Esercizio 1

1. Si considerino testi in chiaro di 4 bit ($\mathcal{P} = \mathbb{Z}_{16}$), chiavi e testi cifrati di 2 bit ($\mathcal{K} = \mathcal{C} = \mathbb{Z}_4$) e la funzione di cifratura $E_K(X) = X + K \mod 4$. Può tale schema essere considerato un cifrario? Spiegare.
2. Si consideri una variante dello schema precedente in cui anche i testi cifrati siano di 4 bit ($\mathcal{C} = \mathbb{Z}_{16}$) e $E_K(X) = X + K \mod 16$; supporre inoltre che la chiave sia scelta in modo casuale ad ogni cifratura ($p_{\mathcal{K}}(K) = 1/4$). Dimostrare che tale cifrario non è perfetto.
3. Qual è la dimensione minima di $\mathcal{K}$ affinchè il cifrario diventi perfetto? Discutere tramite la teoria di Shannon.

Esercizio 2

Cosa sono e a cosa servono i certificati a chiave pubblica? Considerare il protocollo di autenticazione

$$\begin{array}{lcll} B & \rightarrow & A & : N_B \\ A & \rightarrow & B & : PK_A, Sign_{SK_A}(N_B, B) \end{array}$$

dove N_B è un nonce generato da B, PK_A e SK_A sono, rispettivamente, le chiavi pubblica e segreta A.
Aggiungere la trasmissione da A a B del certificato per la chiave pubblica PK_A di A, emesso da una Certification Authority T (con chiavi PK_T, SK_T), spiegando:

1. come viene verificato il certificato da B;
2. perchè è necessario trasmettere tale certificato ai fini dell'autenticazione di A.

Esercizio 3

Dare la definizione di funzione hash one-way e mostrare almeno un esempio in cui risulta necessaria tale proprietà. Dare infine un esempio di funzione hash NON one-way, spiegando opportunamente.

Esercizio 4

Considerare il protocollo

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

dove PK_A è la chiave pubblica di A, N_B è un nonce generato da B, M_A e M_B sono due messaggi generati rispettivamente da A e B.

1. Quali garanzie di sicurezza (identificazione di A e autenticazione e segretezza di M_A e M_B) ha B al termine del protocollo?
2. cosa cambia se il protocollo viene modificato come segue

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

Esercizio 5 (facoltativo)

Dare la definizione di autenticazione di entità basata sulle "correspondence assertions" $begin(A, B)$ e $end(B, A)$, spiegandola intuitivamente. Illustrare almeno un esempio di attacco catturato da tale definizione (in cui cioè non c'è corrispondenza).