III Bienal da SBM – IME/UFG - 2006

A Criptografia Clássica no Ensino Médio

Theodoro Becker de Almeida*
Tiago Xavier Padilha*
Arthur de Oliveira Rodrigues*
Orientadora: Prof.ª Dr.ª Virgínia Maria Rodrigues*

Faculdade de Matemática – PUCRS - Porto Alegre, RS

Introdução

A necessidade de preservar informações consideradas sensíveis para um certo grupo e não permitir que estas fossem de conhecimento de grupos rivais, acompanhou o homem desde quando ele começou a viver em sociedade. A criptografia - do grego *kryptós*, escondido, e *gráphein*, escrever - é um conjunto de técnicas que permite escrever em "cifra" (ou "código") uma mensagem, de modo que somente o destinatário legítimo a compreenda.

Com base no baixo desempenho em matemática dos egressos do Ensino Médio, criar novas propostas para desenvolver os conteúdos é um desafio constante para os professores.

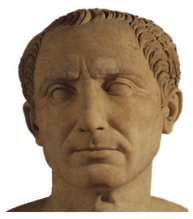
Alguns Códigos de Criptografia Clássica

Código de César

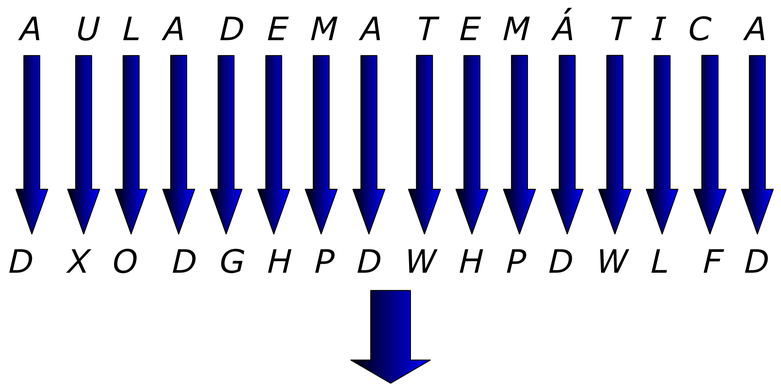
Nesta cifra cada letra do alfabeto é substituída por outra transladada algumas posições à frente. *(chave ↔ n.° de posições)*

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
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

Ex.:
Mensagem: AULA DE MATEMÁTICA
Chave K = 3



Caio Júlio César (101 a.C. - 44 a.C.) Hábil militar e político, teve uma vida marcada por importantes realizações, entre as quais, atribui-se ter sido o precursor na utilização de uma cifra monoalfbética.



MENSAGEM CODIFICADA:

DXODGHPDWHPDWLFD

Tabela Espartana

Baseia-se em um processo de "transposição": a mensagem é disposta nas linhas de uma tabela, que é transmitida por colunas, embaralhando as letras:

chave ↔ dim. da tabela

Ex.:
Mensagem: OFICINA DE CRIPTOGRAFIA
Chave C = 6x4

OFICINA DE CRIPTOGRAFIA

O	F	I	C
I	N	A	D
E	C	R	I
P	T	O	G
R	A	F	I
A	A	B	C

MENSAGEM CODIFICADA:

OIEPRAFNCTABIAROFCCDIGID

Cifra de Hill

O emissário corresponde números às letras, dispõe a mensagem em uma matriz que é multiplicada por outra (*matriz-chave*), e envia o resultado dessa multiplicação, linha por linha.

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Ex.:
Mensagem M: ESTOU NA ESCOLA

Chave C = $\begin{bmatrix} 1 & 2 & 3 & 0 \\ 2 & 3 & 2 & 1 \\ 0 & 0 & 1 & 2 \\ 1 & 2 & 3 & 1 \end{bmatrix}$

E S T O U N A E S C O L A

5 19 20 15 21 14 1 5 19 3 15 12 1

M = $\begin{bmatrix} 5 & 19 & 20 & 15 \\ 21 & 14 & 1 & 5 \\ 19 & 3 & 15 & 12 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ → **MC =** $\begin{bmatrix} 58 & 97 & 118 & 74 \\ 54 & 94 & 107 & 21 \\ 37 & 71 & 114 & 45 \\ 1 & 2 & 3 & 0 \end{bmatrix}$

Envia-se as linhas da matriz *MC*.

MENSAGEM CODIFICADA:

58 97 118 74 54 94 107 21 37 71 114 45 1 2 3 0

OFICINA REALIZADA PARA ALUNOS DO ENSINO MÉDIO, DIA 06 DE OUTUBRO DE 2006, NO COLÉGIO ESTADUAL INÁCIO MONTANHA (PORTO ALEGRE , RS)

Alguns comentários dos alunos:

"A Oficina me ajudou muito a melhorar minha aprendizagem sobre matrizes."

"Achei ótimo pois vi uma aplicação de matrizes na Criptografia."

"Me ajudou porque sempre tive dificuldades em multiplicar matrizes e achar inversas."

Conclusão

Observamos que a criptografia apresenta uma aplicação de tópicos de matemática que permitem que ela seja explorada no Ensino Médio. Em particular, atividades utilizando os códigos acima poderiam ser realizadas em sala de aula ao trabalhar-se com matrizes.

Referências
[1] C. J. Costa e L.M.S Figueiredo,*Criptografia Geral* (Curso de Criptografia e Segurança em Redes). Rio de Janeiro: UFF/CEP, 2005.
[2] D. Kahn, *The Codebreakers.* Macmillan Publishing Company, New York, 1967.
[3] A. J. Menezes, *et al, Handbook of Applied Cryptography.*CRC Press, 1997.
[4] S. Singh, *O Livro dos Códigos.* Rio de Janeiro, Record, 2001.
[5] D. R. Stinson, *Cryptography: Theory and Practice.* CRC Press, 1995.

[*] E-mails: beckerdealmeida@yahoo.com.br, tiago_pucrs@yahoo.com.br, arthur.rodrigues@hotmail.com, virginia@pucrs.br