Actividad en clase, semana 7. Hill

Azpeitia García Karyme Ivette

March 27, 2023

1 Intrucciones:

1. Completa la frase: *Mi super poder como estudiante es
2. Escoge una matriz apropiada de Hill para cifrar la frase y cifrala.
3. Pónla en el classroom.
4. Escoge un criptograma del classroom.

1.1 Cifrado

`Mi super poder como estudiante es remar`

1. Dividimos el texto, separamos en pares y a cada par le asociamos un vector.

MI	SU	PE	RP	OD	ER	CO	MO	ES
(12,8)	(18,20)	(15,4)	(17,15)	(14,13)	(4,17)	(2,14)	(12,14)	(4,18)

TU	DI	AN	TE	ES	RE	MA	RZ
(19,20)	(3,8)	(0,13)	(19,4)	(4,18)	(17,4)	(12,0)	(17,25)

2. Escogemos una matriz de $2x2$ con $(det, 26) = 1$ Tenemos la matriz

$$\begin{matrix} 1 & 0 \\ 2 & 1 \end{matrix} \tag{1}$$

donde su determinante es $1 \cdot 1 - 2 \cdot 0 = 1 mod 26$

3. Ciframos, multiplicamos vector por matriz *Trabajamos con mod 26*

(MI)$\rightarrow (12,8)\begin{matrix} 1 & 0 \\ 2 & 1 \end{matrix} = (12 \cdot 1 + 8 \cdot 2, 12 \cdot 0 + 8 \cdot 1) = (2,8) \rightarrow$(CI)

(SU)$\rightarrow (18,20)\begin{matrix} 1 & 0 \\ 2 & 1 \end{matrix} = (18 \cdot 1 + 20 \cdot 2, 18 \cdot 0 + 20 \cdot 1) = (6,20) \rightarrow$(GU)

(PE)$\rightarrow (15,4)\begin{matrix} 1 & 0 \\ 2 & 1 \end{matrix} = (15 \cdot 1 + 4 \cdot 2, 15 \cdot 0 + 4 \cdot 1) = (23,4) \rightarrow$(XE)

(RP)$\rightarrow (17,15)\begin{matrix} 1 & 0 \\ 2 & 1 \end{matrix} = (17 \cdot 1 + 15 \cdot 2, 17 \cdot 0 + 15 \cdot 1) = (21,15) \rightarrow$(VP)

(OD)$\rightarrow (14,3)\begin{matrix} 1 & 0 \\ 2 & 1 \end{matrix} = (14 \cdot 1 + 3 \cdot 2, 14 \cdot 0 + 3 \cdot 1) = (20,3) \rightarrow$(UD)

(ER)$\rightarrow (4,17)\begin{matrix} 1 & 0 \\ 2 & 1 \end{matrix} = (4 \cdot 1 + 17 \cdot 2, 4 \cdot 0 + 17 \cdot 1) = (12,17) \rightarrow$(MR)

(CO)$\rightarrow (2,14)\begin{matrix} 1 & 0 \\ 2 & 1 \end{matrix} = (2 \cdot 1 + 14 \cdot 2, 2 \cdot 0 + 14 \cdot 1) = (4,14) \rightarrow$(EO)

(MO)$\rightarrow (12,14)\begin{matrix}1 & 0\\ 2 & 1\end{matrix} = (12\cdot 1+14\cdot 2, 12\cdot 0+14\cdot 1) = (14,14) \rightarrow$(OO)

(ES)$\rightarrow (4,18)\begin{matrix}1 & 0\\ 2 & 1\end{matrix} = (4\cdot 1+18\cdot 2, 4\cdot 0+18\cdot 1) = (14,18) \rightarrow$(OS)

(TU)$\rightarrow (19,20)\begin{matrix}1 & 0\\ 2 & 1\end{matrix} = (19\cdot 1+20\cdot 2, 19\cdot 0+20\cdot 1) = (7,20) \rightarrow$(HU)

(DI)$\rightarrow (3,8)\begin{matrix}1 & 0\\ 2 & 1\end{matrix} = (3\cdot 1+8\cdot 2, 3\cdot 0+8\cdot 1) = (19,8) \rightarrow$(TI)

(AN)$\rightarrow (0,13)\begin{matrix}1 & 0\\ 2 & 1\end{matrix} = (0\cdot 1+13\cdot 2, 0\cdot 0+13\cdot 1) = (0,13) \rightarrow$(AN)

(TE)$\rightarrow (19,4)\begin{matrix}1 & 0\\ 2 & 1\end{matrix} = (19\cdot 1+4\cdot 2, 19\cdot 0+4\cdot 1) = (1,4) \rightarrow$(BE)

(ES)$\rightarrow$(OS)

(RE)$\rightarrow (17,4)\begin{matrix}1 & 0\\ 2 & 1\end{matrix} = (17\cdot 1+4\cdot 2, 17\cdot 0+4\cdot 1) = (25,4) \rightarrow$(ZE)

(MA)$\rightarrow (12,0)\begin{matrix}1 & 0\\ 2 & 1\end{matrix} = (12\cdot 1+0\cdot 2, 12\cdot 0+0\cdot 1) = (12,0) \rightarrow$(MA)

(RZ)$\rightarrow (17,25)\begin{matrix}1 & 0\\ 2 & 1\end{matrix} = (17\cdot 1+25\cdot 2, 17\cdot 0+25\cdot 1) = (15,25) \rightarrow$(PZ)

