Esercizio - Cifrario a blocchi a 4 bit in modalità CBC e CTR

Si consideri un cifrario a blocchi che opera su blocchi di 4 bit. La funzione di cifratura E è definita dalla seguente tabella:

Input	$E(\cdot)$
0000	0001
0001	0010
0010	1011
0011	1111
0100	1101
0101	0000
0110	0011
0111	1001
1000	0110
1001	1000
1010	0101
1011	0111
1100	1110
1101	1100
1110	1010
1111	0100

La funzione di decifratura D è l'inversa di E. Ad esempio:

$$E(0000) = 0001 \Rightarrow D(0001) = 0000,\ 2mm]\Rightarrow D(0000) = 0101,\ 2mm]E(0110) = 0011 \Rightarrow D(0011) = 0110,\ 2mm]E(1001) = 1000 \Rightarrow D(1001) = 0111,\ 2mm]\Rightarrow D(0110) = 1000.$$

Modalità CBC (Cipher Block Chaining)

In CBC la cifratura e la decrittazione avvengono a blocchi. - **Cifratura:**

$$C_i = E(P_i \oplus C_{i-1}) \quad \text{con } C_0 = \text{IV}$$

- **Decrittazione:**

$$P_i = D(C_i) \oplus C_{i-1}$$

Consideriamo il seguente ciphertext:

$$CT = (\underline{1101})\ 1001\ 0101\ 0110,$$

dove:

$$C_0 = 1101 \quad \text{(IV)}, \quad C_1 = 1001, \quad C_2 = 0101, \quad C_3 = 0110.$$

Calcoliamo il plaintext:

Blocco 1:

$$P_1 = D(1001) \oplus C_0.$$

Sapendo che $E(0111) = 1001$, vale $D(1001) = 0111$. Quindi:

$$P_1 = 0111 \oplus 1101 = 1010.$$

Blocco 2:

$$P_2 = D(0101) \oplus C_1.$$

Poiché $E(1010) = 0101$, abbiamo $D(0101) = 1010$. Così:

$$P_2 = 1010 \oplus 1001 = 0011.$$

Blocco 3:

$$P_3 = D(0110) \oplus C_2.$$

Dato che $E(1000) = 0110$ implica $D(0110) = 1000$, allora:

$$P_3 = 1000 \oplus 0101 = 1101.$$

Pertanto, il plaintext in modalità CBC è:

$$PT_{\text{CBC}} = 1010\ 0011\ 1101.$$

Modalità CTR (Counter Mode)

In CTR si utilizza un contatore per generare un keystream. Si parte da un contatore iniziale CTR_0 e, per ogni blocco i, si calcola:

$$k_i = E(CTR_0 + i).$$

La cifratura avviene tramite:

$$C_i = P_i \oplus k_i.$$

Consideriamo il plaintext:

$$PT = 0001\ 0010\ 0011,$$

diviso in 3 blocchi da 4 bit, e il contatore iniziale:

$$CTR_0 = 1100.$$

Gli altri contatori sono:

$$CTR_1 = 1100, \quad CTR_2 = 1100 + 1 = 1101, \quad CTR_3 = 1100 + 2 = 1110.$$

(con le addizioni eseguite modulo 2^4).
Calcoliamo il keystream:

- Per $CTR_1 = 1100$: $E(1100) = 1110$ quindi $k_1 = 1110$;
- Per $CTR_2 = 1101$: $E(1101) = 1100$ quindi $k_2 = 1100$;
- Per $CTR_3 = 1110$: $E(1110) = 1010$ quindi $k_3 = 1010$.

Ora, la cifratura dei blocchi si ottiene:

- **Blocco 1:**

$$C_1 = 0001 \oplus 1110 = 1111.$$

- **Blocco 2:**

$$C_2 = 0010 \oplus 1100 = 1110.$$

- **Blocco 3:**

$$C_3 = 0011 \oplus 1010 = 1001.$$

Quindi, il ciphertext in modalità CTR è:

$$CT_{\text{CTR}} = 1111\ 1110\ 1001.$$