IT8044 - Elective-III : Information Security System

P. Pages : 2

GUG/S/18/7097

Time : Three Hours

‖‖‖‖‖‖‖‖‖‖‖
2197

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. Assume suitable data wherever necessary.
5. Illustrate your answers wherever necessary with the help of neat sketches.

1. a) What is security attack? Explain with proper example. **8**

b) Explain Network security model with proper diagram. **8**

OR

2. Write short note on:-

a) Authentication. **4**

b) Access control. **4**

c) Data Confidentiality. **4**

d) Data Integrity. **4**

3. Discuss data encryption standard in detail with proper diagram. **16**

OR

4. a) Differentiate between Differential and linear cryptanalysis. **8**

b) Write a note with proper diagram on key Distribution scenario. **8**

5. a) Explain Euclidean and Extended Euclidean algorithm with proper example. **8**

b) What are the important characteristic of public- key cryptosystem? **8**

OR

6. Write a note on.

a) Key exchange protocol. **4**

b) Man in the middle attack. **4**

c) Mutual Authentication. **4**

d) One way Authentication. **4**

7. a) What is IP- security? State application of IP- security. **8**

b) Write short note on -

i) Transport mode. **4**

ii) Tunnel mode. **4**

OR

8. Discuss in detail Kerberos $X \cdot 509$ with proper diagram. **16**

9. Write short note on -

a) RFC 822. **4**

b) Multipurpose mail extension. **4**

c) S/MIME functionality. **4**

d) S/MIME certificate processing. **4**

OR

10. Write short note on -

a) Intrusion Techniques. **4**

b) Intrusion Detection. **4**

c) Rule based intrusion detection. **4**

d) Distributed intrusion detection. **4**

****