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

Esercizi di Verifica Giugno 1998

Nome e Cognome: Matricola:

Spazio riservato alla correzione

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

1. *15 punti*
   Descrivere una implementazione per le "blind signature".

2. *20 punti*
   Descrivere come avviene la generazione dei bit casuali/pseudocasuali nel PGP.

3. *20 punti*
   Definire le proprietà di *Completezza*, *Soundness*, *Zero-knowledge* e *Prova di Conoscenza* per un Sistema di Prova.

4. *30 punti*
   Descrivere il protocollo per la prova di conoscenza per i grafi Hamiltoniani. Dimostrare le proprietà del protocollo.

5. *15 punti*
   Descrivere un Fair Cryptosystem. Illustrare le proprietà.