DoE

23\12\16

7th Sem (Regular)
IS IT-4043
IT

AUTUMN END SEMESTER EXAMINATION-2016

7th Semester B.Tech

INFORMATION SECURITY

IT-4043

(Regular-2013 Admitted Batch)

Time: 3 Hours **Full Marks: 60**

Answer any Six questions including question No.1 which is compulsory.

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable and all parts of a question should be answered at one place only.

1. Answer in brief: [2 × 10

a) Stream cipher is very time consuming as compared to Block cipher - Justify.

b) Why AES supports modern cryptography - Discuss.

c) Differentiate between VIRUS and WORM.

d) What is the principle behind One- Time Pads? Why they are highly secure?

e) By using Caesar cipher technique, decipher the Cipher text ***VFLHQFHFRQJUHVV***.

f) Discuss the importance of public key cryptography and private key cryptography.

g) By using Rail-Fence technique, decipher the Cipher text ***NTIGSMOSBEOHNIIPSIL***.

h) Discuss the different types of intrusion.

i) Differentiate between digital signatures and digital certificates.

j) Discuss IP spoofing with suitable example.

2. a) What are the different types of attack models? Explain each in brief. [4

b) Find the cipher text of the message ***IT IS NEVER TOO LATE TO LEARN*** by Double- Columnar transposition using the keys ***beauty*** and ***world***. [4

3. a) Encrypt the Plain Text message ***MIND MOVES MOUNTAINS*** with the help of keyword ***all is well*** by using the Playfair cipher technique. Write the different steps involved in the process. [4

b) Discuss the pros and cons of MD5 and SHA-1 algorithms. [4

4. a) Discuss the importance of firewall in a secured communication. Also, explain any two types of firewall. [4

b) Differentiate between foot printing and port scanning. [4

5. a) Explain the Expansion Permutation and S-box substitution steps involved in each round of DES algorithm. [4

b) Explain how the 2DES is more secured than to the DES. Also, discuss how it is vulnerable to the meet in the middle attack. [4

6. a) Given p=19, q=23, and e=3, find n, Φ(n) and d using RSA algorithm. [4

b) Discuss the different components of Public Key Infrastructure. [4

7. a) In the Diffie- Hellman protocol, g=7, p=23, x=3 and y=5, what is the value of the symmetric key? [4

b) Discuss how captcha mechanism helps in satisfying the authentication/authorization. [4

8. Write Short notes (any two): [4 × 2

a) MAC Flooding

b) Denial of Service Attack

c) SQL Injection

d) Cryptanalysis

– ***** –