Esercizio 1

Dare la definizione formale di cifrario a spostamento. Dimostrare, tramite un controesempio, che il cifrario non è perfetto se, come avviene normalmente, la chiave viene riutilizzata per cifrare le diverse lettere di una frase. Sotto quale condizione il cifrario diventa perfetto? Discutere e dare una dimostrazione formale.

Esercizio 2

Viene emessa una tessera elettronica a punti per l'utilizzo di una funivia. Tale tessera contiene una parte di memoria (inizialmente contenente tutti zeri) in cui è possibile scrivere il valore 1 una volta sola: una volta settato un bit a 1 è impossibile riportarlo a 0. Proporre un protocollo che permetta la carica dei punti da parte della biglietteria e l'utilizzo, a scalare, da parte dell'utente. Fare in modo che l'utente non possa 'ricaricare' da solo i punti.

Esercizio 3

Dare la definizione di firma elettronica e mostrare come realizzare uno schema di firma tramite il cifrario a chiave pubblica RSA. Un principio, denominato *key-separation*, prevede di utilizzare coppie differenti di chiavi per cifrare e firmare. Perchè è importante applicare tale principio? Illustrare tramite un esempio.

Esercizio 4

Considerare il semplice protocollo di autenticazione unilaterale:

$$A \quad \rightarrow \quad B \quad : \; E_K(\text{“sono proprio io e sono le ore:”}, T_A)$$

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

1. Mostrare un attacco di *reflection* in cui il nemico riesce a sfruttare una sessione parallela per fingere di essere B con A.
2. La sicurezza del protocollo cambierebbe se il messaggio inviato fosse “sono proprio A e sono le ore”, T_A? Spiegare.

Esercizio 5 (facoltativo)

Dare la definizione di funzione hash strong collision-free e one-way. Dare un esempio di funzione che non soddisfa tali proprietà spiegando in dettaglio.