Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: B. Masucci

Appello dell'8/05/2007

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

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

1. (30 punti) Descrivere ed analizzare lo schema di firme RSA.
   a. (10 punti) Descrivere le fasi di generazione delle chiavi, firma e verifica.
   b. (10 punti) Sia (n=49, e=11) la chiave pubblica di Alice.
      i. Calcolare la chiave privata di Alice, illustrando le computazioni.
      ii. Calcolare la firma di Alice sul messaggio m=8, illustrando le computazioni. Inoltre controllare che la verifica abbia successo.
   c. (10 punti) Discutere come la proprietà di omomorfismo di RSA possa essere utilizzata per attaccare lo schema.

2. (30 punti) Schema di Diffie-Hellman per l'accordo su chiavi tra due partecipanti.
    a. (15 punti) Descrivere ed analizzare gli algoritmi per la generazione dei parametri pubblici e per l'accordo sulla chiave.
    b. (5 punti) E' possibile utilizzare p=11, g=5 come parametri pubblici? Giustificare la risposta.
    c. (10 punti) Si consideri la generalizzazione dello schema per n partecipanti. Quanti messaggi deve inviare ciascun partecipante? Quanti scambi di messaggi in totale sono necessari?

3. (20 punti) Descrivere ed analizzare il DES doppio.
    a. (5 punti) Descrivere il DES doppio.
    b. (15 punti) Analizzare la sicurezza del DES doppio rispetto ai seguenti attacchi
        i. (5 punti) ricerca esaustiva;
        ii. (10 punti) meet in the middle attack.

4. (20 punti) Considerare la seguente funzione hash: sia $w_0(M)$ (risp, $w_1(M)$) il numero di 0 (risp, di 1) presenti nel messaggio $M=m_1m_2m_3\ldots$. La funzione h(M) è definita come segue:

$$h(M)= \begin{cases} 1 & \text{se } w_0(M) < w_1(M) \\ 0 & \text{se } w_0(M) > w_1(M) \\ m_1 & \text{se } w_0(M) = w_1(M) \text{ (dove } M=m_1m_2m_3\ldots) \end{cases}$$

   a. (5 punti) Calcolare l'hash dei seguenti messaggi $M_1=\{00011\}$, $M_2=\{100101\}$, $M_3=\{00111\}$, $M_4=\{0101010101\}$.
   b. (15 punti) Discutere le proprietà di sicurezza della funzione hash precedentemente descritta.