Code : 061505

B.Tech 5th Semester Exam., 2019

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) Cryptology is the combination of

(i) plaintext and cipher text

[✓ *(ii)* encryption and decryption]

(iii) cryptography and cryptanalysis

(iv) attack and encryption

(b) Threatening to confidentiality is affected with

(i) active attack

[✓ *(ii)* passive attack]

(iii) denial of service attack

(iv) None of the above

(c) In symmetric key cryptography, same key is used by

(i) one party

(ii) multi party

(iii) third party

[✓ *(iv)* both party]

(d) In RSA, $\phi(n)$ = _____ in terms of p and q.

(i) $(p)/(q)$

(ii) $(p)(q)$

[✓ *(iii)* $(p-1)(q-1)$]

(iv) $(p+1)(q+1)$

(e) What is the security goal based on access control?

(i) Authentication

(ii) Authorization

(iii) Accountability

(iv) All of the above

(f) Related to information security, confidentiality is the opposite of which of the following?

(i) Closure

(ii) Disclosure

(iii) Disposal

(iv) Disaster

(g) What is the software called that is designed to exploit a computer user and is a broad term covering computer viruses, worms, Trojan, adware, etc.?

(i) Backdoors

(ii) Key-logger

(iii) Malware

(iv) Bots

(h) If an attacker stole a password file that contained one-way encrypted passwords, what type of an attack would he/she perform to find the encrypted password?

(i) Man-in the middle attack

(ii) Birthday attack

(iii) Denial of service attack

(iv) Dictionary attack

(i) Intruders are most common security threats which are known to be

(i) account access

(ii) data access

(iii) hacker or cracker

(iv) computer access

(j) Which of the following is least secured method of authentication?

[✓ *(i)* Keycard]

(ii) Fingerprint

(iii) Retina pattern

(iv) Password

2. *(a)* Briefly describe the terms snooping, sniffing and spoofing. Also mention which type of attack can be possible with these terms respectively. 9

(b) What are the different categories of security mechanism that exist? Relate all of them with security services. 5

3. *(a)* Differentiate cryptanalysis with Brute-force attack. 4

(b) What is Kerckhoffs' principle? Mention the categories of cryptanalysis attack. 5

(c) What is double transposition cipher? How can this technique be better than traditional transposition cipher? 5

4. *(a)* How are state and word calculations performed in AES algorithm? Mention the formula to recognize block bytes from state 6

(b) What are the differences between symmetric key cryptography and asymmetric key cryptography? Which one is more convenient? 8

5. *(a)* What is stream cipher? Explain how A5/1 steam cipher can provide the privacy over the air communication for GSM cellular network. 7

(b) Write short notes on RC4 with respect to the following terms : 7

(i) Full form and history

(ii) Variants

(iii) Random number generator

(iv) Attacks

6. *(a)* State knapsack problem statement with its all features. What are different kinds of variants used in knapsack problem? What is the other name of knapsack problem? 7

(b) In the RSA public key encryption scheme, each user has a public key 'e' and a private key 'd'. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe? If safe, then explain your answer. 7

7. *(a)* Elaborate all issues and concerns related to biometric devices. 6

(b) What is hash function? Explain how one-way hash function works. 4

(c) What are different applications of digital signature that exist? Explain any one in detail. 4

8. *(a)* What is software flaw (bugs)? How much they can affect any system? 6

(b) List out with explanation any 5 categories of famous attack exist in miscellaneous software based attack. 8

9. *(a)* How can operating system security be achieved through different functions? Justify the answer with proper reference. 7

(b) Briefly describe security evaluated and security focused operating system with all features. 7

★★★