Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 19/06/2015

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

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

1. (25 punti) Password ed autenticazione.
   a. (5 punti) Si chiarisca che cosa è una password ed il suo utilizzo.
   b. (5 punti) Si chiarisca ed analizzi l'uso di funzioni di cifratura e funzioni hash per un sistema di password.
   c. (5 punti) Si descriva ed analizzi l'autenticazione a due fattori (two-factor authentication)
   d. (10 punti) Si analizzino le problematiche di sicurezza legate alla scelta ed all'uso delle password.

2. (30 punti) Schema di firme RSA.
    a. (10 punti) Descrivere le fasi di generazione delle chiavi, firma e verifica.
    b. (10 punti) Analizzare la sicurezza dello schema di firme RSA.
    c. (10 punti) Chiarire come firmare nella pratica facendo uso dello schema RSA.

3. (20 punti) Certificati e PKI.
    a. (5 punti) Chiarire cos'è un certificato e descrivere il formato X.509.
    b. (5 punti) Chiarire l'importanza e l'utilizzo dei certificati.
    c. (10 punti) Chiarire le funzioni di un'autorità di certificazione (CA) e la gestione della fiducia di certificati emessi da CA diverse.

4. (25 punti) Funzioni hash.
Si consideri la seguente proposta di funzione hash valida per messaggi m di almeno 160 bit, costruita a partire dal cifrario simmetrico DES in modalità CBC con chiave 00…0 e IV = 00…0: per un messaggio m di almeno 160 bit, sia

$$H_{daanalizzare}(m) = \text{ultimi 160 bit di } CBC\text{-}DES_{00\ldots0}(m)$$

utilizzando IV = 00…0.
Analizzarne la sicurezza della proposta, giustificando le risposte.