1. Alice usa il crittosistema **RSA** per ricevere messaggi da Bob. Alice sceglie:
- p=13, q=17
- il suo esponente pubblico è e=7

Alice pubblica il prodotto N=pq=221 e l'esponente e=7

1) Verificare che e=7 è un esponente valido per l'algoritmo RSA
2) Calcolare **d**, la chiave privata di Alice

Bob vuole inviare ad Alice il testo P=19, cifrandolo

3) Che valore Bob invia ad Alice?
4) Verificare che Alice riesca a decifrare tale messaggio.

[Scrivere tutti i passaggi per ottenere il risultato per tutte le domande]

(6 punti / 24)

2. Consideriamo il seguente Cifrario Affine: $e(x) = ax+b \bmod 26$, con a=7 e b=4

1) a=7 è una scelta valida per il parametro "a"? Giustificare il perché della propria risposta.
2) b=2 è una scelta valida per il parametro b ? Giustificare il perché della propria risposta.
3) Cifrare con questo cifrario il plaintext "sicurezza"
4) Calcolare la funzione di decifratura **d(y)**
5) Decifrare il ciphertext "gaekg"
6) Decifrare il ciphertext "ahozgrhg"

(6 punti / 24)

3. Descrivere in dettaglio il protocollo di Diffie-Hellman e discutere i suoi aspetti di sicurezza e l'attacco MiTM.

(4 punti / 24)

4. In cosa consiste una vulnerabilità di SQL injection? Fate anche un esempio pratico di come si sfrutta un SQL injection. Quali modi si possono utilizzare per proteggersi? Cosa potrebbe fare un attaccante sfruttando questa vulnerabilità?

(4 punti / 24)