Sistemi di Elaborazione (Sicurezza su Reti)	**Anno Acc. 1998-99**

Esercizi di Verifica Dicembre 1998

Nome e Cognome: Matricola:

Spazio riservato alla correzione

1	2	3	4	**Tot.**
/25	/25	/25	/25	/100

1. *25 punti*
   Descrivere il crittosistema di ElGamal, lo schema di Diffie-Hellman, ed analizzare la relazione tra i due.

2. *25 punti*
   Enunciare e dimostrare la relazione tra la proprietà di sicurezza forte per le funzioni hash e la proprietà di "one-way."

3. *25 punti*
   Fornire un semplice esempio numerico delle fasi di *generazione parametri*, *generazione firma*, e *verifica firma* per lo schema di firme di Lamport.

4. *25 punti*
   Descrivere ed analizzare il crittosistema di Rabin.