Trabalho 1
Cifra de Vigenère

Lucas Resende Silveira Reis, 18/0144421

[1]Dep. Ciência da Computação – Universidade de Brasília (UnB)
CiC 0201 - SEGURANÇA COMPUTACIONAL

toy.lcdv@hotmail.com

Abstract. *This corresponds to project 1, on encryption, decipherment and frequency attack on the Vigenère Cipher.*

Resumo. *Este corresponde ao trabalho 1, sobre cifração, decifração e ataque por frequência sobre a Cifra de Vigenère.*

1. Introdução

A cifra de Vigenère, uma variação da cifra de substituição polialfabética, é uma técnica de criptografia que se baseia em uma senha para aplicar várias cifras de César em letras de um texto original.Nesse trabalho iremos falar sobre a cifra vigenère que é um método de criptografia que utiliza uma série de diferentes ”cifras de César”. Na parte 1 será gerado um criptograma a partir de uma mensagem e senha e depois iremos descriptografar utilizando a mensagem criptografada e a sua senha. Já na parte 2, faremos um programa que consegue encontrar a senha de uma mensagem cifrada a partir de análise frequência numérica.

1.1. Parte 1

Aqui foi pedido para que um cifrador recebesse uma mensagem, e que essa mensagem deve ser cifra segundo a cifra Vigenère, para que assim fosse criado um criptograma que depois seria usado em um decifrador, que ao receber o criptograma e a chave decifra segundo a cifra de Vigenère, assim recuperando a mensagem original.

Como funciona:

- escolha uma senha e uma mensagem.
- repita a senha até que tenha o tamanho da mensagem. Por exemplo: Mensagem: trabalhos Senha: casa, a repetição seria casacasac. Cada letra do alfabeto pode ser associada com um número que vai de 0 a 26.
- Agora, para cifrar ou decifrar uma mensagem, você olha para a próxima letra da senha e usa o número associado a ela como o deslocamento. Esse deslocamento determina quantas posições no alfabeto a letra da mensagem será deslocada.

	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

Figura 1. Aqui está a grade de Vigenère, que ilustra como é cifrado. Por exemplo com a mensagem “trabalho” e senha “casa” a primeira letra fica ‘v’, e no final forma o criptograma “vrsbclzo”.

Com o programa feito é possível colocar mensagens com todos os tipos de caracteres, mesmo os não alfabéticos. O programa ainda sim será capaz de cifrar e decifrar segundo a cifra de Vigenère. Nele primeiro será pedido a senha e depois a mensagem. Após ser submetido já será mostrada a mensagem criptografada e a mensagem recuperada através da senha.

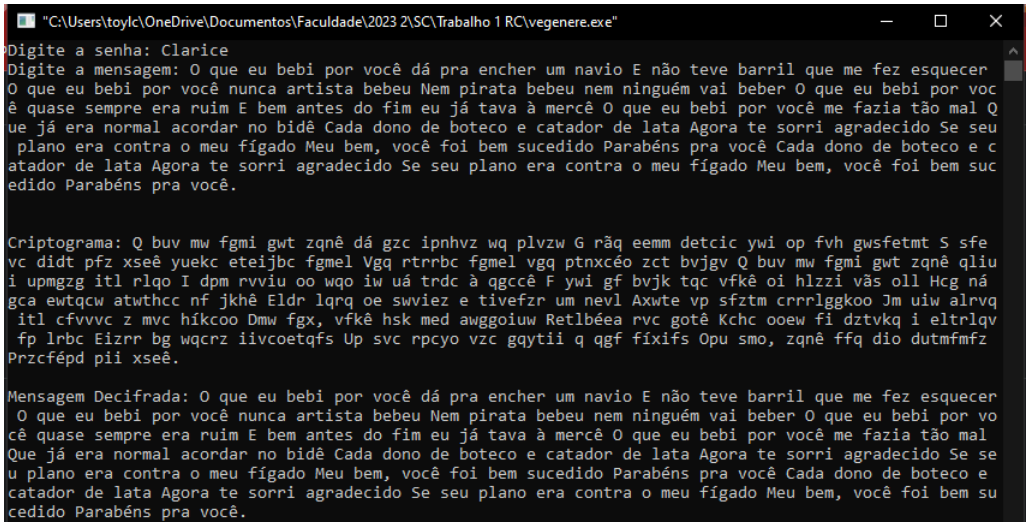

Figura 2. Resultado

2. Parte 2

Agora na parte 2 é requisitado que o programa recebe uma mensagem criptografada em inglês e uma em português. A senha dessas mensagens deve ser recuperada. Deve ser utilizado análise de frequência numérica para o ataque.

