Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: B. Masucci

Prova intercorso del 31/01/2006

Non è ammesso alcun materiale per la consultazione. Buon lavoro!

1	2	3	4	totale
/25	/25	/20	/20	/90

1. (25 punti) Funzioni hash.
   Enunciare e dimostrare la relazione tra la proprietà di sicurezza forte per le funzioni hash e la proprietà di "one-way".

2. (25 punti) Descrivere ed analizzare lo schema di firme RSA.
   - (5 punti) Descrivere le fasi di generazione delle chiavi, firma e verifica.
   - (10 punti) Sia (n=35, e=5) la chiave pubblica di Alice.
     i. Calcolare la chiave privata di Alice mediante l'algoritmo di Euclide esteso.
     ii. Calcolare la firma di Alice sul messaggio m=5, illustrando le computazioni. Inoltre controllare che la verifica abbia successo.
   - (10 punti) Discutere come la proprietà di omomorfismo di RSA possa essere utilizzata per attaccare lo schema.

3. (20 punti) Descrivere lo schema di autenticazione di Lamport.

4. (20 punti) Schema di Diffie-Hellman per l'accordo su chiavi tra due partecipanti.
   - (10 punti) Descrivere ed analizzare gli algoritmi per la generazione dei parametri pubblici e per l'accordo sulla chiave.
   - (10 punti) Analizzare la sicurezza dello schema.