Esercizio 1

Si consideri un cifrario S a sostituzione con chiave π:

```
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. Considerare il cifrario $S' = S \times S$ ottenuto iterando S due volte con la stessa chiave π menzionata sopra. Che cifrario si ottiene?
2. Cosa accade se, nell'iterazione del punto precedente, si utilizza la chiave π prefissata nel primo cifrario S ma si sceglie la chiave π' del secondo cifrario S in modo equiprobabile (quindi diversa per ogni lettera da cifrare)?
3. Valutare infine, tramite la teoria di Shannon, la sicurezza di tutte le composizioni di cifrari discusse ai punti precedenti.

Esercizio 2

Per quale motivo nell'implementazione del RSA non si calcola l'elevamento a potenza X^b come b moltiplicazioni di X? Illustrare brevemente l'algoritmo square-and-multiply spiegando perché esso risulta adatto all'implementazione di RSA.

Esercizio 3

Definire i *Message Authentication Codes (MAC)*. Mostrare un protocollo di autenticazione di entità basato su MAC e discutere le principali differenze rispetto all'autenticazione sfida/risposta bassata su cifratura e/o decifratura.

Esercizio 4

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

1. A e B condividono una chiave a lungo termine simmetrica K_{AB};
2. Autenticazione e segretezza 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, che è segreta e non è una replica;
3. Autenticazione e segretezza di M_B: B vuole inviare ad A un messaggio cifrato con la chiave di sessione K_s. Il messaggio deve inoltre essere autenticato: A deve essere sicura che il messaggio proviene da B e non è una replica.

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

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.