Università degli Studi di Torino

Corso di Laurea in Informatica

Esame di Sicurezza – 25 giugno 2015

Nome Cognome

Numero documento

1. Descrivere il formato dello Authentication Header Ipsec (AH) e commentare il significato e l'utilizzo di ogni campo

2a. La firma grafometrica

A) è la scansione della firma autografa

B) comprende la scansione della firma autografa e altri dati biometrici cifrati

C) comprende la scansione della firma autografa e altri dati biometrici non cifrati

D) è l'encryption RSA, fatta con la chiave privata, del digest del documento da firmare

E) è il digest dell'encryption RSA, fatta con la chiave privata, del documento da firmare

2b. L'attacco noto come CSRF (cross site request forgery)

A) permette di eseguire codice dannoso sul server web attaccato

B) permette di eseguire codice dannoso sul browser della vittima

C) permette di eseguire codice dannoso sia sul browser della vittima che sul server

D) usa le credenziali attive sul browser per eseguire delle operazioni non desiderate

E) intercetta i cookie presenti sul browser per utilizzarli successivamente come autenticazione

3. Nello standard ISO 27001, che cosa sono i “controlli” e in base a quali criteri vengono selezionati?

4. Per quale motivo il one-time pad è più sicuro di un cifrario di Vernam con una chiave di lunghezza fissa?

5. Dimostrare le due seguenti proprietà:

A. $(ab) \bmod M = [(a \bmod M)(b \bmod M)] \bmod M$

B. $(a^b) \bmod M = (a \bmod M)^b \bmod M$