Università degli Studi di Torino

Corso di Laurea in Informatica

Esame di Sicurezza – 10 luglio 2015

Nome Cognome

1. Descrivere la funzione di hash SHA-1

2a. il metodo di scambio chiavi di Diffie-Hellman

A) si basa su particolari attacchi di tipo man in the middle

B) si basa sulla difficoltà di calcolare il logaritmo discreto

C) si basa sulla difficoltà di fattorizzare rapidamente un grande numero primo

D) si basa sulla difficoltà di fattorizzare il prodotto di due grandi numeri primi

E) si basa sulla difficoltà di calcolare l'esponente modulare

2b. L'attacco noto come XSS (cross site scripting)

A) permette di eseguire codice dannoso sul server web attaccato

B) permette di intercettare password memorizzate su un database

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) può ottenere cookie del browser e utilizzarli successivamente come autenticazione

3. Descrivere la vulnerabilità OWASP nota come "insecure direct object reference"

4. Che cos'è una marca temporale (timestamp)?

5. Consideriamo il cifrario RSA con modulo n=pq, esponente privato d ed esponente pubblico e. Sia il messaggio da cifrare m=iq<n. Cifrando m otteniamo $c = m^e \bmod n$. Dimostrare che decifrando c otteniamo nuovamente m, ovvero che $c^d \bmod n = m$.