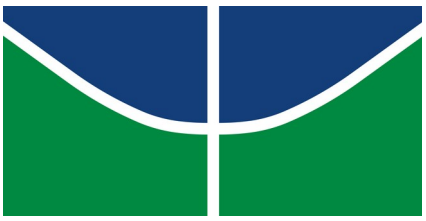

Universidade de Brasília – UnB
Instituto de Ciências Exatas
Dpt. Ciência da Computação
Segurança Computacional 2022/2

Cifra de Vigenère

Codificador, decifrador e recuperação de chave
por análise de frequência (Kasiski)

Emanuel Firmino Abrantes
19/0105747

Dezembro – 2022
Brasília/DF

Introdução

O presente relatório tem por objetivo descrever o funcionamento do algoritmo desenvolvido em linguagem C++ que implementa a cifração, decifração e a recuperação de chave por análise de frequência (método Kasiski) da cifra de Vigenère.

Cifra de Vigenère

A cifra pode ser definida como uma evolução da cifra de César, uma vez que a cifração utiliza-se do deslocamento do alfabeto, mas não limita-se a uma simples substituição de caracteres.

O processo de codificação necessita de uma chave, na qual será iterada e, cada caracter da mesma, corresponderá a um valor de deslocamento do alfabeto (que será utilizado para cifrar cada letra da mensagem). Desta forma, o criptograma gerado terá um período de cifração igual ao tamanho da chave.

	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

Figura 1.1: Tábua cifradora/decifradora de Vigenère.

Classe ‘Vigenere’

O algoritmo, desenvolvido em C++, tem seu funcionamento em torno da classe desenvolvida, nomeda de “Vigenere”.

```
class Vigenere+$
{$
public:$
>   int* repeatedSequencesLength(std::string);$
>   int possibleKeyLength(int*);$
>   std::string encryptDecrypt(std::string, std::string, bool);
>   std::string possibleKey(std::string, int, int);$
>   std::string staticFilter(std::string);$
$
private:$
>   bool isValid(char);$
>   bool isUpper(char);$
>   char floorFilter(char);$
};$
```

Figura 1.2: classe “Vigenere”.

Métodos da classe

- **encryptDecrypt(mensagem, chave, decrypt=false)**: Cifra ou decifra (a depender do valor booleano atribuído à ‘decrypt’; por padrão, cifra) a mensagem passada por parâmetro, utilizando a chave informada;

- **staticFilter(mensagem)**: Realiza um filtro na mensagem informada, retirando quaisquer caracteres não pertencentes ao alfabeto (letras maiúsculas são mapeadas para suas respectivas letras minúsculas). É utilizado para facilitar a busca por sub strings no método de recuperação de chave por análise de frequência;

- **isValid(caracter)**: Retorna verdadeiro se o caracter informado é uma letra (minúscula ou maiúscula). Retorna falso, caso contrário;

- **isUpper(letra):** Retorna verdadeiro se a letra informada é maiúscula: falso, caso contrário;

- **floorFilter(letra maiúscula):** Retorna a letra minúscula correspondente;

- **repeatedSequencesLength(mensagem filtrada):** Retorna um ponteiro para integer com as quantidades de caracteres entre sub strings repetidas;

- **possibleKeyLength(ponteiro para integer):** Verifica se as quantidades são múltiplas de valores entre 2-24 e retorna o provável valor do tamanho da chave usada para cifrar (2-24);

- **possibleKey(mensagem filtrada, língua, tamanho da chave):** Levando em consideração o tamanho da chave, verifica-se a frequência das letras na mensagem filtrada e busca o deslocamento que possui a menor diferença possível, e, por consequência, encontrando o caracter correspondente à cada posição da chave (a língua fornecida possui a frequência das letras para tal).

Ataque de recuperação de chave

Para a demonstração do funcionamento do ataque, foi utilizado o criptograma fornecido para quebra: desafio1.txt.

Primeiramente é realizado a chamada ao método staticFilter, do qual retira todos os caracteres que não são letras (letras acentuadas também são removidas).

