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

Esercizi di Verifica Novembre 1998

Nome e Cognome: Matricola:

Spazio riservato alla correzione

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

1. *25 punti*
   Mostrare che per ogni messaggio M e per ogni chiave K vale che se $C = DES_K(M)$ allora $\bar{C} = DES_{\bar{K}}(\bar{M})$.

2. *25 punti*
   Illustrare come rompere il DES doppio mediante un attacco chosen plaintext. Qual'è la complessità dell'attacco?

3. *25 punti*
   Illustrare i cifrari RC5 ed RC6 e le loro caratteristiche salienti.

4. *25 punti*
   In uno schema RSA ogni utente ha (n, e) come chiave pubblica ed (n, d) come chiave privata. Si supponga che un malintenzionato venga a conoscenza della chiave privata di Alice. Alice deve generare una nuova coppia di chiavi. Si accorge di avere conservato la fattorizzazione di n e preferisce usare lo stesso modulo evitando di calcolarne uno nuovo. Genera così una nuova coppia e', d', ottenendo la nuova chiave pubblica (n, e') e la nuova chiave privata (n, d'). Commentare la scelta di Alice.