

B.Tech III Year II Semester (R13) Regular & Supplementary Examinations May/June 2017
CRYPTOGRAPHY & NETWORK SECURITY
(Information Technology)

Time: 3 hours

Max. Marks: 70

PART - A
(Compulsory Question)

- 1 Answer the following: (10 X 02 = 20 Marks)
- (a) Convert the given text "WELCOME" into cipher text using rail fence technique.
 - (b) Define RC4.
 - (c) State whether symmetric & asymmetric cryptographic algorithm need key exchange.
 - (d) Define primality testing.
 - (e) What is DSS?
 - (f) Differentiate authentication and authorization.
 - (g) What is PGP?
 - (h) Define x.509.
 - (i) Differentiate spyware and virus.
 - (j) Define SSL.

PART - B
(Answer all five units, 5 X 10 = 50 Marks)

UNIT - I

- 2 Write about any two classical crypto systems with suitable examples.

OR

- 3 Write Ten strength's of the data encryption standard.

UNIT - II

- 4 Write short notes:

- (a) Chinese remainder theorem.
- (b) Linear congruence.

OR

- 5 Explain ELGamal cryptographic system in detail.

UNIT - III

- 6 Draw and explain cryptographic hash function with suitable example.

OR

- 7 Explain federated identity management in detail.

UNIT - IV

- 8 Write short notes:

- (a) Electronic mail security.
- (b) S/MIME.

OR

- 9 Explain remote user authentication using symmetric encryption.

UNIT - V

- 10 What is Malicious software? Explain in detail.

WWW.MANARESULTS.CO.IN

- 11 Explain security policies in detail.