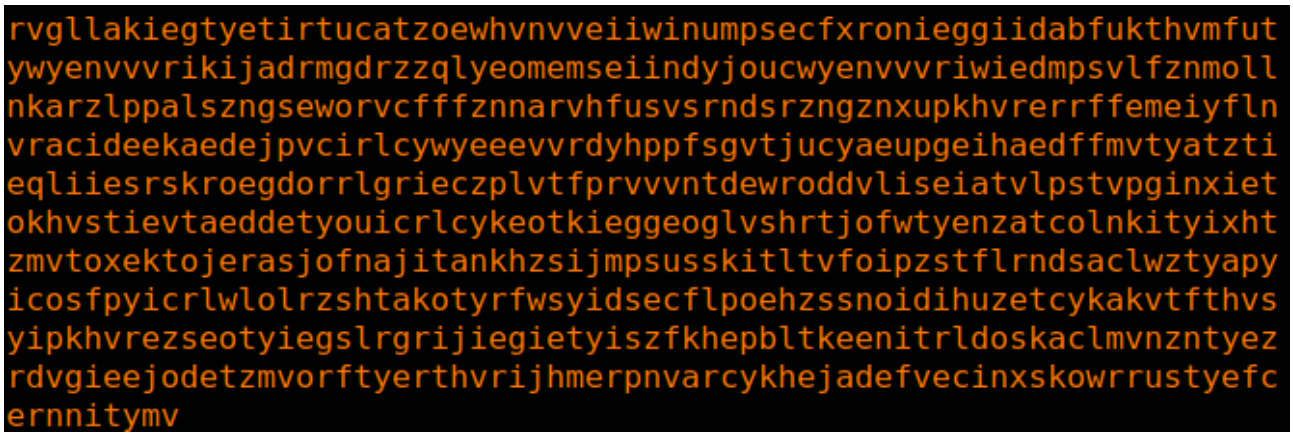

Figura 1.3: Criptograma filtrado.

Em seguida é utilizado o método repeatedSequencesLength, na qual procura por sub strings repetidas e a quantidade de caracteres entre estas.

```
kieg 353
secf 455
iegg 313
ywye 153
wyen 40
```

Figura 1.4: sequências de quatro caracteres repetidas com a respectiva quantidade de caracteres entre.

Com as quantidades de caracteres entre sub strings em mãos, é possível determinar o tamanho da chave usada para criptografar. Neste caso, tamanho 5 (utilizando o método possibleKeyLength).

Por fim, utilizando o método possibleKey, é possível obter a chave (utilizando as frequências de letras, para português ou para o inglês).

```
float frequency_EN[] = {$
>   0.082, 0.015, 0.028, 0.043, 0.127, 0.022,$
>    0.02, 0.061,  0.07, 0.015, 0.077,  0.04,$
>   0.024, 0.067, 0.075, 0.019,  0.01,  0.06,$
>   0.063, 0.091, 0.028, 0.098, 0.024, 0.015,$
>    0.02, 0.007++$
};$

float frequency_PT[] = {$
>   0.146,  0.01, 0.039,  0.05, 0.126,  0.01,$
>   0.013, 0.008, 0.062, 0.004, 0,002, 0.028,$
>   0.047, 0.045, 0.097, 0.025, 0.012, 0.065,$
>   0.068, 0.043, 0.036, 0.016, 0.004, 0.025,+$
>   0.001, 0.047+$
};$
```

Figura 1.5: Frequências das letras (em %).

Resultado final:

```
regulating the circulation.  whenever i
find myself growing grim about the mouth; whenever it is a damp,
drizzly november in my soul; whenever i find myself involuntarily
pausing before coffin warehouses, and bringing up the rear of every
funeral i meet; and especially whenever my hypos get such an upper
hand of me, that it requires a strong moral principle to prevent me
from deliberately stepping into the street, and methodically knocking
people's hats off--then, i account it high time to get to sea as soon
as i can.  this is my substitute for pistol and ball.  with a
philosophical flourish cato throws himself upon his sword; i quietly
take to the ship.  there is nothing surprising in this.  if they but
knew it, almost all men in their degree, some time or other, cherish
very nearly the same feelings towards the ocean with me.

 key [ arara ]
```

Figura 1.6: Texto descriptografado, com a senha descoberta ‘arara’.