322755 (22)

BE (7th Semester)

Examination, April-May, 2014

Branch : CSE, IT

CRYPTOGRAPHY & NETWORK SECURITY

Time Allowed : Three Hours

Maximum Marks : 80

Minimum Pass Marks : 28

Note : Part (a) of each question is compulsory. Solve any two parts from rest.

Q. 1. (a) Define cryptography and crytoanalysis. 2

(b) Explain various types of security attacks. 7

(c) Explain Data Encryption Standard Scheme along with working of each block associated with it. 7

(d) Write short note on any two :

(i) Transportation technique

(ii) Diffusion and confusion

(iii) Cipher block chaining mode

Q. 2. (a) What comman mathematical constants a used in RC5.

(b) Discuss Blowfish encryption algorithm. 7

(c) Write in detail about RC-05 characteristics and key generation technique. 7

(d) Discuss the basic criteria at AES evaluatio and it's round structure. 7

Q. 3. (a) What is need for Network Security ? 2

(b) Describe Diffie-Hellman key exchange algorithm 7

(c) Explain working of MD-5. 7

(d) Differentiate between conventional encryption and public key encryption. 7

Q. 4. (a) Differentiate between Transport mode & tunnel mode of authentication header. 2

(b) Discuss about digital signature standard & digital signature algorithm technique. 7

(c) Explain SSL & TSL architecture with diagram. 7

(d) Explain the operational description of PGP (Pretty Good Privacy). 7

Q. 5. (a) Define virus & its types. 2

(b) Discuss about firewall. 7

(c) Explain electronic payment system with an appropriate example. 7

(d) Explain various classes of intruders & also discuss types of intrusion techniques. 7