B.E.(with Credits)-Regular-Semester 2012 - Information Technology Sem VIII

IT8044 - Elective-III : Information Security System

P. Pages : 1 **GUG/W/16/7097**

Time : Three Hours * 4 8 6 9 * Max. Marks : 80

Notes : 1. Same answer book must be used for all questions.
2. All questions carry marks as indicated.
3. Due credit will be given to neatness and adequate dimensions.
4. Illustrate your answers wherever necessary with the help of neat sketches.

1. a) What is the difference between passive and Active security threats ? **8**

b) What is the OSI security Architecture ? **8**

OR

2. a) List and briefly define categories of security mechanisms. **8**

b) Write short note on: **8**
a) Data Integrity b) Data confidentiality

3. a) What are the two general approaches to attacking a Cipher. Explain each in detail. **8**

b) Explain substitution and Transposition Technique with example. **8**

OR

4. a) Explain playfair cipher with example. **8**

b) Decipher the message YITJP GWJOW FAQTQ using the hill cipher with inverse key **8**
$\begin{pmatrix} 5 & 1 \\ 2 & 7 \end{pmatrix}$ Show your Calculation and Result.

5. a) Explain in detail use of public key cryptosystems. Also state the requirements for public key cryptography. **10**

b) What are the four possible approaches to attacking the RSA algorithm. Explain each in detail. **6**

OR

6. a) Explain RSA Algorithm with an example. **8**

b) Write short notes on public key cryptosystems with proper diagram. **8**

7. a) Explain Transport and Tunnel modes with respect to AH and ESP. **8**

b) Write short note on oakley key determination protocol. **8**

OR

8. Explain with proper diagram Kerberos in detail. **16**

9. Write short note on: **16**
i) PGP ii) S/MIME

OR

10. a) Explain Intrudes and also explain Instrusion techniques in detail. **10**

b) List and explain the characteristics of Firewall. **6**

****