De lo anterior la frase cifrada es: `GIGUXEVPUDMREOOOOSHUTIANBE`

1.2 Descifrar

Tomando de classroom la siguiente frase de mi compañero Ricardo Luévano:

`GK EA IB XK FX ZD SS MC AG GB OB NN QF AG MD HH`

Dado que sabemos la parte de la frase cifrada, tenemos las siguientes relaciones:

MI	SU	PE	RP	OD	ER	CO	MO	ES
GK	EA	IB	XK	FX	ZD	SS	MC	AG

TU	DI	AN	TE	ES		
GB	OB	NN	QF	AG	MD	HH

- Encontrando la matriz de cifrado:
  (PE)$\rightarrow (15,4)\begin{matrix}a & b\\ c & d\end{matrix} = (15\cdot a+4\cdot c, 15\cdot b+4\cdot 1d = (8,1) \rightarrow$(IB) (RP)$\rightarrow (17,15)\begin{matrix}a & b\\ c & d\end{matrix} = (17\cdot a+15\cdot c, 17\cdot b+15\cdot d) = (23,10) \rightarrow$(XK)
- Resolvemos el sistema de ecuaciones
  1)

$$\begin{aligned} 15a+4c &= 8\\ 17a+15c &= 23 \end{aligned}$$

- Despejamos a de $15a+4c=8$ tenemos:

$$\begin{aligned} a &= \frac{1}{15}(8-4c)\\ a &= 7(8-4c)\\ a &= 2-c \end{aligned}$$

- Sustituimos a en $17a + 15c = 23$

$$\begin{aligned} 17(4 - 2c) + 15c &= 23 \\ 68 - 34c + 15c &= 23 \\ 16 - 8c + 15c &= 23 \\ 16 + 7c &= 23 \\ 7c &= 7 \\ c &= 1 \end{aligned}$$

- De lo anterior tenemos que $a = 2$ y $c = 1$

  2)

$$\begin{aligned} 15b + 4d &= 1 \\ 17b + 15d &= 10 \end{aligned}$$

- Despejamos b de $15b + 4d = 1$ tenemos

$$\begin{aligned} b &= \frac{1}{15}(1 - 4d) \\ b &= 7(1 - 4d) \\ b &= 7 - 2d \end{aligned}$$

- Sustituimos en $17b + 15d = 10$

$$\begin{aligned} 17(7 - 2d) + 15d &= 10 \\ 119 - 34d + 15d &= 10 \\ 15 + 7d &= 10 \\ 7d &= 10 - 15 \\ d &= 15(-5) \\ d &= 3 \end{aligned}$$

De lo anterior tenemos que $b = 1$ y $d = 3$, por lo tanto la matriz de cifrado es $\begin{matrix} 2 & 1 \\ 1 & 3 \end{matrix}$.

Ahora calculamos la matriz inversa para poder descifrar.

- Sabemos que el determinante es distinto de 0 por lo que existe su matriz inversa.
- Escribimos la matriz aumentada:

$$\begin{matrix} 2 & 1 & 1 & 0 \\ 1 & 3 & 0 & 1 \end{matrix}$$

- Encuentra el pivote en la columna número 1 e intercambia la fila número 2 con la fila número 1

$$\begin{matrix} 1 & 3 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{matrix}$$

- Elimina la columna numero 1

$$\begin{matrix} 1 & 3 & 0 & 1 \\ 0 & -5 & 1 & -2 \end{matrix}$$

- Encuentra el pivote en la columna número 2 dividiendo la fila número 2 entre -5

$$\begin{matrix} 1 & 3 & 0 & 1 \\ 0 & 1 & -\frac{1}{15} & \frac{2}{5} \end{matrix}$$

- Elimina la columna numero 2

$$\begin{matrix} 1 & 0 & \frac{3}{15} & -\frac{1}{15} \\ 0 & 1 & -\frac{1}{15} & \frac{2}{5} \end{matrix}$$

- Ahí está la matriz inversa a la derecha

$$\begin{matrix} 1 & 0 & \frac{3}{15} & -\frac{1}{15} \\ 0 & 1 & -\frac{1}{15} & \frac{2}{5} \end{matrix}$$

Por lo tanto la matriz inversa es:

$$\begin{matrix} \frac{3}{15} & -\frac{1}{15} \\ -\frac{1}{15} & \frac{2}{5} \end{matrix}$$

Ahora, como trabajamos en $mod 26$ tenemos:

$$\begin{matrix} 11 & 5 \\ 5 & 16 \end{matrix}$$

Ahora desciframos para `MD HH`

Donde `MD(12,3)` y `HH(7,7)`, entonces:

(MD)$\rightarrow (12,3)\begin{matrix} 11 & 5 \\ 5 & 16 \end{matrix} = (12 \cdot 11 + 3 \cdot 5, 12 \cdot 5 + 3 \cdot 16) = (17,4) \rightarrow$(RE)

(HH)$\rightarrow (7,7)\begin{matrix} 11 & 5 \\ 5 & 16 \end{matrix} = (7 \cdot 11 + 7 \cdot 5, 7 \cdot 5 + 7 \cdot 16) = (8,17) \rightarrow$(IR)

Por lo tanto la frase cifrada es `MI SUPER PODER COMO ESTUDIANTE ES REIR`