

Criptografia: Parte 06 (Cifra de Vigenère-2)

Mário Leite

...

A **Parte 5** abordou a teoria geral do método da “Cifra de Vigenère” baseado num algoritmo de substituição *polialfabética*, trazendo mais segurança na proteção das mensagens. O programa “**ProgCifraVigenere**”, testado em Visualg, é uma aplicação simples e didática deste tipo de *codificação/decodificação*, baseado na álgebra do método, que pode ser resumida nas duas equações abaixo e considerando que as letras da grelha são numeradas de **0** (para A) até **25** (para Z) como foi mostrado na **tabela CVI.1** da **Parte 5**. Assim temos as duas seguintes expressões:

$$\begin{aligned} C_j &= (P_j + K_i) \bmod 26 && // \text{para cifrar} \\ P_j &= (C_j - K_i) \bmod 26 && // \text{para decifrar} \end{aligned}$$

j ==> índice da letra (variando de 0 a 25).

C_j ==> valor numérico do caractere de índice **j** da mensagem cifrada.

P_j ==> valor numérico do caractere de índice **j** da mensagem original.

K_j ==> valor numérico do caractere de índice **j** da chave.

A **tabela CVII.1** mostra um esquema de como seria aplicada a equação para **cifrar** a mensagem “DESTRUIREMAILSDAPONTE”, baseada nos índices de **0** a **25** das letras.

A **tabela CVII.2** mostra um esquema de como seria aplicada a equação para **decifrar** a mensagem cifrada “SMPNCYKFTUXCWWFOEWKNP”.

Observe na **tabela CVII.2** que, pela álgebra de Vigenère para decifragem $(C_j - K_j) \bmod 26$, algumas letras da mensagem original não deram certo (faixas sombreadas), pois a subtração nesses casos deu negativa e a expressão para decifrar não pode ser aplicada. Para resolver esses casos, deve-se adicionar **26** ao resultado da subtração; deste modo, a decifragem das letras ficaria assim, na sequência:

$(-8 + 26) \bmod 26$	$=$	18	(letra S)
$(-7 + 26) \bmod 26$	$=$	19	(letra T)
$(-9 + 26) \bmod 26$	$=$	17	(letra R)
$(-9 + 26) \bmod 26$	$=$	17	(letra R)
$(-18 + 26) \bmod 26$	$=$	8	(letra I)
$(-11 + 26) \bmod 26$	$=$	15	(letra P)
$(-13 + 26) \bmod 26$	$=$	13	(letra N)
$(-7 + 26) \bmod 26$	$=$	19	(letra T)

A **figura CVII.1** mostra a saída do programa “**ProgCifraVigenere**” para a opção **1** do menu: “**Apenas exibir a Grelha de Vigenère**”. As **figuras CVII.2** e **CVII.3** mostram as saídas do programa para a opção: “**Cifrar uma mensagem**”, respectivamente.

Continua com a “Cifra de Vigenère-3 (Parte 7)”

Letra Orig.	Valor Orig.	Letra Ch.	Valor Ch.	Soma	Soma mod 26	Letra cifrada
D	3	P	15	18	18	S
E	4	I	8	12	12	M
S	18	X	23	41	15	P
T	19	U	20	39	13	N
R	17	L	11	28	2	C
U	20	E	4	24	24	Y
I	8	C	2	10	10	K
R	17	O	14	31	5	F
E	4	P	15	19	19	T
M	12	I	8	20	20	U
A	0	X	23	23	23	X
I	8	U	20	28	2	C
L	11	L	11	22	22	W
S	18	E	4	22	22	W
D	3	C	2	5	5	F
A	0	O	14	14	14	O
P	15	P	15	30	4	E
O	14	I	8	22	22	W
N	13	X	23	36	10	K
T	19	U	20	39	13	N
E	4	L	11	15	15	P

Tabela CVII.1 - Esquema de Cifragem com a Álgebra de Vigenère

Letra Cifr.	Valor Cifr.	Letra Ch.	Valor Ch.	Subtração	Sub. mod 26	Letra Orig.
S	18	P	15	3	3	D
M	12	I	8	4	4	E
P	15	X	23	-8		
N	13	U	20	-7		
C	2	L	11	-9		
Y	24	E	4	20	20	U
K	10	C	2	8	8	I
F	5	O	14	-9		
T	19	P	15	4	4	E
U	20	I	8	12	12	M
X	23	X	23	0	03	A
C	2	U	20	-18		
W	22	L	11	11	11	L
W	22	E	4	18	18	S
F	5	C	2	3	3	D
O	14	O	14	0	0	A
E	4	P	15	-11		
W	22	I	8	13	14	O
K	10	X	23	-13		
N	13	U	20	-7		
P	15	L	11	4	4	E

