Università degli Studi di Torino

Corso di Laurea in Informatica

Esame di Sicurezza – 11 luglio 2014 – Prof. Bergadano

Nome Cognome

Fila Posto

Numero documento

1. Descrivere la metodologia di analisi dei rischi definita da OWASP

2a. in IPSEC con AH il MAC autentica

A) il solo payload

B) il payload e i campi variabili dell'intestazione IP

C) il payload e i campi fissi e variabili dell'intestazione IP

D) il payload e i campi fissi dell'intestazione IP

E) i soli campi variabili dell'intestazione IP

2b. un cifrario a sostituzione monoalfabetica

A) sostituisce ad ogni singola lettera del testo in chiaro un'altra lettera, in base ad una sostituzione che può cambiare più volte man mano che si procede nello scorrimento del testo stesso

B) sostituisce ad ogni coppia di lettere del testo in chiaro un'altra coppia di lettere, in base ad una sostituzione che può cambiare più volte man mano che si procede nello scorrimento del testo stesso

C) sostituisce ad una n-upla di lettere del testo in chiaro un'altra n-upla di lettere, in base ad una sostituzione che può cambiare una sola volta man mano che si procede nello scorrimento del testo stesso

D) sostituisce ad una n-upla di lettere del testo in chiaro un'altra n-upla di lettere, in base ad una sostituzione che può cambiare più volte man mano che si procede nello scorrimento del testo stesso

E) sostituisce ad una n-upla di lettere del testo in chiaro un'altra n-upla di lettere, in base ad una sostituzione che non può mai cambiare man mano che si procede nello scorrimento del testo stesso

3. Definire che cos'è una funzione di hash resistente alle collisioni

4. Differenza tra un packet filter e un firewall applicativo

5. Algoritmo per calcolare l'inverso moltiplicativo in aritmetica modulo n