Aplicação à Criptografia

Reginaldo J. Santos
Departamento de Matemática-ICEx
Universidade Federal de Minas Gerais
http://www.mat.ufmg.br/~regi

12 de maio de 2004

	a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
o	p	q	r	s	t	u	v	w	x	y	z	à	á	â
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
ã	ç	é	ê	í	ó	ô	õ	ú	ü	A	B	C	D	E
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
U	V	W	X	Y	Z	À	Á	Â	Ã	Ç	É	Ê	Í	Ó
60	61	62	63	64	65	66	67	68	69	70	71	72	73	74
Ô	Õ	Ú	Ü	0	1	2	3	4	5	6	7	8	9	:
75	76	77	78	79	80	81	82	83	84	85	86	87	88	89
;	<	=	>	?	@	!	"	#	$	%	&	’	(	)
90	91	92	93	94	95	96	97	98	99	100	101	102	103	104
*	+	,	-	.	/	[	\	]	_	{	|	}		
105	106	107	108	109	110	111	112	113	114	115	116	117		

Tabela 1: Tabela de conversão de caracteres em números

Exemplo 1. Vamos transformar uma mensagem em uma matriz da seguinte forma. Vamos quebrar a mensagem em pedaços de tamanho 3 e cada pedaço será convertido em

uma matriz coluna usando a Tabela 1 de conversão entre caracteres e números.

Considere a seguinte mensagem criptografada

```
1ydobbr,?
```
(1)

Quebrando a mensagem criptografada em pedaços de tamanho 3 e convertendo cada pedaço para uma coluna de números usando a Tabela 1 obtemos a matriz

$$Y = \begin{bmatrix} 80 & 15 & 18 \\ 25 & 2 & 107 \\ 4 & 2 & 94 \end{bmatrix}$$

Sabendo-se que esta mensagem foi criptografada fazendo o produto da mensagem inicial pela matriz

$$M = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

então

$$X = M^{-1}Y$$

será a mensagem inicial convertida para números, ou seja,

$$X = M^{-1}Y = \begin{bmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 80 & 15 & 18 \\ 25 & 2 & 107 \\ 4 & 2 & 94 \end{bmatrix} = \begin{bmatrix} 59 & 15 & 5 \\ 21 & 0 & 13 \\ 4 & 2 & 94 \end{bmatrix}$$

Convertendo para texto usando novamente a Tabela 1 obtemos que a mensagem que foi criptografada é

```
Tudo bem?
```
(2)

Referências

[1] Reginaldo J. Santos. *Um Curso de Geometria Analítica e Álgebra Linear*. Imprensa Universitária da UFMG, Belo Horizonte, 2003.