# CSS322 – Modes of Operation Notes

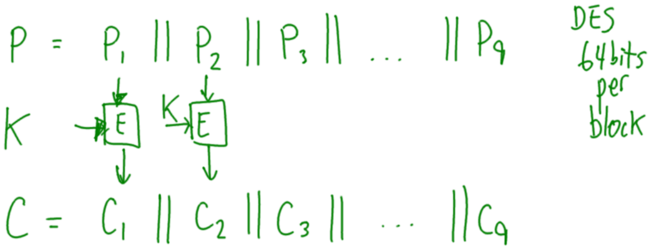
$P = P_1 \| P_2 \| P_3 \| \dots \| P_q$
DES 64bits per block
K
E
K
E
$C = C_1 \| C_2 \| C_3 \| \dots \| C_q$

Figure 1: ECB Produces Repeating Ciphertext; Lecture 07

CBC : $P_1 = P_2$

$$\left.\begin{aligned} X_1 &= P_1 \oplus IV \\ C_1 &= E(K, X_1) \end{aligned}\right] P_1$$

$$\left.\begin{aligned} X_2 &= P_1 \oplus C_1 \\ C_2 &= E(K, X_2) \end{aligned}\right] P_2$$

Does $C_1 == C_2$ ?

$C_1 = E(K, P_1 \oplus IV)$

$C_2 = E(K, P_1 \oplus C_1)$

if $IV == \underset{\substack{\uparrow \\ \text{random}}}{C_1}$ then $C_1 = C_2$ (BAD)

Figure 2: Conditions when CBC produces repeating ciphertext; Lecture 08

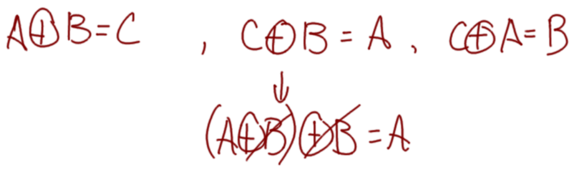

Figure 3: Inverse of XOR is XOR; Lecture 08

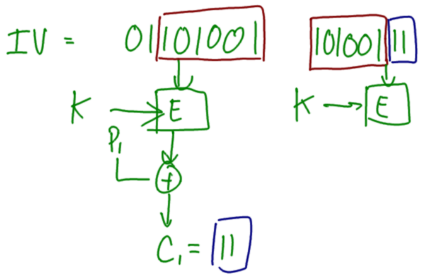

Figure 4: CFB Shift Register; Lecture 08