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

Esercizi di Verifica Gennaio 1999

Nome e Cognome: Matricola:

Spazio riservato alla correzione

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

1. *20 punti*
   Definire le proprietà di *Completezza*, *Soundness*, *Zero-knowledge* e *Prova di conoscenza* per un Sistema di Prova.

2. *25 punti*
   Descrivere un protocollo zero-knowledge per la prova di conoscenza per grafi 3-colorabili.

3. *30 punti*
   Descrivere ed analizzare lo schema a soglia di Shamir (k, n) per la condivisione dei segreti. Fornire un semplice esempio numerico delle varie fasi.

4. *25 punti*
   Definire le proprietà dell'*Oblivious Transfer* ed illustrare un protocollo che lo realizzi.