Code : 061805

B.Tech. 8th 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) Questions No. 1 is compulsory.

1. Define any 7 out of the following 10 terms: (2×7)

(a) Public key cryptography

(b) Digital Signature

(c) Non-repudiation

(d) Authentication

(e) Firewall

(f) Virus

(g) CAPTCHA

(h) Intrusion Detection

(i) Confusion

(j) Avalanche Effect

2. (a) What is Codebook Cipher ? Explain with the help of an example how it can provide security. 7

P.T.O

(b) Explain Transposition Cipher Method and using the method produce the Ciphertext for the following Plaintext: "sack gaul spare no one" and the key pattern is:

1 → 4, 2 → 8, 3 → 1, 4 → 5, 5 → 7, 6 → 2, 7 → 6 and 8 → 3. 7

3. (a) Write down the working of RC4 algorithm. Take an example to support your answer. 7

(b) Define AES. Enlist the key difference in the working mechanisms of AES and DES. 7

4. (a) Explain the Diffie-Hellman key exchange algorithm with the help of a suitable example. 7

(b) Using RSA algorithm find the pair of public key and private key when, p=7, q=13 and e=5. Also encrypt the message M=10.

5. (a) What do you mean by a Cryptographic Hash function? Give an example to show how it works. 7

(b) What is the importance of passwords in providing security? What are the basic things that should be kept in mind while creating a Password? 7

(a) What is Biometrics? Give a real world example of how Biometrics is used as a method of

7

(b) How does the Two-Factor authentication work? Is it secure? Justify your statement. 7

7. (a) Draw an Access Control Matrix for an Organization. Describe how it can be used to derive ACLs and C-lists. 7

(b) Encipher the plaintext "ITS COOL" using affine cipher technique when encipherment function is E(x) = (5x + 8) MOD 26. 7

8. (a) What do you mean by a Malware ? Define the different categories of Malwares and how they work. 7

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

9. Write short notes on the following: 7×2

(a) Fiestel Cipher

(b) Salami Attack

***