Esercizio 1

1. Si considerino testi in chiaro e testi cifrati di 4 bit ($\mathcal{P} = \mathcal{C} = \mathbb{Z}_{16}$) e chiavi di 1 bit ($\mathcal{K} = \mathbb{Z}_2$) con la seguente funzione di cifratura $E_k(x_0, x_1, x_2, x_3) = x_0 \oplus k, x_1 \oplus k, x_2 \oplus k, x_3 \oplus k$. Supporre inoltre che la chiave sia scelta in modo casuale ad ogni cifratura ($p_{\mathcal{K}}(k) = 1/2$). Dimostrare che il cifrario è perfetto oppure, nel caso non lo sia, mostrare un controesempio.
2. Valutare la sicurezza del cifrario ottenuto iterando quattro volte il cifrario del punto precedente, in cui la chiave sia scelta in modo casuale ad ogni iterazione.
3. Valutare, infine, la sicurezza della variante al cifrario precedente in cui $\mathcal{K} = \mathbb{Z}_2 \times \mathbb{Z}_4$, $E_{(k,j)}(x_0, x_1, x_2, x_3) = x_0 \oplus k_0, x_1 \oplus k_1, x_2 \oplus k_2, x_3 \oplus k_3$, dove

$$k_i = \begin{cases} k & \text{se } i = j \\ 0 & \text{altrimenti} \end{cases}$$

   e la chiave (k, j) è scelta in modo equiprobabile $p_{\mathcal{K}}(k, j) = 1/2 \times 1/4 = 1/8$

Esercizio 2

Definire *Message Authentication Codes (MAC)* e *firma elettronica* evidenziando le principali similitudini e differenze e i principali vantaggi e svantaggi. Mostrare, infine, un protocollo di autenticazione di entità basato su MAC e uno basato su firma.

Esercizio 3

Spiegare perchè le seguenti funzioni hash sono inadeguate per un utilizzo crittografico, indicando, per ognuna, un possibile scenario di attacco

1. Il testo X viene diviso in blocchi $X_1, \ldots, X_n$ ognuno di 256 bit. $h(X) = X_1 \oplus X_2 \oplus \ldots \oplus X_n$;
2. Il testo X viene diviso in blocchi $Z_1, \ldots, Z_m$ ognuno di 128 bit, $g(X) = E_{Z_1}(Z_1) \oplus E_{Z_2}(Z_2) \oplus \ldots E_{Z_m}(Z_m)$, dove E cifra testi di 128 bit utilizzando chiavi di 128 bit.
3. Il testo X viene diviso in blocchi $R_1, \ldots, R_t$ ognuno di 64 bit, $w(X) = E_{R_1}(E_{R_2}(\ldots E_{R_t}(0)\ldots))$, dove E cifra testi di 64 bit utilizzando chiavi di 64 bit.

Esercizio 4

Considerare il protocollo

$$\begin{array}{lcll} A & \rightarrow & B & : N_A \\ B & \rightarrow & A & : E_{PK_A}(M_B, N_A, N_B, B) \\ A & \rightarrow & B & : M_A, N_B, A \end{array}$$

dove PK_A è la chiave pubblica di A, N_A e N_B sono nonce generati rispettivamente da A e B, M_A e M_B sono due messaggi generati rispettivamente da A e B.
Quali garanzie di sicurezza (identificazione di entità, autenticazione e segretezza di M_A e M_B) hanno A e B al termine del protocollo? Modificare leggermente il protocollo in modo che garantisca autenticazione mutua tra A e B.

Esercizio 5 (facoltativo)

Esistono attacchi su protocolli crittografici che si basano sulla similitudine eccessiva tra differenti messaggi del protocollo stesso (attacchi "type-flaw"). Illustrare un esempio di tale tipologia di attacchi.