

Reg. No. :

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

Question Paper Code : 86541

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2021.

Sixth/Eighth Semester

Electronics and Communication Engineering

CS 1028 A – NETWORK SECURITY

(Regulations 2008)

Time : Three hours

Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Encrypt the following plain text using a Caesar cipher of key 20. Plaintext
Time and tide wait for none
2. Using rain fence of depth 2, encrypt the following plain text.
Plaintext: Our eyes determine the horizon
3. What is MAC?
4. What is meant by Digital Signature?
5. Give advantages of DES.
6. What is the need for Authentication?
7. What is a trusted system?
8. What are the important components of distributed IDS?
9. Write the types of WLAN.
10. What are the advantages of wireless LAN security?

PART B — (5 × 16 = 80 marks)

11. (a) Discuss the classical encryption techniques in detail.

Or

- (b) Explain the advanced encryption standards.

12. (a) (i) Consider a Diffie-Hellman key exchange scheme with a common prime $q = 71$ and a primitive root $a = 7$.

(1) If user A has private key $X_A = 5$, what is A's public key Y_A ?

(2) If user B has private key $X_B = 12$, what is B's public key Y_B ?

(3) What is the shared secret key? (8)

(ii) Briefly describe the RSA algorithm. (8)

Or

(b) Explain the requirements for authentication and digital signature and the basic authentication techniques.

13. (a) Explain about X.509 Authentication Service with a suitable illustration.

Or

(b) Describe the features of Encapsulating Security Payload in detail.

14. (a) What is Intrusion? And explain about Intrusion Detection techniques in detail. (16)

Or

(b) Explain about Firewall design principles in detail. (16)

15. (a) Discuss about the wireless LAN security standards. (16)

Or

(b) (i) Explain the key hierarchy of WLAN security. (8)

(ii) Write in detail about the confidentiality and integration of WLAN security. (8)
