Lista de Revisão de Criptografia, Matrizes e Sistemas[1]

1.6 Criptografia com Matrizes

Sejam A e B matrizes 2×2, onde B é a matriz inversa de A. [Dúvidas sobre matrizes? Este capítulo tem um apêndice que pode lhe ajudar! Veja na página 13]

$$A = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} \text{ e } B = \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix}$$

Vamos utilizar essas duas matrizes como "chaves" para codificar e decodificar a mensagem. O remetente vai usar a matriz A para codificar a mensagem e o destinatário vai usar a matriz B para decodificar a mensagem. O primeiro passo para codificar uma mensagem é convertê-la da forma alfabética para uma forma numérica. Então vamos utilizar a tabela abaixo:

Valores para as letras

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P	Q	R	S	T	U	V	X	W	Y	Z	.	!	#	
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

O remetente e o destinatário devem conhecer essa tabela de valores. Lembramos que esses valores são arbitrários e, desde que sejam combinados entre o remetente e o destinatário, podem assumir quaisquer valores. Vamos fazer um exemplo com a frase:"Eu acredito na educação."

1º Passo: Vamos fazer a correspondência entre as letras e os números usando a tabela dada.

E	U	#	A	C	R	E	D	I	T	O	#	N	A	#	E	D	U	C	A	Ç	A	O	.
5	21	29	1	3	18	5	4	9	20	15	29	14	1	29	5	4	21	3	1	3	1	15	27

Usamos o símbolo # entre as palavras para não gerar confusão. Como temos a matriz decodificadora A de ordem 2×2, vamos colocar a sequência de números dispostos em uma matriz de duas linhas. Se o número de elementos da mensagem for ímpar, podemos acrescentar um caracter vazio (não vai alterar a mensagem). No caso o número 30.

$$M = \begin{bmatrix} 5 & 21 & 29 & 1 & 3 & 18 & 5 & 4 & 9 & 20 & 15 & 29 \\ 14 & 1 & 29 & 5 & 4 & 21 & 3 & 1 & 3 & 1 & 15 & 27 \end{bmatrix}$$

2º Passo: Agora temos que codificar a mensagem, para que possamos enviá-la. Para fazer isso basta multiplicar a matriz A pela M tal que A.M=N.

$$\begin{aligned} N &= \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 5 & 21 & 29 & 1 & 3 & 18 & 5 & 4 & 9 & 20 & 15 & 29 \\ 14 & 1 & 29 & 5 & 4 & 21 & 3 & 1 & 3 & 1 & 15 & 27 \end{bmatrix} \\ &= \begin{bmatrix} 29 & 64 & 116 & 8 & 13 & 75 & 18 & 13 & 30 & 61 & 60 & 114 \\ 24 & 43 & 87 & 7 & 10 & 57 & 13 & 9 & 21 & 41 & 45 & 85 \end{bmatrix} \end{aligned}$$

1 O texto utilizado é oriundo do Programa PET-UFPR (Prof. Alexandre Kirilov)

Assim temos os elementos de N que constituem a mensagem criptografada.

3º Passo: Quando o destinatário receber a mensagem N codificada ele terá que usar a matriz B para decodificar e obter a matriz original, e então poder ler a mensagem. Multiplicando a matriz B por N:

$$\begin{aligned} B.N &= \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix} . \begin{bmatrix} 29 & 64 & 116 & 8 & 13 & 75 & 18 & 13 & 30 & 61 & 60 & 114 \\ 24 & 43 & 87 & 7 & 10 & 57 & 13 & 9 & 21 & 41 & 45 & 85 \end{bmatrix} \\ &= \begin{bmatrix} 5 & 21 & 29 & 1 & 3 & 18 & 5 & 4 & 9 & 20 & 15 & 29 \\ 14 & 1 & 29 & 5 & 4 & 21 & 3 & 1 & 3 & 1 & 15 & 27 \end{bmatrix} = M \end{aligned}$$

Agora é só reverter os números da matriz B.N para conseguir a sua mensagem:

5	21	29	1	3	18	5	4	9	20	15	29	14	1	29	5	4	21	2	1	3	1	15	27
E	U	#	A	C	R	E	D	I	T	O	#	N	A	#	E	D	U	C	A	Ç	A	O	.

Note que na mensagem inicial revertida em números tem várias repetições de números, enquanto que a mensagem codificada não contém números repetidos, tornando-a mais difícil de ser desvendada. O que precisa ser escondido são apenas as matrizes A e B.

A seguir faremos mais um exemplo, dessa vez com uma matriz A 3×3. Vamos usar a matriz A e a inversa dela B como:

$$A = \begin{bmatrix} 3 & 1 & 2 \\ 2 & 1 & -1 \\ 3 & 1 & 3 \end{bmatrix} \text{ e } B = \begin{bmatrix} 4 & -1 & -3 \\ -9 & 3 & 7 \\ -1 & 0 & 1 \end{bmatrix}$$

Vamos usar a frase "The plot thickens" que em português significa "Entrou areia". Agora seguiremos o mesmo processo da frase anterior.

1º Passo: Consultando a tabela "Valores para as letras" podemos converter a nossa frase em números e arranjá-la em uma matriz 6×3.

$$M = \begin{bmatrix} 20 & 8 & 5 & 29 & 16 & 12 \\ 15 & 20 & 29 & 20 & 8 & 9 \\ 3 & 11 & 5 & 14 & 19 & 30 \end{bmatrix}$$

2º Passo: Para codificar a mensagem multiplicaremos a matriz M pela A, assim temos N = A.M

$$\begin{aligned} N &= \begin{bmatrix} 3 & 1 & 2 \\ 2 & 1 & -1 \\ 3 & 1 & 3 \end{bmatrix} . \begin{bmatrix} 20 & 8 & 5 & 29 & 16 & 12 \\ 15 & 20 & 29 & 20 & 8 & 9 \\ 3 & 11 & 5 & 14 & 19 & 30 \end{bmatrix} \\ &= \begin{bmatrix} 81 & 66 & 54 & 135 & 94 & 105 \\ 52 & 25 & 34 & 64 & 21 & 3 \\ 84 & 77 & 59 & 149 & 113 & 135 \end{bmatrix} \end{aligned}$$

Assim temos a nossa matriz N com a mensagem criptografada.

3º Passo: Para decodificar vamos multiplicar a nossa matriz B com a matriz N para conseguirmos a matriz M com a mensagem original.

$$B.N = \begin{bmatrix} 4 & -1 & -3 \\ -9 & 3 & 7 \\ -1 & 0 & 1 \end{bmatrix} . \begin{bmatrix} 81 & 66 & 54 & 135 & 94 & 105 \\ 52 & 25 & 34 & 64 & 21 & 3 \\ 84 & 77 & 59 & 149 & 113 & 135 \end{bmatrix}$$

$$= \begin{bmatrix} 20 & 8 & 5 & 29 & 16 & 12 \\ 15 & 20 & 29 & 20 & 8 & 9 \\ 3 & 11 & 5 & 14 & 19 & 30 \end{bmatrix} = M$$

Exercício 1. Determine as matrizes nos casos abaixo:

a) $\begin{bmatrix} 3 & 0 & 4 \\ 0 & -2 & 2 \\ 0 & -6 & 3 \end{bmatrix} + \begin{bmatrix} 1 & 2 & 3 \\ -5 & 0 & 6 \\ -7 & 1 & 13 \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$

b) $\begin{bmatrix} 3 & 2 & 4 \\ 0 & -2 & 5 \\ 1 & -6 & 8 \end{bmatrix} + \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} 4 & 4 & 7 \\ 4 & -6 & 11 \\ 8 & -5 & 17 \end{bmatrix}$

c) $\begin{bmatrix} 0 & 0 & -5 \\ 2 & -2 & 12 \\ 9 & -6 & 6 \end{bmatrix} - \begin{bmatrix} 10 & -2 & 3 \\ 5 & 0 & -6 \\ -7 & 11 & 3 \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$

d) $\begin{bmatrix} 0 & 9 & 2 \\ 0 & -2 & 5 \\ -1 & -1 & 5 \end{bmatrix} - \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} 1 & -4 & 0 \\ -4 & -6 & 11 \\ 2 & -4 & 16 \end{bmatrix}$

Exercício 2. Codifique/decodifique as mensagens abaixo:

Usando a matriz $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ codifique a palavra SHERLOCK.

Usando a matriz B$= \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}$ codifique a palavra WATSON.

Utilizando a matriz C$= \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix}$ decodifique a mensagem 52, 64, 40, 43.

Exercício 3. Quando possível, calcule:

a) AB b) BA c) CD d) DC e) AD f) BC

Dados $A = \begin{bmatrix} 1 & 5 \\ 1 & 2 \\ 2 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 2 & 1 \\ 3 & 2 & 1 \end{bmatrix}$, $C = \begin{bmatrix} 2 & 5 \\ 5 & 2 \end{bmatrix}$, e $D = \begin{bmatrix} 1 & 2 \\ 4 & 2 \end{bmatrix}$

Exercício 4. Quando possível, determine a matriz inversa de:

a) $A = \begin{pmatrix} 1 & 3 \\ 2 & 7 \end{pmatrix}$ b) $B = \begin{pmatrix} 2 & 5 & -1 \\ 4 & -1 & 2 \\ 0 & 4 & 1 \end{pmatrix}$ c) $C = \begin{pmatrix} 1 & -1 & 2 \\ 3 & 2 & -4 \\ 0 & 1 & -2 \end{pmatrix}$

Exercício 5. Calcule:

a) $2.\begin{bmatrix} 1 & -9 \\ 7 & 2 \end{bmatrix} + 3.\begin{bmatrix} 1 & -9 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

b) $-5.\begin{bmatrix} 1 & 0 \\ 6 & 2 \end{bmatrix} - 3.\begin{bmatrix} 2 & -9 \\ 0 & -2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

Exercício 6. Utilizando matrizes, resolva:

a) $\begin{cases} 2x + y - 2z = 10 \\ 3x + 2y + 2z = 1 \\ 5x + 4y + 3z = 4 \end{cases}$ b) $\begin{cases} x + 2y - z = 0 \\ 2x - y + 3z = 0 \\ 4x + 3y + z = 0 \end{cases}$

d) $\begin{cases} x + y + z = 4 \\ 2x + 5y - 2z = 3 \\ x + 7y - 7z = 5 \end{cases}$ e) $\begin{cases} x - 2y + 3z = 0 \\ 2x + 5y + 6z = 0 \end{cases}$