Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 1/09/2014

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

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

1. (20 punti) Descrivere ed analizzare il crittosistema DES.
   a. (15 punti) Descrivere gli algoritmi di cifratura, decifratura, ed espansione della chiave.
   b. (5 punti) Provare che la decifratura si può effettuare utilizzando lo stesso algoritmo di cifratura con le sottochiavi schedulate in ordine inverso.

2. (25 punti) Si consideri la seguente funzione di cifratura simmetrica a sostituzione

$$E_{(a,b)}(x)=ax+b \bmod 26$$

con chiave k = (a,b), dove $b \in Z_{26}$, e $x \in Z_{26}$.

   i. (10 punti) Si determini sotto quali condizioni sul parametro a della chiave, la funzione di cifratura E risulta univocamente decifrabile.
   ii. (10 punti) In conseguenza di quanto stabilito al punto i), si determini la dimensione dello spazio delle chiavi.
   iii. (5 punti) Sia k=(a,b)=(7,3). Si determini la cifratura del messaggio CIAO.

3. (30 punti) Schema di firme RSA.
    a. (10 punti) Descrivere le fasi di generazione delle chiavi, firma e verifica e dimostrare che le operazioni di firma e verifica sono una l'inversa dell'altra.
    b. (10 punti) Sia (n=35, e=11) la chiave pubblica di Alice.
        i. Calcolare la chiave privata di Alice mediante l'algoritmo esteso di Euclide.
        ii. Calcolare la firma di Alice sul messaggio m=8, mediante un algoritmo di esponenziazione modulare a scelta tra left-to-right e right-to-left.
    c. (10 punti) Analizzare la sicurezza dello schema.

4. (25 punti) Schema di Diffie-Hellman per l'accordo su chiavi tra due partecipanti.
    a. (20 punti) Descrivere ed analizzare gli algoritmi per la generazione dei parametri pubblici e per l'accordo sulla chiave. Inoltre, analizzare la sicurezza dello schema.
    b. (5 punti) E' possibile utilizzare p=17, g=2 come parametri pubblici? Giustificare la risposta.