B.E. Eighth Semester (Computer Science & Engineering) (CGS)

10358 : Professional Elective - II : Network Security : 8 KS 04 / 8 KE 04

P. Pages : 2 | AU - 3018

Time : Three Hours | Max. Marks : 80

* 0 6 8 7 *

Notes : 1. Due credit will be given to neatness and adequate dimensions.
2. Assume suitable data wherever necessary.
3. Illustrate your answer necessary with the help of neat sketches.
4. Use of pen Blue/Black ink/refill only for writing the answer book.

1.	a)	Explain cipher block chaining modes with the help of diagram and example.	7
	b)	What is Network security? Explain network security model.	7
		OR	
2.	a)	Explain DES algorithm in detail with its strength and drawback.	7
	b)	Explain the RFC publication procedure.	7
3.	a)	What are the requirement of hash function? Explain importance of each property.	7
	b)	What is public key cryptography? Explain RSA algorithm with suitable example.	6
		OR	
4.	a)	In public-key system using RSA, you intercept the ciphertext C = 10. sent to a user whose public key is e = 5, n = 35. What is the plaintext M?	7
	b)	How can message Authenticate by using a MAC?	6
5.	a)	State the problem that Kerberos address. Explain simple authentication dialogues with As and TGS for Kerberos for version 4.	7
	b)	What are the five services provided by PGP? Explain Authentication and confidentiality.	6
		OR	
6.	a)	Explain the general format of x.509 and revocation of certificate.	7
	b)	Explain s/MIME functionality in detail.	6
7.	a)	What is IPsec? List and explain its applications and benefits.	7
	b)	Explain web traffic security approaches with suitable diagram.	7
		OR	

http://www.sgbauonline.com

http://www.sgbauonline.com

8.	a)	What is secure Electronic transaction (SET)? Explain purchase request and payment.	**7**
	b)	What is an Authentication Header? Explain in detail.	**7**
9.	a)	Explain Network management protocol Architecture with the help of diagram.	**7**
	b)	Explain UNIX password scheme with diagram.	**6**

OR

10.	a)	What is Prony? Explain protocol architecture involving Prony.	**7**
	b)	Explain how to improve password security using proactive password checker?	**6**
11.	a)	List our types of firewall and explain packet filtering router with suitable diagram.	**7**
	b)	Explain taxonomy of malicious program.	**6**

OR

12.	a)	Explain Distributed Denial of service attacks with suitable diagram.	**7**
	b)	Explain the following malicious software. i) Backdoor. ii) Logic Bomb. iii) Trojan Horses.	**6**

****