Code : 061505

B.Tech 5th Semester Exam., 2018

INFORMATION SECURITY

Time : 3 hours *Full Marks* : 70

Instructions :

(i) The marks are indicated in the right-hand margin.

*(ii) There are **NINE** questions in this paper.*

*(iii) Attempt **FIVE** questions in all.*

*(iv) Question No. **1** is compulsory.*

1. Choose the correct alternative (any *seven*) : 2×7=14

(a) An encryption algorithm transforms plaintext into

(i) cipher text

(ii) simple text

(iii) plaintext

(iv) empty text

(b) From a bank's perspective, which is usually more important?

(i) The integrity of its customer's data

(ii) The confidentiality of the data

(iii) Depends upon customer's choice

(iv) None of the above

(c) Which one is not belongs to passive attack?

(i) Traffic analysis

(ii) Interception

(iii) Interruption

(iv) Snooping

(d) DES follows

(i) Hash algorithm

(ii) Caesars cipher

(iii) Feistel cipher structure

(iv) SP networks

(e) In asymmetric encryption

(i) same key is used for encryption and decryption

(ii) different keys are used for encryption and decryption

(iii) no key is required for encryption and decryption

(iv) None of the above

(f) Which of the following does authentication aim to accomplish?

(i) Restrict what operations/data the user can access

(ii) Determine if the user is an attacker

(iii) Flag the user if he/she misbehaves

(iv) Determine who the user is

(g) Which happens first-authorization or authentication?

(i) Authorization

(ii) Authentication

(iii) Both are same

(iv) None of the above

(h) What is the purpose of a denial of service attack?

(i) Exploit a weakness in the TCP/IP stack

(ii) To execute a Trojan on a system

(iii) To overload a system so it is no longer operational

(iv) To shutdown services by turning them off

(i) Which of the following is a software that once installed on your computer, tracks your Internet browsing habits and sends you popups containing advertisements related to the sites and topics you have visited?

(i) Backdoors

(ii) Adware

(iii) Malware

(iv) Spyware

(j) Communication in client server systems may use Sockets and

(i) Process Control Block (PCB)

(ii) Remote Procedure Calls (RPCs)

(iii) Kernel Mode

(iv) Registers

2. (a) What do you mean by information security? Explain with characteristics. 6

(b) Write short notes on cryptographer, intruder, cryptanalysis and cryptography. 8

3. (a) Elaborate the concept of project VENONA with all features. 5

(b) Encrypt the message 'attackxatxdawn' using a double transposition cipher with 4 rows and 4 columns, using the row permutation (1, 2, 3, 4) → (2, 4, 1, 3) and the column permutation (1, 2, 3, 4) → (3, 1, 2, 4). 9

4. (a) Write with explanation, the important design considerations for a stream cipher. 7

(b) Differentiate the Feistel and non-Feistel design architecture with all characteristics. 7

5. (a) How is block cipher different from stream cipher? State all features to satisfy this. 5

(b) Explain the detailed architecture of AES with all necessary steps of working for each round methodology. 9

6. (a) What is public key cryptography? Explain the relationship of public key cryptography with real world events. 6

(b) Explain the detailed working of RSA with all possible cases by taking suitable example of assumed parameters. 8

7. (a) Define authentication, authorization and availability by suitable example. 6

(b) Why are biometric devices used in extent amount now-a-days? Justify your answer. 4

(c) What do you mean by digital signature? How does it provide privacy, integrity and safety? 4

8. (a) What is the difference between authentication and authorization? Give any two examples of authentication technique. 7

(b) What do you mean by malware? Explain in detail about its vulnerabilities. 7

9. (a) What do you mean by trusted operating system? List some of the certified trusted operating systems with specification. 7

(b) What are the three security functions that an OS should deal with? How does the OS deal with these issues? 7

★★★