Code : 061505

B.Tech 5th Semester Exam., 2017

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. Define the following terms (any *seven*) : 2×7=14

(a) Codebook cipher

(b) Inference control

(c) Honeypots

(d) Logic bomb

(e) Brute-force attack

(f) Trapdoor

(g) Three-factor authentication

(h) Cross-site scripting

(i) Cookies

(j) Code obfuscation

2. *(a)* What are the key principles of Information Security? Explain the attacks that can break integrity of a message. 3+4

(b) Explain with suitable examples different substitution techniques which are used in traditional cryptography. 7

3. *(a)* Use a one-letter frequency attack to decipher the following message :

ONHOVEJHWOBEVGWOCBWHNUGBLHGBGR

(Assume that it is enciphered using monoalphabetic substitution cipher)

Use encryption key (3 2 6 1 5 4) to produce the transposition cipher of the above message. 3+4

(b) How does Vigenere cipher work? Give an example. 7

4. *(a)* Why are stream ciphers faster than block ciphers? Explain any one stream cipher algorithm. 2+5

(b) Explain Diffie-Hellman key exchange algorithm with an example. 7

5. (a) What are the common issues that PKI deals and how? 7

(b) What information must a digital certificate contain? What additional information can a digital certificate contain? 4+3

6. (a) What is Access Control Matrix? Discuss two advantages of ACLs over capabilities. 3+4

(b) Briefly explain a multilevel security model which deals with confidentiality of information. 7

7. (a) Explain three software flaws that make software insecure. 7

(b) Explain different types of IDS used for information security. 7

8. (a) Explain authentication methods using symmetric key and public keys with [redacted] 7

(b) Consider the following mutual authentication protocol, where K_{AB} is a shared symmetric key :

(i) $A \rightarrow B$: "I am Alice", R

(ii) $B \rightarrow A : E(R, K_{AB})$

(iii) $A \rightarrow B : E(R+1, K_{AB})$

Explain two different attacks that attacker can use to convince B that she is Alice. 7

9. (a) What is trusted computing base or TCB? What are the different implementation features of Next Generation Secure Computing Base? 2+5

(b) What security functions are used in modern operating systems? Explain it. 7

★ ★ ★