### Esercizio 1

Si consideri la composizione di un cifrario a sostituzione con chiave:

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

con un cifrario a spostamento, con chiave $k = 7$.

1. Mostrare la cifratura, tramite la composizione dei due cifrari, del testo in chiaro `JAVA`;
2. Mostrare che la stessa cifratura si ottiene, equivalentemente, con un solo cifrario a sostituzione con opportuna chiave (indicare la chiave);
3. Dimostrare che, in generale, la composizione di un cifrario a sostituzione $\mathrm{S}_1$ e di un cifrario a spostamento $\mathrm{S}_2$ con chiavi equiprobabili, è equivalente a un cifrario a sostituzione con chiavi equiprobabili. Dimostrare cioè che $\mathrm{S}_1 \times \mathrm{S}_2 = \mathrm{S}_1$.

### Esercizio 2

Dare la definizione formale di cifrario a blocchi (block cipher) e di cifrario a flusso (stream cipher), mostrando che uno è un caso particolare dell'altro. Fornire un esempio per entrambi i tipi di cifrario che illustri la definizione formale di cui sopra.

### Esercizio 3

Quali sono le definizioni di funzione hash *strong collision-free* e di funzione hash *one-way*? Dare un esempio di funzione hash che non sia strong collision-free e un esempio di funzione hash che non sia one-way. Si puo' dimostrare che l'assenza di una proprietà implica sempre l'assenza dell'altra: discutere basandosi sugli esempi proposti.

### Esercizio 4

Considerare il semplice protocollo

$$\begin{array}{lcccl} \text{Messaggio} & A & \rightarrow & B & : N_A \\ \text{Messaggio} & B & \rightarrow & A & : E_K(A, N_A, N_B, K_1) \\ \text{Messaggio} & A & \rightarrow & B & : E_K(A, N_B, K_2) \end{array}$$

dove $K$ è una chiave a lungo termine condivisa tra $A$ e $B$, $N_A$ e $N_B$ sono due nonce, e $K_1$ e $K_2$ sono due "sottochiavi" che verranno usate per generare una chiave di sessione $K_s = K_1 \oplus K_2$.

1. Quali proprietà di autenticazione e segretezza garantisce tale protocollo? Discutere.
2. Per ottimizzare l'implementazione del protocollo viene proposto di aggiungere $N_A$ nell'ultimo messaggio in modo che abbia la stessa forma del precedente: $E_K(A, N_A, N_B, K_2)$. Che tipo di problemi puo' generare questa modifica? Discutere.

### Esercizio 5 (facoltativo)

La crittografia a chiave pubblica si basa generalmente su problemi difficili da risolvere. Questo consente di dimostrare teoremi sulla robustezza (relativa) del cifrario. Mostrare un risultato di questo tipo, discutendolo brevemente.