Esercizio 1

Si consideri un cifrario in cui i testi in chiaro e i testi cifrati sono di d bit ($|\mathcal{P}| = |\mathcal{C}| = 2^d$), mentre le chiavi sono di $e \leq d$ bit ($|\mathcal{K}| = 2^e$). La funzione di cifratura è definita come segue: $E_{k_0,\ldots,k_{e-1}}(x_0,\ldots,x_{d-1}) = x_0 \oplus k_{(0 \bmod e)},\ldots,x_i \oplus k_{(i \bmod e)},\ldots,x_{d-1} \oplus k_{(d-1 \bmod e)}$.

1. Considerare il caso $d = 8$, $e = 1$ e mostrare le due possibili cifrature del testo in chiaro 11001011;
2. Dimostrare, tramite un controesempio, che se $e < d$ il cifrario non è perfetto;
3. Se $d = e$, quale altra condizione è necessaria (e sufficiente) affinchè il cifrario diventi perfetto? Discutere tramite la teoria di Shannon.

Esercizio 2

Si deve cifrare una trasmissione satellitare a pagamento per proteggerne la segretezza. I dati vengono trasmessi un byte alla volta e si predilige la qualità della trasmissione all'integrità dei dati.

1. Quale modalità del DES (o di un qualsiasi altro cifrario a blocchi) è la più adatta a questo tipo di applicazione e perchè?
2. Mostrare gli schemi di cifratura e decifratura.
3. Perchè richiedere l'integrità potrebbe danneggiare la qualità della trasmissione?

Esercizio 3

Dare la definizione di funzione hash collision free e illustrare uno scenario in cui risulta indispensabile tale proprietà. Dare infine un esempio di funzione hash NON collision free, spiegando opportunamente.

Esercizio 4

Considerare il semplice protocollo di autenticazione mutua:

$$\begin{array}{lcll} A & \rightarrow & B & : E_K(\text{“eccomi qua!!”}) \\ B & \rightarrow & A & : E_K(\text{“ciao anche io sono qua!!”}) \end{array}$$

in cui K è la chiave a lungo termine condivisa tra A e B.

1. Mostrare i due attacchi di *replay* (*replica*) in cui il nemico riesce a impersonare, rispettivamente, A e B;
2. “Riparare” il protocollo indicando quali sono le *sfide* (*challange*), anche se implicite, e quali la *risposte* (*response*); mostrare come gli attacchi del punto precedente vengono evitati;
3. É possibile un attacco di tipo *reflection*? Discutere ed, eventualmente, correggere ulteriormente il protocollo.

Esercizio 5 (facoltativo)

Cosa si intende per *crittoanalisi differenziale*? Illustrare tale tecnica su i primi 3 round del DES.