IT8044 - Elective-III : Information Security System

P. Pages : 1   **GUG/W/18/2054**

Time : Three Hours |||||||||||||||||||||||||| Max. Marks : 80
                              * 1 5 7 0 *

_____

Notes : 1. Same Answer book must be used for all questions.
2. All questions are compulsory.
3. All questions carry equal marks.
4. Due credit will be given to neatness and adequate dimensions.
5. Assume suitable data wherever necessary.

1.	a)	Explain the key principles of security with suitable example.	**8**
	b)	What is a vulnerability? Explain by giving suitable example.	**8**

OR

2.	a)	Discuss different types of security breaches.	**8**
	b)	What is intrusion detection system? Explain in detail.	**8**

3.		What is AES? What are the major parameters used in AES? Explain the processing of plain text with a suitable diagram.	**16**

OR

4.	a)	What is the purpose of the S-Boxes in DES? What is the criteria to design S-Boxes?	**10**
	b)	Write note with proper diagram on key distribution scenario.	**6**

5.	a)	What is the strength of RSA? Explain.	**8**
	b)	Write note on	**8**

     i)   Digital signature.   ii)   Digital certificate.

OR

6.		Explain Diffie Hellman key Exchange Algorithm in detail. What is "Man-in-the middle attack" on Diffie Hellman algorithm?	**16**

7.	a)	What is X.509 certificate? Discuss.	**8**
	b)	Write note on.	**8**

     i)   Packet sniffing.   ii)   Packet spoofing.

OR

8.	a)	Explain in detail IP security architecture.	**8**
	b)	Write note on.	**8**

     i)   Kerberos.   ii)   Web Security Requirements.

9.	a)	What are the services provided by PGP? Why it is required?	**8**
	b)	Write a note on SSL.	**8**

OR

10.		Explain	**16**

     i)   Electronic Mail Security.   ii)   Intrusion Detection System.
     iii)   VPN.   iv)   Distributed intrusion detection.

****