11/5/22

Indian Institute of Engineering Science and Technology, Shibpur

B. Tech. (CST) 6th Semester End-Semester Examination, 2022

Information Security and Cryptography (CS 3204)

Time: 2 Hours **Full Marks: 30**

Answer question number 1, 2 and any three from the rest.

1. Choose the correct answer from the given options:

(a) Which principle of security is assured using message-digest algorithms?

(i) Confidentiality (ii) Integrity

(iii) Authentication (iv) Non-repudiation

(b) A packet filter is also termed as ....

(i) Application gateway (ii) Screening router

(iii) Switch (i) None of these

(c) The length of input pad (ipad) in HMAC algorithm is ....

(i) 16 bit (ii) 32 bit

(iii) 8 bit (iv) None of these

(d) Which of the malicious programs don't require host program to replicate?

(i) Trap door (ii) Logic bombs

(iii) Zombie (iv) Trojan horse

(e) Which of the following is a cryptanalysis technique?

(i) Key wrapping (ii) IP spoofing

(iii) IP sniffing (iv) Frequency analysis

(f) The input to the SHA 1 algorithm is divided into blocks of .... bit for further processing

(i) 32 (ii) 64

(iii) 256 (iv) 512

[1 x 6]

2. Answer any three of the following questions briefly:

(a) Compare and contrast MD 5 and SHA-1 algorithms.

(b) What is the difference between message-digest and message authentication code?

(c) Write down the disadvantages of HMAC?

(d) Very briefly explain the different phases that a typical virus goes through during its lifetime.

[2 x 3]

3. (a) Prove the correctness of Diffie-Hellman Key-exchange algorithm mathematically.

(b) Alice & Bob want to establish a secret key using Diffie Hellman Key-exchange algorithm assuming the following values:

n = 11 (divisor), g = 5 (power), x = 2 (chosen by Alice), y = 3 (chosen by BoB);

Find the value of the secret keys (k1 & K2) calculated by them.

(c) Write down the motivations behind the use of digital envelope.

[2 + 2 + 2]

4. (a) What is the utility of access control matrix?

(b) Draw and explain the security life cycle.

(c) Let, P denotes the possible protection states of a protection system and Q denotes the states in which the system is authorised to reside. Now, explain how (P – Q) is dealt with in designing a secure system

[1 + 3 + 2]

5. (a) What is digital certificate?

(b) What is the role of a CA and RA?

(c) Explain the steps of digital certificate creation.

[1 + 2 + 3]

6. (a) Draw the labelled diagram of different possible configurations of firewalls and briefly explain their working.

(b) What do you mean by Virtual Private Networks (VPN)?

(c) Explain the working principle of VPN.

[3 + 1 + 2]

7. Write short notes on any two of the following:

(a) Digital Signature Algorithm

(b) Authentication Tokens

(c) Biometric Authentication

[2 x 3]