Universidade Estadual de Campinas - Faculdade de Ciências Aplicadas
LE106 - Geometria Analítica e Álgebra Linear
Atividade 3 – 22/05/2020

Grupos de até 4 alunos ou individual.

RA e Nome 1: _____

RA e Nome 2: _____

RA e Nome 3: _____

RA e Nome 4: _____

Questão	Pontos	Nota
1	5	
2	5	
Total	10	

Criptografia

Um **criptograma** é uma mensagem codificada. A palavra grega *kryptos* significa "escondido". Existem várias formas de criptografar uma mensagem. Um método que utiliza a multiplicação de matrizes para **codificar e decodificar** mensagens é apresentado a seguir. O método utiliza a seguinte correspondência no processo de codificação e decodificação:

0 = _	9 = i	18 = r
1 = a	10 = j	19 = s
2 = b	11 = k	20 = t
3 = c	12 = l	21 = u
4 = d	13 = m	22 = v
5 = e	14 = n	23 = w
6 = f	15 = o	24 = x
7 = g	16 = p	25 = y
8 = h	17 = q	26 = z

Exemplo de codificação, passo a passo:

Utilize a seguinte matriz invertível (chave da criptografia) para codificar:

$$A = \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix}$$

1. Digite a mensagem para ser codificada: *meet me monday*

   Considere apenas letras minúsculas e espaços. Não inclua pontuação ou outros tipos de caracteres ou letras maiúsculas.

2. Particione a mensagem (incluindo espaços em branco) em uma matriz de caracteres. O número de colunas da matriz deve ser o mesmo da matriz A. Ou seja, se a última coluna não tiver elementos suficientes, você deverá completar com espaço:

   [[*mee*], [*t m*], [*e m*], [*ond*], [*ay*]]

3. Utilize a correspondência numérica para criar outra matriz:

   [[13, 5, 5], [20, 0, 13], [5, 0, 13], [15, 14, 4], [1, 25, 0]

4. Multiplique cada linha da matriz numérica pela matriz A, como mostrado a seguir:

$$[13\ \ 5\ \ 5].\begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = [13\ \ -26\ \ 21]$$

$$[20\ \ 0\ \ 13].\begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = [33\ \ -53\ \ -12]$$

$$[5\ \ 0\ \ 13].\begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = [18\ \ -23\ \ -42]$$

$$[15\ \ 14\ \ 4].\begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = [5\ \ -20\ \ 56]$$

$$[1\ \ 25\ \ 0].\begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = [-24\ \ 23\ \ 77]$$

5. A sequência de linhas codificadas é:
   [13 −26 21][33 −53 −12][18 −23 −42][5 −20 56][−24 23 77]

6. E finalmente, a mensagem codificada:
   13 -26 21 33 -53 -12 18 -23 -42 5 -20 56 -24 23 77

Em outras palavras, se $X = [x_1\ \ x_2\ \ x_3]$ é uma matriz $1xn$ não codificada, então $Y = XA$, com A_{nxn} e Y é a correspondente matriz codificada $1xn$.

Desta forma, se a pessoa que recebe a mensagem quiser descriptografar, basta fazer: $X = YA^{-1}$

Exemplo de decodificação, passo a passo:

Utilize a inversa da matriz A:

$$A^{-1} = \begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix}$$

1. Digite a mensagem para ser decodificada: 13 -26 21 33 -53 -12 18 -23 -42 5 -20 56 -24 23 77

2. Particione a mensagem em grupos com a mesma quantidade de colunas da matriz A^{-1}:
   $[13\ \ -26\ \ 21][33\ \ -53\ \ -12][18\ \ -23\ \ -42][5\ \ -20\ \ 56][-24\ \ 23\ \ 77]$

3. Multiplique cada linha da matriz numérica pela matriz A^{-1}, como mostrado a seguir:

$$[13\ \ -26\ \ 21].\begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = [13\ \ 5\ \ 5]$$

$$[33\ \ -53\ \ -12].\begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = [20\ \ 0\ \ 13]$$

$$[18\ \ -23\ \ -42].\begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = [5\ \ 0\ \ 13]$$

$$[5\ \ -20\ \ 56].\begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = [15\ \ 14\ \ 4]$$

$$[-24\ \ 23\ \ 77].\begin{bmatrix} -1 & -10 & -8 \\ -1 & -6 & -5 \\ 0 & -1 & -1 \end{bmatrix} = [1\ \ 25\ \ 0]$$

4. A sequência decodificada é:
   $[[13, 5, 5], [20, 0, 13], [5, 0, 13], [15, 14, 4], [1, 25, 0]$

5. Utilize a correspondência numérica para criar outra matriz:
   [[*mee*], [*t m*], [*e m*], [*ond*], [*ay*]]

   E uma lista (pode facilitar): ['*m*','*e*','*e*','*t*',' ','*m*','*e*',' ','*m*','*o*','*n*','*d*','*a*','*y*',' ']

6. E finalmente, a mensagem decodificada:
   meet me monday

Questão 1 ..... *5 pontos*
Implemente a codificação de uma mensagem.

Questão 2 ..... *5 pontos*
Implemente a decodificação de uma mensagem.