

Reg. No. :

--	--	--	--	--	--	--	--	--	--	--

Question Paper Code: 92021

M.E. DEGREE EXAMINATION, DECEMBER 2013.

Elective

Communication Systems

01PCM509 - COMMUNICATION NETWORK SECURITY

(Regulation 2013)

Duration: Three hours

Maximum: 100 Marks

Answer ALL Questions.

PART A - (10 x 2 = 20 Marks)

1. What is the OSI security architecture?
2. What is steganography? How does it differ from cryptography?
3. What is meant by avalanche effect?
4. What are the evaluation criteria for AES?
5. Enlist the properties of digital signature.
6. Mention types of attacks addressed by message authentication.
7. What are the parameters required for security associations?
8. What is meant by dual signature with example?
9. What are the security threats in sensor network?
10. Define DoS attack.

PART - B (5 x 14 = 70 Marks)

11. (a) (i) List and briefly define categories of passive and active attacks. (8)
(ii) Explain the model of network security. (6)

Or

- (b) (i) Explain in detail security services. (8)

- (ii) Explain various method of steganography in network security. (6)
12. (a) (i) Explain any three substitution techniques and list their merits and demerits. (8)
- (ii) Perform encryption and decryption using RSA algorithm.
 $p = 3, q = 11, e = 7$ and message bill $m = 5$ (6)

Or

- (b) Explain various modes of operation in DES. List out the advantages and limitation of DES. (14)
13. (a) Explain in detail about how SHA used for authentication. (14)

Or

- (b) (i) Define biometrics authentication and explain how the biometrics used to provide entity. (7)
- (ii) Consider a Diffie – Hellman scheme with a common prime $q = 11$ and a primitive root $\alpha = 2$.
- a. If user A has public key $Y_A = 9$, what is A's private key X_A ?
- b. If user B has public key $Y_B = 3$, what is the shared secret key K, shared with A? (7)

14. (a) (i) Compare the mode transfers in IP sec services. (4)
- (ii) Discuss different types of firewall and compare their features. (10)

Or

- (b) What are the approaches for web security? Explain in detail SSL protocol stack architecture with neat diagram. (14)
15. (a) Write about the security issues in WEB for Wi-Fi network. (14)

Or

- (b) Write short notes on
- i) Assess the security for 4G networks. (7)
- ii) Security in Ad hoc network (7)

PART - C (1 x 10 = 10 Marks)

16. (a) Briefly explain principles and Architecture SET. (10)

Or

- (b) What are the requirements of Kerberos? Explain about Kerberos version 4. (10)