Block Cipher Operations

Tristan Erney
November 2nd, 2021
Intro to Cryptology
Hands On Exercise 9

1)

CBC Mode

$P_i = C_{i-1} \text{ xor } D_k(C_i)$ $\quad C_i = E_k(P_i \text{ xor } C_{i-1})$
$= C_{i-1} \text{ xor } D_k(E_k(P_i \text{ xor } C_{i-1}))$
$= C_{i-1} \text{ xor } P_i \text{ xor } C_{i-1}$
$= P_i$

CFB Mode

$P_i = C_i \text{ xor } L_s(E_k(X_i))$ $\quad C_i = P_i \text{ xor } L_s(E_k(X_i))$
$= P_i \text{ xor } L_s(E_k(X_i)) \text{ xor } L_s(E_k(X_i))$
$= P_i$

2)

a) CFB-32

$P_i = C_i \text{ xor } L_{32}(E_k(X_i))$ $\quad X_{i+1} = R_{32}(X_i) \,||\, C_i$

b)

$C = C_1` \; C_2 \; C_3 \; C_4 \ldots C_n$

$P_1` = C_1` \text{ xor } L_{32}(E_k(X_1))$ $\quad X_2` = R_{32}(X_1) \,||\, C_1`$
$P_2` = C_2 \text{ xor } L_{32}(E_k(X_2`))$ $\quad X_3` = C_1` \,||\, C_2$
$P_3` = C_3 \text{ xor } L_{32}(E_k(X_3`))$ $\quad X_4 = C_2 \,||\, C_3$
$P_4 = C_4 \text{ xor } L_{32}(E_k(X_4))$ $\quad X_5 = C_3 \,||\, C_4$

The only affected blocks are $P_1$, $P_2$, and $P_3$, therefore this concludes that $P_i` = P_i$ for all $i <= 4$.

3)

$C = C_1` \; C_2 \; C_3 \; C_4 \ldots C_n$
$P_1` = C_0 \text{ xor } D_k(C_1`)$
$P_2` = C_1` \text{ xor } D_k(C_2)$
$P_3 = C_2 \text{ xor } D_k(C_3)$
$P_4 = C_3 \text{ xor } D_k(C_4)$

Setting the affected ciphertext block to $C_1$, we can see in our example that $P_1$ and $P_2$ are the only blocks affected in the plaintext.
Therefore, the two blocks which are affected are block i and i + 1.