Sistemi di Elaborazione (Sicurezza su Reti)	**Anno Acc. 1997-98**

Esercizi di Verifica Maggio 1998

Nome e Cognome: Matricola:

Spazio riservato alla correzione

1	2	3	4	5	**Tot.**
/30	/20	/25	/10	/15	/100

1. *30 punti*
   Descrivere lo schema per le firme digitali DSS.
   (a) Descrivere l'algoritmo per la firma.
   (b) Descrivere l'algoritmo per la verifica.
   (c) Illustrare brevemente l'algoritmo per la generazione delle chiavi.

2. *20 punti*
   Fare un semplice esempio per illustrare il funzionamento dello schema di firme di Lamport e quello di Bos-Chaum.

3. *25 punti*
   Derivare la relazione che c'è tra probabilità di errore, numero di elementi scelti e cardinalità dell'insieme di campionatura nel paradosso del compleanno.

4. *10 punti*
   Descrivere brevemente un sistema per la certificazione del tempo, ed enunciare le caratteristiche di sicurezza.

5. *15 punti*
   Descrivere brevemente il protocollo dei puzzle di Merkle per l'accordo su chiavi. Qual'è la complessità di tempo necessaria per le parti?