Nome: [redacted] Fondamenti di Cybersecurity 19-06-2025 Cognome: [redacted] Matricola: [redacted]

1. Alice usa il crittosistema **RSA** per ricevere messaggi da Bob. Alice sceglie:
   - **p=11, q=17**
   - il suo esponente pubblico è **e=7**

   Alice pubblica il prodotto **n=pq=187** e l'esponente **e=7**
   - a) Verificare che **e=7** è un esponente valido per l'algoritmo RSA
   - b) Calcolare **d**, la chiave privata di Alice

   Bob vuole inviare ad Alice il testo **P=19**, cifrandolo
   - c) Che valore Bob invia ad Alice?
   - d) Verificare che Alice riesca a decifrare correttamente tale messaggio.

   [Scrivere TUTTI i passaggi (utilizzando gli algoritmi Euclidean, Extended Euclidean e Square and Multiply) per ottenere il risultato per tutte le domande a) b) c) e d)]

   (8 punti / 30)

2. **L'attacco Meet-in-the-Middle di Double DES.**
   a) Definire il Block Cipher Double DES
   b) Dimostrare in modo chiaro e dettagliato questo attacco (illustrando con delle tabelle) e calcolare il tempo di computazione totale approssimato per ottenere/ricavare la copia di chiavi.

   (7 punti / 30)

3. a) Descrivere in modo dettagliato il protocollo di scambio di chiavi di **Diffie-Hellman (DH)**.
   b) Su quale **tecnica** si basa la **sicurezza** del protocollo DH ?
   c) Presentare l'attacco di **Man-in-the-Middle** che puo' avere luogo con questo protocollo.

   (6 punti / 30)

4. **Buffer Overflow.**
   a) Descrivere in cosa consiste un attacco di tipo **buffer overflow**.
   b) Quando e' possibile attuarlo?
   c) Fornire un esempio semplice di un programma vulnerabile.
   d) Esistono precauzioni o contromisure?

   (6 punti / 30)

5. a) Descrivere il permesso speciale **setuid** del filesystem Linux.
   b) Perché puo' essere pericoloso dal punto di vista sicurezza?

   (3 punti / 30)