

Reg. No. :

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

Question Paper Code : 61153

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2014.

Eighth/Sixth Semester

Electronics and Communication Engineering

CS 1028 A — NETWORK SECURITY

(Regulation 2008)

Time : Three hours

Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Convert the plaintext "anna university" into cipher text using rail fence transposition technique.
2. What is an avalanche effect in DES?
3. Find out gcd (161, 28) using Euclidean algorithm.
4. Mention any two applications of MAC.
5. What are the drawbacks of more secure authentication dialogue?
6. List out any two functions of S/MIME.
7. Define three classes of intruders.
8. What is a trusted system?
9. What is wireless LAN?
10. What is the need for wireless LAN security?

PART B — (5 × 16 = 80 marks)

11. (a) Describe briefly about DES in detail.

Or

- (b) What is the need for AES? Write about the features of AES and its evaluation criteria.

12. (a) Perform encryption and decryption using the RSA algorithm for $p = 5$; $q = 11$; $e = 3$ and $M = 9$.

Or

(b) Discuss briefly about authentication protocols.

13. (a) Write about Kerberos.

Or

(b) Discuss about ESP in detail.

14. (a) Explain about intrusion detection in detail.

Or

(b) Discuss about fire wall.

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

Or

(b) Describe about wireless LAN security factors and issues.

