Criptografia: Parte 05 (Cifra de Vigenère-1)

Mário Leite

...

Embora o programa-exemplo "**ProgCifraCesar**", apresentado anteriormente, tenha sido implementado de maneira bem geral e que até possa servir para todos os métodos de codificação conhecidos como "Cifragens de Cesar", mesmo assim representa métodos baseados em substituições ***monoalfabéticas***. E do ponto de vista da segurança eles deixam muito a desejar quando comparados com os métodos que utilizam chaves simétricas; por isto, já nos séculos passados os criptólogos da época começaram a pesquisar métodos de chave simétricas, mas que que poderiam oferecer maior proteção às mensagens. Assim, no século XVI o francês *Blaise de Vigenère* ficou muito interessado nos sistemas de codificação e começou a estudar alternativas mais seguras de cifragens. Então, baseado em trabalhos já existentes, aperfeiçoou um método mais seguro de substituição de modo que uma letra da mensagem não fosse substituída sempre por uma outra única letra, mas, sim por outras na mesma mensagem; e baseado nesta ideia foi criada uma tabela conhecida como "Grelha de Vigenère" ou "Tabua Recta". Assim, estava criada a chamada "Cifra de Vigenère", que ficou com o mérito do método por tê-lo aperfeiçoado através dessa "grelha" (vide **tabela CVI.1**). Este método foi considerado indecifrável durante muito tempo, e até apelidado de "Le Chiffre Indéchiffrable" por ser de difícil decodificação com os recursos de criptoanálises disponíveis na época, até que em 1854 *Charles Babbage* conseguiu decifrá-lo através da análise de frequência[1].

O método de criptografia pela **"Cifra de Vigenére"** é baseado em uma chave única que serve tanto para codificar quanto para decodificar a mensagem; é como uma chave física que "*fecha a porta ao girar na fechadura para a direita*" e "*abre a porta ao girar na fechadura para a esquerda*". Observe o esquema mostrado do **quadro CVI.1** para codificar a mensagem "**DESTRUIREMAILSDAPONTE**" (mensagem de um corrupto querendo esconder uma de suas falcatruas), cuja chave de *codificação/decodificação* é a palavra "**PIXULECO**". Observe que na **tabela CVI.2** uma mesma letra da mensagem original foi substituída por várias, e não por apenas uma única. Por exemplo, a letra "**E**" foi substituída por "**M**", por "**P**" e por "**T**" nas suas três ocorrências. Se fosse utilizada a "Cifragem de Cesar" com deslocamento 3 ela seria substituída somente pela letra "**H**" nas três ocorrências da mensagem. Outro detalhe a ser observado no método de *codificar/decodificar* com a "Cifra de Vigenère" é que no dispositivo montado para o algoritmo a chave abrange toda a mensagem original; a chave "PIXULECO" tem oito caracteres enquanto a mensagem original tem vinte e um; então, foi preciso repetir os caracteres da chave até alcançar o mesmo tamanho da mensagem. Portanto, além de ser um método de cifragem com substituição ***polialfabética***, a "Cifra de Vigenère" é também *monogrâmica* (substituição de caracteres do texto original por um outro com o comprimento do texto codificado igual ao comprimento da mensagem original).

O esquema da **tabela CVI.2** mostras que a primeira letra "**D**" da mensagem para se transformar em "**S**" pode ser considerada como a intersecção da letra "**D**" da primeira linha com a letra "**P**" da primeira coluna, assim como as demais, numa matriz quadrada 26x26.

---

[1] **Análise de frequência** é um método empregado para decifrar mensagens criptografadas por meio da análise no texto codificado observando padrões que se repetem constantemente. Neste caso o criptoanalista (o quebrador de códigos) estuda a frequência com que certas letras aparecem no texto em função do idioma em que a mensagem foi escrita. Em Português as letras que mais aparecem nos textos são **"a"** e **"e"** (14.63% e 12.57%, respectivamente), e as que menos ocorrem: **"w"** e **"y"** (0.01%, ambas). Já no inglês, **"e"** é a letra mais frequente com 12.70% e a menos frequente é a letra **"z"** com 0.07%, de acordo com as informações pesquisadas no *link* https://pt.wikipedia.org/wiki/Frequ%C3%AAncia_de_letras (acesso em 26/12/2020 -12h50)

Continua com a "Cifra de Vigenère-2" (Parte 06)

0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Tabela CVI.1 - Grelha 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
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Tebala CVI.2 - Metodologia de Codificação com a Grelha de Vigenère

Mensagem	D	E	S	T	R	U	I	R	E	M	A	I	L	S	D	A	P	O	N	T	E				
Chave	P	I	X	U	L	E	C	O	P	I	X	U	L	E	C	O	P	I	X	U	L				
Cifragem	S	M	P	N	C	Y	K	F	T	U	X	C	W	W	F	O	E	W	K	N	P				

Quadro CVI.1 - Esquema de codificação/decodificação de Vigerère