Cognome: Nome: Matricola:

Sicurezza su Reti

Docente: A. De Santis

Appello del 25/07/2014

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

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

1. (20 punti) Cifrari classici.
   a. (5 punti) Dare una classificazione dei possibili attacchi per un crittosistema simmetrico, in base alla conoscenza e alla potenza dell'avversario.
   b. (15 punti) Secondo la classificazione precedente dire a quali tipi di attacchi resistono i seguenti cifrari, motivando la risposta con un esempio:
      i. Cifrario a sostituzione
      ii. Cifrario di Vigenere
      iii. Cifrario di Hill

2. (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=5) la chiave pubblica di Alice.
        i. Calcolare la chiave privata di Alice, illustrando le computazioni.
        ii. Calcolare la firma di Alice sul messaggio m=10, illustrando le computazioni. Inoltre, controllare che la verifica abbia successo.
    c. (10 punti) Discutere la sicurezza della firma RSA.

3. (25 punti) Certificati digitali.
    a. (10 punti) Si illustri la funzione di un certificato digitale e si chiarisca qual è il ruolo di una autorità di certificazione
    b. (15 punti) Si faccia un esempio di come Alice e Bob possano usare certificati rilasciati da due diverse CA e si faccia un esempio di utilizzo di una certification path.

4. (25 punti) Autenticazione.
    a. (10 punti) Si illustri l'autenticazione basata su password chiarendo le tecniche e la sicurezza.
    b. (5 punti) Si illustrino l'autenticazione basata su tecniche challange - response.
    c. (10 punti) Si illustri l'autenticazione basata su tecniche biometriche chiarendo la relativa sicurezza.