Loïc Galland
199804131911

1MA464

(2) cipher text = SOSS

$A = \begin{pmatrix} 16 & 25 \\ 25 & 16 \end{pmatrix}$

first I calculate the determinant

$\det(A) = 16 \times 16 - 25 \times 25$
$= -369$
$= 21 \mod 26$

Then i need to find $\det^{-1}$

$\det . \det^{-1} = 1 \mod 26$
$21 . x = 1 \mod 26$
$21 . 5 = 1 \mod 26$
$105 = 1 \mod 26$

Now we calculate the adj(A)

$\operatorname{adj}(A) = \begin{pmatrix} 16 & -25 \\ -25 & 16 \end{pmatrix} \equiv \begin{pmatrix} 16 & 1 \\ 1 & 16 \end{pmatrix} \mod 26$

Then calculate A'

$A' = \det^{-1} . (\operatorname{adj}(A))$
$= 5 . \begin{pmatrix} 16 & 1 \\ 1 & 16 \end{pmatrix} = \begin{pmatrix} 80 & 5 \\ 5 & 80 \end{pmatrix} \equiv \begin{pmatrix} 2 & 5 \\ 5 & 2 \end{pmatrix} \mod 26$

Now to decrypt we just need to use the A' to encrypt the cipher text

$\begin{pmatrix} S \\ O \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 14 \end{pmatrix}$

$A' . \begin{pmatrix} S \\ O \end{pmatrix} \equiv \begin{pmatrix} 2 & 5 \\ 5 & 2 \end{pmatrix} . \begin{pmatrix} 18 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 2 \times 18 + 5 \times 14 \\ 5 \times 18 + 2 \times 14 \end{pmatrix} \equiv \begin{pmatrix} 36 + 70 \\ 90 + 28 \end{pmatrix} \equiv \begin{pmatrix} 106 \\ 118 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 14 \end{pmatrix} \mod 26 \Rightarrow \begin{pmatrix} C \\ O \end{pmatrix}$

$\begin{pmatrix} S \\ S \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 9 \end{pmatrix}$

$A' . \begin{pmatrix} S \\ S \end{pmatrix} \equiv \begin{pmatrix} 2 & 5 \\ 5 & 2 \end{pmatrix} . \begin{pmatrix} 18 \\ 9 \end{pmatrix} \equiv \begin{pmatrix} 2 \times 18 + 5 \times 9 \\ 5 \times 18 + 2 \times 9 \end{pmatrix} \equiv \begin{pmatrix} 81 \\ 108 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 4 \end{pmatrix} \mod 26 \Rightarrow \begin{pmatrix} D \\ E \end{pmatrix}$

So the plaintext is CODE

① CBC = CBC is a AES block cipher. It uses XOR on the firstplaintext block with a vector before encrypting the plaintext. It also use block chaining by XOR every plaintext block with the ciphertext of the previous block

ECB = It is used for block operations. It uses the principle that each block of plaintext has a defined ciphertext for it and it goes both ways. Therefore the same plaintext will always get the same ciphertext

③ $E_2(X) = 5x+11 \mod 26$

Inverse of $E_2(x) \to D_2(Y) = 21(y-11) \mod 26$

Resulting ciphertext = doxxm $d=3$ $o=14$ $x=23$ $m=12$

So now we use that numbers to figure out what letters we get after the first encryption

$D_2(d) = 21(3-11) = 14 \mod 26 \to O$ | $D_2(x) = 21(23-11) = 18 \mod 26 \to S$

$D_2(o) = 21(14-11) = 11 \mod 26 \to L$ | $D_2(m) = 21(12-11) = 21 \mod 26 \to V$

So after the first encryption we should get the ciphertext = OLSSV

Now we need to find $E_1(X) = ax+b$

We know that

$14 = a7+b \mod 26$ and $11 = a4+b \mod 26$

Now we need to find a and b

$$\begin{aligned} 14 &= a7+b \\ -\ 11 &= a4+b \\ \hline \frac{3}{3} &= \frac{3a}{3}+0 \mod 26 \end{aligned}$$

$\to a = 3 \times 3^{-1}$ we find the 3^{-1} with the eucledian algo we get 9

$a = 3 \times 9 = 27 = 1 \mod 26$

$14 = 7 \times 1 + b$ Therefore $E_1(X) = 1x + 7 \mod 26$

$b = 14-7$

$= 7$