Code: 13A05702

R13

B.Tech IV Year I Semester (R13) Supplementary Examinations June 2018

CRYPTOGRAPHY & NETWORK SECURITY

(Computer Science & Engineering)

Time: 3 hours Max. Marks: 70

PART – A

(Compulsory Question)

*****

1 Answer the following: (10 X 02 = 20 Marks)

(a) Differentiate stream cipher and block cipher.

(b) Sketch neatly the decryption of output feedback mode.

(c) State Fermat's theorem.

(d) Differentiate conventional and public-key cryptosystem.

(e) What are the requirements of message authentication?

(f) What is one-way function?

(g) What are the ways to distribute public keys?

(h) What is S / MIME?

(i) Define security policy.

(j) What is IDS?

PART – B

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

UNIT – I

2 Explain in detail about OSI security architecture.

OR

3 (a) Explain the steps involved in RC4.

(b) Discuss different block cipher modes of operation

UNIT – II

4 Write short notes on: (i) Linear congruence. (ii) Exponentiation and discrete logarithm.

OR

5 (a) Explain in detail about Elgamal cryptosystem.

(b) In RSA system, the public key of given user e = 31, n = 3599 what is the private key of the user?

UNIT – III

6 With an example, explain in detail about Secure Hash Algorithm.

OR

7 Explain in detail about HMAC and Digital Signature Standard.

UNIT – IV

8 Explain in briefly about Kerbero and give its requirements..

OR

9 (a) Discuss in brief about PGP.

(b) Explain the format of X.509v3 certificate and certificate revocation list.

UNIT – V

10 (a) Briefly explain about transport layer security.

(b) With a neat diagram, explain the operation of SSL Record Protocol.

OR

11 (a) List the five important features of IKE Key determination algorithm.

(b) What are the design goals for a firewall? Also mention its limitations.

*****