Análise de Frequência de Letras: Nesse método, é calculada a frequência de ocorrência de cada letra no texto cifrado. Essa frequência é comparada com a frequência média de ocorrência de letras em uma determinada língua, como o português ou o inglês. A ideia é que, em um texto cifrado usando a cifra de Vigenère, as letras correspondentes à mesma letra da chave terão uma frequência semelhante. Assim, calculando as frequências das letras no texto cifrado e comparando-as com as frequências típicas da língua alvo, é possível identificar caracteres da chave.

Letra	Frequência
a	14.63%
b	1.04%
c	3.88%
d	4.99%
e	12.57%
f	1.02%
g	1.30%
h	1.28%
i	6.18%
j	0.40%
k	0.02%
l	2.78%
m	4.74%
n	5.05%
o	10.73%
p	2.52%
q	1.20%
r	6.53%
s	7.81%
t	4.34%
u	4.63%
v	1.67%
w	0.01%
x	0.21%
y	0.01%
z	0.47%

Tabela 1. Frequências relativas das letras em português

Análise de Repetições de Agrupamentos: Esse método envolve a busca por padrões de repetições de grupos de letras em um texto cifrado. Se houver repetições de grupos de letras em intervalos regulares no texto cifrado, isso pode indicar o comprimento da chave. Uma vez que o comprimento da chave é determinado, é possível dividir o

texto cifrado em várias sequências, cada uma correspondente a uma letra da chave. Em seguida, pode-se realizar análises de frequência em cada sequência, como mencionado anteriormente, para determinar os caracteres da chave. Exemplo de repetição de grupo 'BFQ': [167, 335, 455]. Estes números são as posições da mensagem onde a repetição foi encontrada.

```
Chave texto PT-BR = CLARICE
Mensagem PT-BR = O QUE EU BEBI POR VOCE DA PRA ENCHER UM NAVIO E NAO TEVE BARRIL QUE ME FEZ ESQU
ECER O QUE EU BEBI POR VOCE NUNCA ARTISTA BEBEU NEM PIRATA BEBEU NEM NINGUEM VAI BEBER O QUE EU
BEBI POR VOCE QUASE SEMPRE ERA RUIM E BEM ANTES DO FIM EU JA TAVA A MERCE O QUE EU BEBI POR VOCE
 ME FAZIA TAO MAL QUE JA ERA NORMAL ACORDAR NO BIDE CADA DONO DE BOTECO E CATADOR DE LATA AGORA
TE SORRI AGRADECIDO SE SEU PLANO ERA CONTRA O MEU FIGADO MEU BEM, VOCE FOI BEM SUCEDIDO PARABENS
 PRA VOCE CADA DONO DE BOTECO E CATADOR DE LATA AGORA TE SORRI AGRADECIDO SE SEU PLANO ERA CONTR
A O MEU FIGADO MEU BEM, VOCE FOI BEM SUCEDIDO PARABENS PRA VOCE
```

Figura 3. Resultado

Essa imagem mostra um print do resultado de um criptograma.

3. Conclusão

A cifra de Vigenère é uma técnica de criptografia histórica que foi inicialmente projetada para aumentar a segurança em relação à cifra de César, que era relativamente fácil de quebrar por meio de análise de frequência. É bom olharmos para meios de criptografia antigos e de como estes são quebrados, pois isso nos mostra os motivos pelo qual buscamos novas maneiras de criptografar.

Referências

[1] Shene, C. K. (s.d.). Recovering the Key in Vigenère Cipher. Michigan Technological University. https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Recover.html

[2] Wikipédia. Frequência de Letras. https://pt.wikipedia.org/wiki/Frequ%C3%AAncia_de_letras

[3] Wikipedia. Vigenère Cipher. https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher#