Criptografia

O estudo da codificação e decodificação de mensagens secretas é denominado **Criptografia**. Os có secretos foram bastante utilizados nas guerras, para transmitir mensagens sem que o inimigo conseg compreendê-las. Hoje em dia há um grande interesse no assunto, devido a necessidade de se trans informações privadas em vias públicas de comunicação, como a internet.

As **cifras** são os códigos usados para transformar um texto comum em um texto cifrado. O proces converter um texto comum em cifrado é chamado **cifrar** ou **codificar**, e o processo inverso é cha **decifrar** ou **decodificar**.

Vamos estudar as chamadas **cifras de Hill** que são baseadas em transformações matriciais. Para utilizaremos a aritmética modular e conceitos da Álgebra Linear, mais especificamente: matrizes, elimir Gaussiana, dependência linear e transformações lineares.

Aritmética Modular

Definição: Dados um número inteiro positivo m e dois inteiros a e b quaisquer, dizemos que **equivalente a** b **módulo m**, e escrevemos:

$$a = b \ \ (mod\ m)$$

se $a - b$ é um múltiplo inteiro de m.

Dado um módulo m, qualquer inteiro a é equivalente, módulo m, a um dos inteiros do conjunto:

$$Z_m = \{0, 1, 2, \ldots, m-1\}$$

denominado conjunto dos **resíduos** de a módulo m.

Teorema: *Dados um inteiro a e um módulo m. Seja R o resto da divisão de $|a|$ por m. Então, o resíd de a módulo m é dado por:*

$$r = \begin{cases} R & se \quad a \geq 0 \\ m - R & se \quad a < 0 \ \ e \ \ R \neq 0 \\ 0 & se \quad a < 0 \ \ e \ \ R = 0 \end{cases}$$

Definição: Dado um número a em Z_m. Dizemos que $a^{-1} \in Z_m$ é o **inverso multiplicativo** de a módu se a $a^{-1} = a^{-1}a = 1\ (mod\ m)$.

Podemos mostrar que se a e m não têm fatores primos comuns, então a tem um único inverso multiplic módulo m. E se a e m têm fatores primos comuns, então a não possui inverso multiplicativo módulo m. disso, se m for primo, então todo $a \in Z_m$ tem único inverso multiplicativo em Z_m.

Com estas definições e resultados, podemos operar com os elementos de Z_m, no que denomin **aritmética modular**, que utilizaremos mais adiante para estudar a codificação e decodificação das cifr Hill.

Exemplo 1: $4 = 0\ (mod\ 2)$, *pois* $4 - 0 = 4$ *é um múltiplo inteiro de* 2.

Exemplo 2: $-2 = 24\ (mod\ 26)$, *pois* $-2 - 24 = -26$ *é um múltiplo inteiro de* 26.

Exemplo 3: *O resíduo módulo* 26 *de* 103 *é* 25.
Dividindo $|103| = 103$ por 26, obtemos um resto R = 25, ou seja, $r = 25$. Assim, $103 = 25\ (mod\ 26$

Exemplo 4: *O resíduo módulo* 26 *de* -64 *é* 14.
Dividindo $|-64| = 64$ por 26, obtemos um resto R = 12. Como $-64 < 0$, temos, $r = 26 - 12 =$
Assim, $-64 = 14\ (mod\ 26)$.

Exemplo 5: $1 + 1 = 0\ (mod\ 2)$.
Na aritmética comum, temos $1 + 1 = 2$. Mas dividindo 2 por 2, obtemos resto 0, ou seja, $2 = 0\ (mo$
Assim, na aritmética módulo 2, temos $1 + 1 = 0\ (mod\ 2)$.

Exemplo 6: 15 *é inverso multiplicativo de* 7 *módulo* 26, *pois* $7 \times 15 = 105 = 1\ (mod\ 26)$.

Jogos de Estratégia
Classificação de Cônicas

Voltar ao Topo.

Cifras de Hill

Uma maneira de tornar o código mais difícil de ser quebrado é dividir o texto em grupos e criptogra texto comum por grupos. Um **sistema poligráfico** é um sistema de criptografia no qual o texto é separad conjuntos de n letras, cada qual é substituído por um conjunto de n letras cifradas. As **cifras de Hill** são classe de sistemas poligráficos, baseados em transformações matriciais.

Vamos numerar cada letra do alfabeto de 1 a 25, e ao Z daremos o valor 0. Cada letra estará determinada por seu número correspondente.

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

No caso mais simples da cifra de Hill, vamos dividir o texto comum em pares de letras e codificá-lo at do seguinte procedimento:

1º) Escolhemos uma matriz 2×2 com entradas inteiras:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

A é denominada **matriz codificadora**.

2º) Dividimos o texto que queremos codificar em pares de letras. Caso o texto tenha um número ímp letras, adicionamos no final uma letra fictícia.

3º) Substituímos cada letra por seu número correspondente. Escrevemos cada par de números p_1 e p_2 (um vetor coluna:

$$p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

Obtemos então os vetores $q = Ap$ cifrados.

4º) Por fim, substituímos cada número dos vetores cifrados q, por suas letras equivalentes. Caso a número do vetor q não pertença ao conjunto Z_{26}, ou seja, não esteja entre 0 e 25, obtemos o seu equiva módulo 26, que esteja em Z_{26}, para podermos substituí-los por suas letras correspondentes. Assim, juntan letras de cada par cifrado, teremos o texto codificado.

Nesse caso mais simples, no qual separamos o texto comum em pares de letras, teremos uma 2-cifra de Em casos mais gerais de uma
n-cifra de Hill, basta separarmos o texto em grupos de n letras e escolher no 1º passo uma matriz codific: $n \times n$.

Exemplo: *Vamos codificar o seguinte texto: ALGEBRA LINEAR, utilizando uma 2-cifra de Hill, c seguinte matriz codificadora:*

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}$$

Primeiramente separamos o texto em pares de letras, da forma:

$$AL \;\; GE \;\; BR \;\; AL \;\; IN \;\; EA \;\; R$$

Como temos um número ímpar de letras, completamos o último par com uma letra fictícia qualquer:

$$AL \;\; GE \;\; BR \;\; AL \;\; IN \;\; EA \;\; RZ$$

Substituímos então cada letra por seu correspondente numérico:

$$1\,12 \quad 7\,5 \quad 2\,18 \quad 1\,12 \quad 9\,14 \quad 5\,1 \quad 18\,0$$

Escrevemos cada par de números como um vetor coluna p e obtemos os vetores cifrados q, da fo
$q = Ap$. Para o par AL, teremos:

$$\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ 12 \end{bmatrix} = \begin{bmatrix} 25 \\ 63 \end{bmatrix}$$

Neste caso, o número 63 não está entre 0 e 25 e não podemos substituí-lo por sua letra correspond
Assim, obtemos o seu equivalente módulo 26, que esteja em Z_{26}.

Dividindo $|63| = 63$ por 26, obtemos um resto R = 11, assim, $63 = 11\ (mod\ 26)$. Dessa forma, obten
vetor cifrado do par de letras AL:

$$q = \begin{bmatrix} 25 \\ 63 \end{bmatrix} = \begin{bmatrix} 25 \\ 11 \end{bmatrix} (mod\ 26)$$

Substituindo pelas letras correspondentes, obtemos o par cifrado: YK. Fazendo o mesmo para os de
pares de letras, teremos:

$$\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 5 \end{bmatrix} = \begin{bmatrix} 17 \\ 46 \end{bmatrix} = \begin{bmatrix} 17 \\ 20 \end{bmatrix} (mod\ 26)$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 2 \\ 18 \end{bmatrix} = \begin{bmatrix} 38 \\ 96 \end{bmatrix} = \begin{bmatrix} 12 \\ 18 \end{bmatrix} (mod\ 26)$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ 12 \end{bmatrix} = \begin{bmatrix} 25 \\ 63 \end{bmatrix} = \begin{bmatrix} 25 \\ 11 \end{bmatrix} (mod\ 26)$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 9 \\ 14 \end{bmatrix} = \begin{bmatrix} 37 \\ 97 \end{bmatrix} = \begin{bmatrix} 11 \\ 19 \end{bmatrix} (mod\ 26)$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 5 \\ 1 \end{bmatrix} = \begin{bmatrix} 7 \\ 20 \end{bmatrix} = \begin{bmatrix} 7 \\ 20 \end{bmatrix} (mod\ 26)$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 18 \\ 0 \end{bmatrix} = \begin{bmatrix} 18 \\ 54 \end{bmatrix} = \begin{bmatrix} 18 \\ 2 \end{bmatrix} (mod\ 26)$$

Portanto, obtemos os respectivos pares de letras cifrados: QT, LR, YK, KS, GT, RB. A
juntando todos os pares de texto codificados, teremos a mensagem codificada:

$$YWQTLRYKKSGTRB$$

Voltar ao Topo.

Inversa de uma matriz módulo m

Para conseguir decodificar uma cifra de Hill, iremos usar a inversa módulo 26 da matriz A codifica
Usamos o número 26 pois estamos trabalhando apenas com as 26 letras do alfabeto, caso se queira ut
acentuações e pontuação, por exemplo, seria necessário trabalhar com outro módulo e seguir os me

passos.

Definição: Seja m um inteiro positivo. Dizemos que uma matriz A, com entradas em Z_m, é **invertív** existir uma matriz B, com entradas em Z_m, tal que:

$$AB = BA = I\ (mod\ m)$$

B é a matriz **inversa** de A módulo m, que denotamos por $A^{-1}\ (mod\ m)$. Dizer que uma matriz est módulo m significa que cada uma das suas entradas está em módulo m.

Teorema: *Uma matriz quadrada A com entradas em Z_m possui inversa módulo m, se e soment $det(A)\ (mod\ m)$ possui inverso multiplicativo módulo m.*

Com isso, podemos determinar quais as matrizes quadradas que são invertíveis em Z_m, para qualqu Isso nos ajuda pois ao codificar algum texto é preciso que a pessoa que receba a mensagem seja cap decifrá-la, caso contrário o texto ficaria para sempre codificado e não transmitiria nenhuma informação. podermos decifrar o código, no primeiro passo da codificação precisamos escolher uma matriz A que invertível.

Teorema: *Seja*Math input error

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

uma matriz 2×2 com entradas em Z_m, invertível módulo m, isto é, $det(A)\ (mod\ m)$ possui in multiplicativo módulo m. Então a inversa de A módulo m é:

$$A^{-1} = det(A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Onde $det(A)^{-1}$ é o inverso multiplicativo módulo m do determinante de A.

Esse teorema nos dá um meio para calcular a inversa módulo m de uma matriz 2×2, que pa propósitos desta aplicação é suficiente. O cálculo de inversas de matrizes de ordem maior envolveria o cálculos e definições, que não faremos aqui.

Exemplo: *Calcule a inversa módulo* 26 *da matriz:*

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}$$

Temos que $det(A) = 5 - 6 = -1 = 25\ (mod\ 26)$. O determinante de A módulo 26, portanto, p inverso multiplicativo módulo 26. Temos: $25 \times 25 = 625 = 1\ (mod\ 26)$. Logo, 25 é o inverso multiplic de 25 módulo 26. Assim, a inversa de A módulo 26 é dada por:

$$A^{-1} = 25 \begin{bmatrix} 5 & -2 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} 125 & -50 \\ -75 & 25 \end{bmatrix} = \begin{bmatrix} 21 & 2 \\ 3 & 25 \end{bmatrix} (mod\ 26)$$

Voltar ao Topo.

Decodificação de uma Cifra de Hill

Suponha que recebemos um texto cifrado e conhecemos a matriz codificadora de uma 2-cifra de Hill:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

que deve ser invertível módulo 26.

Se p é um vetor com os correspondentes numéricos de um par de letras de texto comum, sabemos pela de codificação que os vetores q, de correspondentes numéricos dos pares de letras cifradas, são obtid forma:

$$q = Ap$$

Assim, podemos dividir o texto cifrado que conhecemos em pares de letras, substituí-los por correspondentes numéricos, escrever cada vetor coluna q e por fim obter os correspondentes vetores forma:

$$p = A^{-1}q$$

Onde, nesse caso, A^{-1} é a inversa módulo 26 de A. Substituindo cada número dos vetores p por suas correspondentes, conseguimos decifrar qual é a mensagem.

Exemplo: *Suponha que recebemos a mensagem: LQPQEECWBY, que foi criptografada por uma* 2*-cif Hill, com a seguinte matriz codificadora:*

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

Vamos obter a mensagem decodificada.

Para isso, vamos obter a matriz inversa módulo 26 da matriz A. Efetuando os cálculos, temos:

$$A^{-1} = \begin{bmatrix} 9 & 0 \\ 8 & 1 \end{bmatrix} \; (mod\ 26)$$

Separamos o texto cifrado em pares de letras, da forma:

$$LQ \;\; PQ \;\; EE \;\; CW \;\; BY$$

E substituindo cada letra por seu correspondente numérico, teremos:

12 17   16 17   5 5   3 23   2 25

Escrevemos cada par de números como um vetor q e obtemos os correspondentes vetores de texto com em módulo 26, da forma: $p = A^{-1}q$. Teremos:

$$\begin{bmatrix} 9 & 0 \\ 8 & 1 \end{bmatrix} \begin{bmatrix} 12 \\ 17 \end{bmatrix} = \begin{bmatrix} 108 \\ 113 \end{bmatrix} = \begin{bmatrix} 4 \\ 9 \end{bmatrix} \; (mod\ 26)$$

$$\begin{bmatrix} 9 & 0 \\ 8 & 1 \end{bmatrix} \begin{bmatrix} 12 \\ 17 \end{bmatrix} = \begin{bmatrix} 108 \\ 113 \end{bmatrix} = \begin{bmatrix} 4 \\ 9 \end{bmatrix} \; (mod\ 26)$$

$$\begin{bmatrix} 9 & 0 \\ 8 & 1 \end{bmatrix} \begin{bmatrix} 16 \\ 17 \end{bmatrix} = \begin{bmatrix} 144 \\ 145 \end{bmatrix} = \begin{bmatrix} 14 \\ 15 \end{bmatrix} \; (mod\ 26)$$

$$\begin{bmatrix} 9 & 0 \\ 8 & 1 \end{bmatrix} \begin{bmatrix} 5 \\ 5 \end{bmatrix} = \begin{bmatrix} 45 \\ 45 \end{bmatrix} = \begin{bmatrix} 19 \\ 19 \end{bmatrix} \; (mod\ 26)$$

$$\begin{bmatrix} 9 & 0 \\ 8 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 23 \end{bmatrix} = \begin{bmatrix} 27 \\ 47 \end{bmatrix} = \begin{bmatrix} 1 \\ 21 \end{bmatrix} \; (mod\ 26)$$

$$\begin{bmatrix} 9 & 0 \\ 8 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 25 \end{bmatrix} = \begin{bmatrix} 18 \\ 41 \end{bmatrix} = \begin{bmatrix} 18 \\ 15 \end{bmatrix} (mod\ 26)$$

Assim, substituindo cada número, dos pares de vetores p obtidos, por suas letras correspondentes, obt os pares de letras de texto comum:

$$DI \;\; NO \;\; SS \;\; AU \;\; RO$$

Juntando os pares de letras, descobrimos que a palavra codificada era: DINOSSAURO.

Suponha agora, que recebemos um texto cifrado e sabemos uma parte do texto decodificado. Vamos ut conceitos da Álgebra Linear e eliminação Gaussiana para obter a matriz decodificadora A^{-1}. Da Ál Linear, sabemos que uma transformação fica bem determinada por seu efeito nos elementos de uma base. esse princípio, teremos o seguinte teorema:

Teorema: *Sejam $p_1, \dots, p_n$ vetores de texto comum, linearmente independentes, e $q_1, \dots, q$ correspondentes vetores cifrados de uma*
n-cifra de Hill. Seja:

$$P = \begin{bmatrix} p_1^t \\ \vdots \\ p_n^t \end{bmatrix}$$

a matriz $n \times n$ de vetores linha $p_1, \dots, p_n$ transpostos. E seja:

$$Q = \begin{bmatrix} q_1^t \\ \vdots \\ q_n^t \end{bmatrix}$$

a matriz $n \times n$ de vetores linha $q_1, \dots, q_n$ transpostos. Então, as operações elementares de linha reduzem Q a matriz identidade I_n, transforma P na matriz $(A^{-1})^t$, sendo A^{-1} a matriz decodificadora.

Assim, para encontrar a transposta da matriz decodificadora A^{-1}, basta sabermos uma sequênc operações elementares de linha que reduzem Q a I_n e aplicarmos essas operações na matriz P.

Exemplo 1: *Suponha que recebemos a mensagem criptografada BEWIXSMFNC e sabemos apenas q texto original começa com a palavra MOVA. Vamos obter a mensagem decodificada.*

Separamos o texto comum conhecido em pares de letras e substituímos por seu equivalente numérico:

$$\begin{matrix} MO & VA \\ 13\ 15 & 22\ 1 \end{matrix}$$

Fazemos o mesmo com o correspondente texto cifrado:

$$\begin{matrix} BE & WI \\ 2\ 5 & 23\ 9 \end{matrix}$$

De modo que os vetores p de texto comum e seus correspondentes vetores cifrados q são:

$$p_1 = \begin{bmatrix} 13 \\ 15 \end{bmatrix}, \quad q_1 = \begin{bmatrix} 2 \\ 5 \end{bmatrix}$$

$$p_2 = \begin{bmatrix} 22 \\ 1 \end{bmatrix}, \quad q_2 = \begin{bmatrix} 23 \\ 9 \end{bmatrix}$$

Queremos reduzir a matriz

$$Q = \begin{bmatrix} q_1^t \\ q_2^t \end{bmatrix} = \begin{bmatrix} 2 & 5 \\ 23 & 9 \end{bmatrix}$$

a matriz identidade de ordem 2, aplicando operações elementares de linhas, e simultaneamente, aplicar mesmas operações na matriz

$$P = \begin{bmatrix} p_1^t \\ p_2^t \end{bmatrix} = \begin{bmatrix} 13 & 15 \\ 22 & 1 \end{bmatrix}$$

obtendo assim a matriz $(A^{-1})^t$. Isso pode ser feito juntando P à direita de Q e aplicando as opera elementares de linhas na matriz resultante $[Q|P]$ até que o lado esquerdo seja reduzido a matriz I_2. A matr lado direito será a que queremos.

$$\begin{bmatrix} 2 & 5 & 13 & 15 \\ 23 & 9 & 22 & 1 \end{bmatrix} \to l_1 \leftrightarrow l_2 \to \begin{bmatrix} 23 & 9 & 22 & 1 \\ 2 & 5 & 13 & 15 \end{bmatrix} \to multiplicamos\ a\ linha\ 1\ por\ 23^{-1} = 17\ (mod\ 2$$

$$\to \begin{bmatrix} 1 & 153 & 374 & 17 \\ 2 & 5 & 13 & 15 \end{bmatrix} \to substituímos\ cada\ entrada\ da\ matriz\ por\ seu\ equivalente\ módulo\ 26$$

$$\to \begin{bmatrix} 1 & 23 & 10 & 17 \\ 2 & 5 & 13 & 15 \end{bmatrix} \to l_2 \leftrightarrow l_2 - 2l_1 \to \begin{bmatrix} 1 & 23 & 10 & 17 \\ 0 & -41 & -7 & -19 \end{bmatrix} \to mod\ 26 \to \begin{bmatrix} 1 & 23 & 10 & 17 \\ 0 & 11 & 19 & 7 \end{bmatrix} \to$$

$$\to multiplicamos\ a\ linha\ 2\ por\ 11^{-1} = 19\ (mod\ 26) \to \begin{bmatrix} 1 & 23 & 10 & 17 \\ 0 & 1 & 361 & 133 \end{bmatrix} \to mod\ 26 \to$$

$$\to \begin{bmatrix} 1 & 23 & 10 & 17 \\ 0 & 1 & 23 & 3 \end{bmatrix} \to l_1 \leftrightarrow l_1 - 23l_2 \to \begin{bmatrix} 1 & 0 & -519 & -52 \\ 0 & 1 & 23 & 3 \end{bmatrix} \to mod\ 26 \to \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 23 & 3 \end{bmatrix}$$

Assim, do lado direito, obtemos a matriz transposta da matriz decodificadora, logo, temos:

$$A^{-1} = \begin{bmatrix} 1 & 23 \\ 0 & 3 \end{bmatrix}\ (mod\ 26)$$

Agora, para decifrar a mensagem, separamos o texto criptografado em pares de letras e substituímos letra por seu número correspondente:

$$\begin{array}{ccccc} BE & WI & XS & MF & NC \\ 2\ 5 & 23\ 9 & 24\ 19 & 13\ 6 & 14\ 3 \end{array}$$

Escrevemos cada par de números como um vetor q e obtemos os correspondentes vetores de texto com em módulo 26. Precisamos fazer isso apenas para a parte do texto que ainda não conhecemos:

$$\begin{bmatrix} 1 & 23 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 24 \\ 19 \end{bmatrix} = \begin{bmatrix} 461 \\ 57 \end{bmatrix} = \begin{bmatrix} 19 \\ 5 \end{bmatrix}\ (mod\ 26)$$

$$\begin{bmatrix} 1 & 23 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 13 \\ 6 \end{bmatrix} = \begin{bmatrix} 151 \\ 18 \end{bmatrix} = \begin{bmatrix} 21 \\ 18 \end{bmatrix}\ (mod\ 26)$$

$$\begin{bmatrix} 1 & 23 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 14 \\ 3 \end{bmatrix} = \begin{bmatrix} 83 \\ 9 \end{bmatrix} = \begin{bmatrix} 5 \\ 9 \end{bmatrix}\ (mod\ 26)$$

Assim, substituindo os pares de números pelas letras correspondentes, obtemos o restante do t $SE\ \ UR\ \ EI$. Logo, conseguimos decifrar a mensagem: $MOVA\ \ SEU\ \ REI$.

Exemplo 2: *Suponha que recebemos um texto que foi criptografado com uma* 3*-cifra de Hill e sabemo. a palavra criptografada FIKYRVMWG, corresponde a palavra de texto comum UNICORNIO. Vamos ob matriz inversa* A^{-1} *da matriz codificadora A, módulo* 26*, com a qual podemos decifrar o restante do textc*

Como o texto foi criptografado por uma 3-cifra de Hill, vamos separar o texto comum conhecido em gı de 3 letras e substituí-las por seus equivalentes numéricos:

$$\begin{array}{ccc} UNI & COR & NIO \\ 21\ 14\ 9 & 3\ 15\ 18 & 14\ 9\ 15 \end{array}$$

Fazemos o mesmo com o correspondente texto cifrado:

$$\begin{array}{ccc} FIK & YRV & MWG \\ 6\ 9\ 11 & 25\ 18\ 22 & 13\ 23\ 7 \end{array}$$

De modo que, os vetores p de texto comum e seus correspondentes vetores cifrados q são:

$$p_1 = \begin{bmatrix} 21 \\ 14 \\ 9 \end{bmatrix}, \quad q_1 = \begin{bmatrix} 6 \\ 9 \\ 11 \end{bmatrix}$$

$$p_2 = \begin{bmatrix} 3 \\ 15 \\ 18 \end{bmatrix}, \quad q_2 = \begin{bmatrix} 25 \\ 18 \\ 22 \end{bmatrix}$$

$$p_3 = \begin{bmatrix} 14 \\ 9 \\ 15 \end{bmatrix}, \quad q_3 = \begin{bmatrix} 13 \\ 23 \\ 7 \end{bmatrix}$$

Queremos reduzir a matriz

$$Q = \begin{bmatrix} q_1^t \\ q_2^t \\ q_3^t \end{bmatrix}$$

a matriz identidade de ordem 3, aplicando operações elementares de linhas, e simultaneamente, aplic mesmas operações na matriz

$$P = \begin{bmatrix} p_1^t \\ p_2^t \\ p_3^t \end{bmatrix}$$

obtendo a matriz $(A^{-1})^t$. Para isso, fazemos do mesmo modo que no exemplo anterior e obtemos:

$$\begin{bmatrix} 6 & 9 & 11 & 21 & 4 & 9 \\ 25 & 18 & 22 & 3 & 15 & 18 \\ 13 & 23 & 7 & 14 & 9 & 15 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 1 & 0 & 0 & 9 & 17 & 18 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 8 & 18 & 17 \end{bmatrix}$$

Assim, a matriz inversa da matriz codificadora A, módulo 26 é:

$$A^{-1}\,(mod\,26) = \begin{bmatrix} 9 & 1 & 8 \\ 17 & 0 & 18 \\ 18 & 0 & 17 \end{bmatrix}$$

Com esta matriz, podemos decifrar o restante do texto. Observe que quando utilizamos uma 3-cifra de para a codificação, precisamos conhecer pelo menos 9 letras de uma palavra de texto comum conseguirmos decodificá-lo. Quanto maior a dimensão da matriz codificadora A, mais difícil se torna cálculos e mais segura se torna a mensagem codificada.

Voltar ao Topo.

Última Atualização: 27/07/2015.