser cifrado, conforme mostrado na figura 1, gerando uma keystream. Após isso, para cada letra do texto a ser cifrado, somamos o valor correspondente dessa letra (sendo que a letra A equivale a 0, B equivale a 1 e assim por diante) com a letra correspondente na keystream. O valor da letra no texto cifrado é o resto da divisão o resultado dessa soma com o tamanho do alfabeto utilizado. Também é possível utilizar

a tabela da figura 2 que basicamente faz o mesmo processo e corresponde cada duas letras a uma nova letra

Text	T	H	I	N	K	A	B	O	U	T	I	T
Key	V	I	N	T	A	G	E	V	I	N	T	A
Cipher	O	P	V	G	K	G	F	J	C	G	B	T

Figure 1. Cifra de Vigenère

	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

Figure 2. Tabela da cifra de Vigenère

5. Decifrando o texto

Para decifrar o texto sabendo qual é a chave, fazemos o processo inverso da cifração. Assim, para cada letra do texto a ser decifrado, subtraímos o valor dessa letra com o valor da chave e somamos o tamanho do alfabeto utilizado até que o número seja positivo.

6. Decifrando o texto sem a chave

Para quebrar a cifra sem saber qual é a chave, podemos descobrir o tamanho da chave e fazer uma análise de frequência com base nisso. Descobrir o tamanho da chave é importante porque se temos duas letras que sabemos que foram cifradas usando a mesma letra correspondente na chave, podemos analisar a frequência que elas aparecem no texto para descobrir qual letra é. Isso não seria possível se analisássemos duas letras que foram cifradas com letras diferentes, pois duas letras diferentes poderiam ter o mesmo resultado final no texto cifrado.

6.1. Encontrando o tamanho da chave

Primeiro definimos o universo das chaves possíveis, no caso usamos os números de 1 até 10. Então, para cada tamanho possível de chave, dividimos o texto em n grupos de letras (sendo n o tamanho da chave) sendo que o primeiro grupo é composto por todas as letras de n em n desde a primeira, o segundo por todas as letras de n em n desde a segunda e assim por diante. Então, para cada grupo calculamos o índice de coincidência dele e obtemos a média de todos esses índices. Assim, o tamanho de chave que tenha o índice de frequência mais próximo do índice de frequência do alfabeto da língua em análise (português ou inglês) será o tamanho de chave mais provável. É válido notar também que todos os números que sejam múltiplos de outro terão o índice de coincidência bastante parecido. O índice de coincidência é a probabilidade de duas letras obtidas aleatoriamente de um texto serem iguais, o que corresponde aproximadamente ao somatório dessa probabilidade para cada letra elevada ao quadrado.

6.2. Análise de frequência

Para cada tamanho possível de chave, mapeamos as frequências das letras no texto a ser decifrado e comparamos com a frequência das letras na língua inglesa ou portuguesa. Assim, tentamos corresponder a frequência de um alfabeto com o outro, utilizando para isso a menor soma das diferenças entre as frequências de cada letra no idioma escolhido (português ou inglês) e a frequência no texto a ser decifrado, ou seja, o alfabeto que possui o menor erro absoluto entre as frequências das letras. Então usamos a letra do alfabeto correspondente para decifrar o texto letra por letra. A opção com a menor diferença absoluta é escolhida por padrão.