SAFM HABEEB 2022MT62009

$P = C = \{A=0, B=1, C=2, \cdots, Z=25, -=26\}$

m = Alphabet size = 27

94.

$$A = \begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} \qquad B = \begin{bmatrix} 1 \\ 4 \end{bmatrix}$$

The message is encrypted using $y \equiv (Ax + B) \% 27$ — (1)

where x is a 2 character chunk of the message each of the 2 chunk received is encrypted as some y and all the chunks are concatenated.

$$\det(A) = 3 \times 7 - 5 \times 2 = 11$$
$$(\det(A))^{-1} \equiv (11)^{-1} \pmod{27}$$

Using extended euclidean algorithm.

$$27 = 2 \times 11 + 5$$
$$11 = 2 \times 5 + 1$$
$$\Rightarrow 1 = 11 - 2 \times 5$$
$$\Rightarrow 1 = 11 - 2(27 - 2 \times 11) = 5 \times 11 - 2 \times 27$$
$$\Rightarrow (5 \times 11) \equiv 1 \pmod{27}$$

$$\Rightarrow 5 \equiv (11)^{-1} \pmod{27}$$
$$\Rightarrow (\det(A))^{-1} \equiv 5 \pmod{27}$$

$$A^{-1} \equiv (\det(A))^{-1} \begin{bmatrix} 7 & -5 \\ -2 & 3 \end{bmatrix} \equiv 5 \begin{bmatrix} 7 & -5 \\ -2 & 3 \end{bmatrix} \pmod{27}$$

$$\Rightarrow A^{-1} \equiv \begin{bmatrix} 35 & -25 \\ -10 & 15 \end{bmatrix} \pmod{27} \equiv \begin{bmatrix} 8 & 2 \\ 17 & 15 \end{bmatrix} \pmod{27}$$

SAEM HABEEB 2022MT62004

We will decrypt using the following eqn

$$x \equiv A^{-1}(y-B) \pmod{27} \quad \text{(from (1))}$$

Cypher: KBI-FTIQTRPTHCJMGNFDJDDUMJDAAAV SZSEFPCL NAJXG.

Cypher length = 44

We will use 22 chunks, we can also form a 2×22 matrix for y's i.e. we will form a 2×22 matrix by augmenting all the 2-chunks in matrix form in order.

Cypher in a 2×22 matrix:

$$Y = \begin{pmatrix} K & I & F & I & T & P & H & J & G & F & J & D & M & D & A & V & Z & E & P & L & A & X \\ B & - & T & Q & R & T & C & M & N & D & D & U & J & A & A & S & S & F & C & N & J & G \end{pmatrix}$$

$$\equiv \begin{pmatrix} 10 & 8 & 5 & 8 & 19 & 15 & 7 & 9 & 6 & 5 & 9 & 3 & 12 & 3 & 0 & 21 & 25 & 4 \\ 1 & 26 & 19 & 16 & 17 & 19 & 2 & 12 & 13 & 3 & 3 & 20 & 9 & 0 & 0 & 18 & 18 & 5 \end{pmatrix}_I$$

$$\begin{matrix} 15 & 11 & 0 & 23 \\ 2 & 13 & 9 & 6 \end{matrix}\Big)$$

$$X = A^{-1}(Y - \underbrace{B|B\cdots|B}_{22 \text{ times}}) \qquad B = \begin{bmatrix} 1 \\ 4 \end{bmatrix} \quad A^{-1} \equiv \begin{pmatrix} 8 & 2 \\ 17 & 15 \end{pmatrix} \pmod{27}$$

$= A^{-1}$

(eq) $Z = Y - \underbrace{B|B|\cdots|B}_{22 \text{ times}} = \begin{pmatrix} 9 & 7 & 4 & 7 & 18 & 14 & 6 & 8 & 5 & 4 & 8 & 2 & 11 & 2 & -1 & 20 & 24 & 3 \\ -3 & 22 & 15 & 12 & 13 & 15 & -2 & 8 & 9 & -1 & -1 & 16 & 5 & -4 & -4 & 14 & 14 & 1 \end{pmatrix}_I$

$$\begin{matrix} 14 & 10 & -1 & 22 \\ -2 & 9 & 5 & 2 \end{matrix}\Big) \pmod{27}$$

$$X = A^{-1}Z \equiv \begin{pmatrix} 8 & 2 \\ 17 & 15 \end{pmatrix}\begin{pmatrix} Z \\ I \end{pmatrix}$$

$$\equiv \begin{pmatrix} 66 & 100 & 69 & 80 & 170 & 142 & 44 & 80 & 58 & 30 & 62 & 48 & 98 & 8 & -16 & 184 & 220 & 26 & 108 \\ 108 & 449 & 293 & 299 & 509 & 463 & 72 & 256 & 220 & 53 & 121 & 274 & 262 & -26 & -77 & 550 & 618 & 66 & 308 \end{pmatrix}_I$$

$$\begin{matrix} 98 & 2 & 180 \\ 305 & 58 & 404 \end{matrix}\Big) \pmod{27}$$

SAEM HABEEB 2022MT62004

$$X = \begin{pmatrix} 12 & 19 & 10 & 26 & 8 & 7 & 17 & 26 & 4 & 3 & 8 & 2 & 17 & 8 & 11 & 26 & 4 & 26 & 0 & 17 \\ 0 & 17 & 23 & 2 & 15 & 4 & 18 & 13 & 4 & 26 & 13 & 4 & 19 & 1 & 4 & 10 & 24 & 12 & 19 & 8 \\ 2 & 18 & & & & & & & & & & & & & & & & & & \\ 4 & 26 & & & & & & & & & & & & & & & & & & \end{pmatrix}$$

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	Z	-
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

$$X = \begin{pmatrix} M & T & I & - & I & H & R & - & E & D & I & V & R & I & L & - & E & - & A & R & C & S \\ A & R & X & C & P & E & S & N & E & - & N & E & T & B & E & K & Y & M & T & I & E & - \end{pmatrix}$$

We now concatenate the column transpose to form the original message

∴ Message: MATRIX-CIPHERS-NEED-INVERTIBLE-KEY-MATRICES-