Tabela CVII.2 - Decifrando a mensagem com a Álgebra de Vigenère

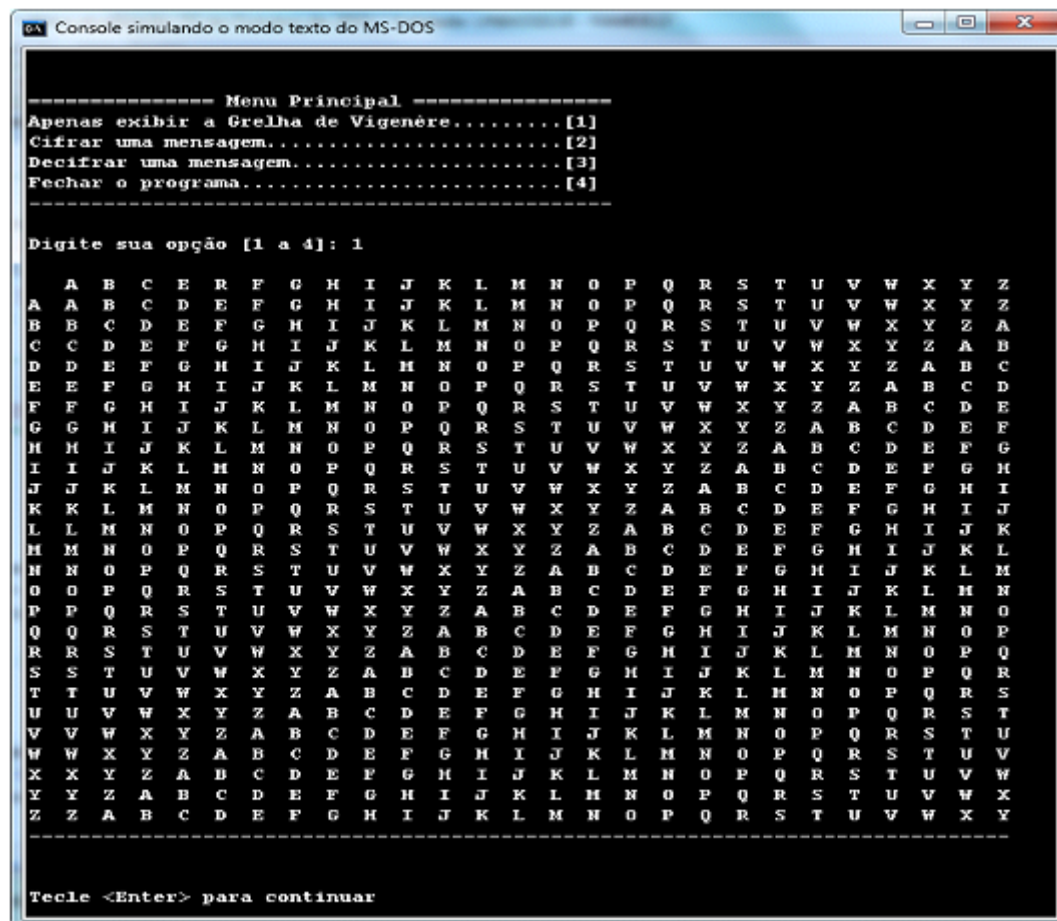
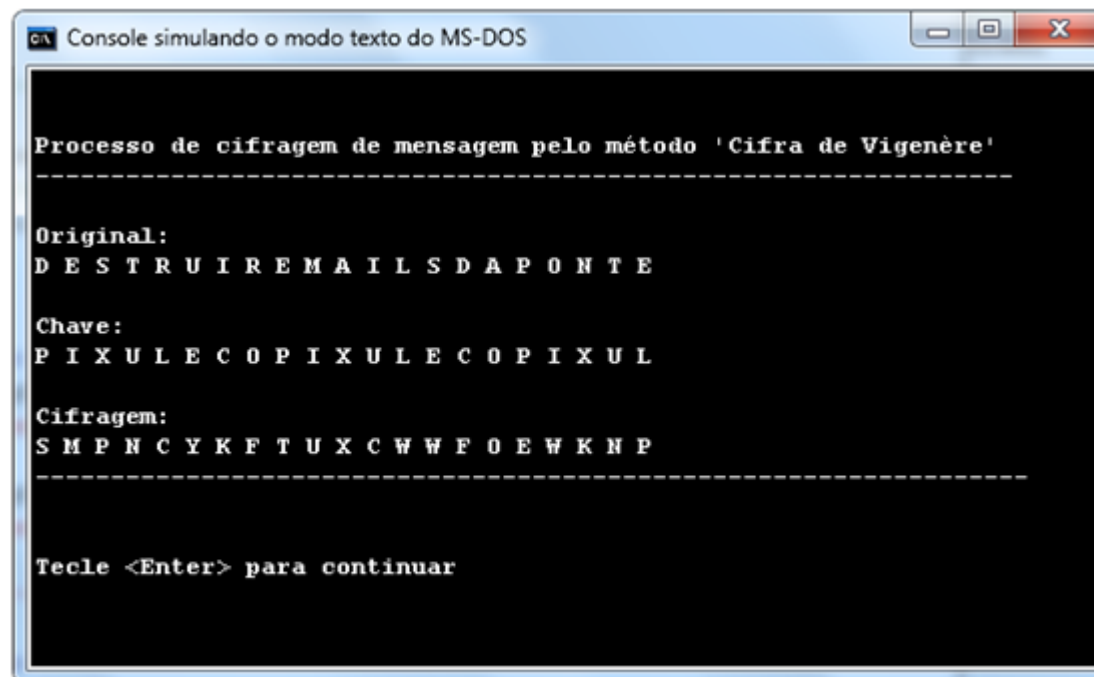


Figura CVII.1 - Opção 1 do menu para mostra a Grelha de Vigenère



Figura CVII.2 - Optando por cifrar a mensagem



```
CA Console simulando o modo texto do MS-DOS

Processo de cifração de mensagem pelo método 'Cifra de Vigenère'
-----

Original:
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

Cifração:
S M P N C Y K F T U X C W W F O E W K N P
-----

Tecle <Enter> para continuar
```

Figura CVII.3 - A mensagem cifrada