Esercizio 1

Si consideri il seguente crittogramma, ottenuto tramite un cifrario a spostamento:

`CSBLZETILQQLALZHPEPTLZPATQBT`

1. Crittoanalizzare tale testo, illustrando il metodo adottato.
2. Sarebbe ancora possibile la crittoanalisi se il testo in chiaro fosse stato cifrato utilizzando uno spostamento differente (scelto a caso, con distribuzione uniforme) per ogni lettera cifrata? Discutere tramite la teoria di Shannon.
3. Considerare, infine, il caso in cui il testo in chiaro sia suddiviso in blocchi di 'd' lettere e tutte le lettere di uno stesso blocco vengano cifrate con la stessa chiave. Dimostrare che questo cifrario non è perfetto anche se le chiavi per i vari blocchi sono scelte a caso con distribuzione uniforme.

Esercizio 2

Definire il cifrario a chiave pubblica RSA. Basandosi poi sui due numeri primi p=11 e q=5, ricavare una coppia di chiavi (a,b) e calcolare la cifratura del testo X=2. Mostrare in dettaglio il procedimento utilizzato per ricavare la coppia di chiavi e discutere se tale procedimento possa essere o meno utilizzato per l'implementazione del cifrario.

Esercizio 3

Si decide di iterare un cifrario idempotente allo scopo di aumentarne la sicurezza. È importante oppure no, per decidere se iterarlo due o tre volte, considerare eventuali attacchi meet-in-the-middle? Cambierebbe la situazione se il cifrario non fosse idempotente? Discutere approfonditamente.

Esercizio 4

Si consideri il seguente protocollo

$$\begin{aligned} B &\rightarrow A : N_B \\ A &\rightarrow B : E_{SK_A}(h(B, M_A, N_B)), E_{PK_B}(M_A) \end{aligned}$$

dove M_A è un messaggio di A, N_B è un nonce generato da B, h è una funzione hash strong collision-free e SK_A, PK_B sono, rispettivamente, la chiave segreta di A e quella pubblica di B.

1. Elencare le proprietà (autenticazione di entità e messaggi, segretezza) garantite dal protocollo evidenziando le componenti dei messaggi necessarie al raggiungimento di tali proprietà e le relative verifiche svolte da A o B.
2. È importante la proprietà strong collision-free di h?
3. Cosa accade se si elimina il nonce dal protocollo?

Esercizio 5 (facoltativo)

Dimostrare che una funzione hash $h : Z \rightarrow W$ strong collision free è anche one-way, quando $|W| \leq |Z|/2$.