Q4

- S-box in DES = Substitute in AES
- XOR with K ? = Add round key in AES
-
-

Q1

→ get multiplicative inverse

$$\rightarrow \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots \\ 1 & 1 & 0 & & \\ 1 & 1 & 1 & & \\ 1 & 1 & 1 & & \\ 1 & 1 & 1 & & \\ 0 & 1 & 1 & & \\ 0 & 0 & 1 & & \\ 0 & 0 & 0 & & \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} \begin{matrix} C \\ \\ \\ \\ \\ \\ \\ 7 \end{matrix}$$

steps بتاعة الـ encryption مش هي هي الـ steps بتاعة الـ decryption

- Sub bytes
- Shift rows
- mix Col.s
- add round key

- inv. shift row
- inv sub bytes
- add key
- inv. Mix

→ inv sub bytes
→ inv shift row
→ inv Mix Col. (5:)
→ $\omega(4,7) \Rightarrow$ inv. Mix Col.
→ add round key

→ shift rows
→ add round key } ممكن يتعملوا بـ word

AES equation

$$\begin{bmatrix} e_{0,j} \\ e_{1,j} \\ e_{2,j} \\ e_{3,j} \end{bmatrix} = \begin{bmatrix} 02 \\ 01 \\ 01 \\ 03 \end{bmatrix} \begin{bmatrix} S[a_{0,j}] \\ S[a_{1,j}-1] \\ S[a_{2,j}-2] \\ S[a_{3,j}-3] \end{bmatrix} \oplus \begin{bmatrix} K_{0,j} \\ K_{1,j} \\ K_{2,j} \\ K_{3,j} \end{bmatrix}$$

⇓

لو عايزة اعمل round 10
هشيل ده

$$Tmp = S_{0,j} + S_{1,j} + S_{2,j} + S_{3,j}$$

$$S'_{0,j} = S_{0,j} \oplus Tmp \oplus \boxed{?} * [S_{0,j} \oplus S_{1,j}]$$