Esercizio 1

Si considerino un cifrario S_1 a spostamento con chiave $k = 4$ e un cifrario a S_2 a sostituzione con chiave:

```
Testo in chiaro: A B C D E F G H I L M N O P Q R S T U V Z
Testo cifrato:   R T F C I M E Z U V Q P G O B D N L H S A
```

1. Mostrare che $S_1 \times S_2 \neq S_2 \times S_1$, cioè che l'ordine in cui si compongono i cifrari è rilevante;
2. Cosa accade se, nella composizioni sopra menzionate, si sceglie la chiave k del cifrario S_1 in modo equiprobabile (quindi diversa per ogni lettera da cifrare)? È ancora vero che $S_1 \times S_2 \neq S_2 \times S_1$?
3. Valutare infine, tramite la teoria di Shannon, la sicurezza di tutte le composizioni di cifrari discusse ai punti precedenti.

Esercizio 2

Spiegare perchè l'autenticazione basata su login/password è considerata "debole". Mostrare le principali differenze rispetto all'autenticazione basata su sfida/risposta. Illustrare, infine, il ruolo di parametri "varianti nel tempo", quali nonce, timestampes o numeri di sequenza.

Esercizio 3

Dare la definizione di cifrario a blocchi (block cipher) e di cifrario a flusso (stream cipher). Mostrare che il cifrario di Vigenere può essere indifferentemente definito sia come cifrario a blocchi che come cifrario a flusso (suggerimento: ragionare sulla dimensione del blocco da cifrare).

Esercizio 4

Scrivere un protocollo basato su nonce e crittografia a chiave asimmetrica che soddisfi le seguenti specifiche:

1. Autenticazione Mutua: A e B si vogliono autenticare entrambi;
2. Autenticazione dell'invio e della ricezione di K_s: A vuole inviare una chiave di sessione K_s autenticata e segreta a B: B deve essere sicuro che la chiave proviene da A e non è una replica; A vuole inoltre una conferma che B abbia ricevuto la chiave.

Discutere la resistenza del protocollo proposto agli attacchi standard di replica. Indicare, infine, la tipologia delle sfide/risposte utilizzate.

Esercizio 5 (facoltativo)

A e B vogliono comunicare tramite crittografia a chiave pubblica. La chiave pubblica di A è certificata da CA_1 quella di B da CA_2. Le chiavi pubbliche delle autorità di certificazione CA_1 e CA_2 sono a loro volta certificate dalla autorità centrale CA_{root}. A e B conoscono (in modo autentico) la chiave pubblica di CA_{root}. Mostrare la "catena" di certificati che B deve richiedere per verificare l'autenticità della chiave pubblica di A. Illustrare come tale catena viene verificata da B.