Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 08/07/2014

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

1	2	3	4	totale
/20	/30	/25	/25	/100

1. (20 punti) DES triplicato.
   a. (5 punti) Descrivere il funzionamento del DES triplicato, indicandone i parametri (numero di fasi, taglia del blocco, taglia della chiave).
   b. (10 punti) Illustrare come rompere il DES triplicato mediante un attacco di tipo known plaintext e analizzare la complessità (tempo, spazio) dell'attacco.
   c. (5 punti) Determinare il numero di coppie necessarie affinché l'attacco abbia successo con probabilità prossima ad 1.

2. (30 punti) Descrivere ed analizzare il crittosistema RSA.
    a. (10 punti) Descrivere ed analizzare la fase di generazione delle chiavi e le fasi di cifratura e decifratura. Inoltre, dimostrare che le operazioni di cifratura e decifratura sono una l'inversa dell'altra.
    b. (10 punti) Sia (n=35, e=5) la chiave pubblica di Alice. Supponiamo che Oscar intercetti il messaggio cifrato C=10, inviato da Bob ad Alice. Illustrare le computazioni effettuate da Oscar per risalire al testo in chiaro.
    c. (10 punti) Analizzare la sicurezza della generazione delle chiavi e della cifratura RSA.

3. (25 punti) Descrivere ed analizzare lo schema di Merkle per l'accordo su chiavi tra due partecipanti.
    a. Descrivere le computazioni effettuate da Alice e analizzarne la complessità.
    b. Descrivere le computazioni effettuate da Bob e analizzarne la complessità.
    c. Descrivere le computazioni che un attaccante passivo deve effettuare per rompere lo schema e analizzarne la complessità.

4.(25 punti) Funzioni hash e protocolli di autenticazione.

a. (10 punti) Si definiscano le proprietà di sicurezza debole, sicurezza forte e one-way per le funzioni hash.
b. (15 punti) Si descriva lo schema di autenticazione di Lamport e si discuta di quale proprietà deve godere la funzione hash utilizzata affinchè lo schema sia sicuro.