Reg. No.

B.E./B.Tech. DEGREE END SEMESTER EXAMINATIONS, APRIL / MAY 2011
INFORMATION TECHNOLOGY BRANCH
SEVENTH SEMESTER – (REGULATION 2004)
IT473 – CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 hr Max.Mark: 100

Answer ALL Questions
Part - A (10×2 = 20 Mark)

1. How to overcome the passive attack generated in a network?
2. How cryptanalysis is possible on mono-alphabetic ciphers?
3. Give the differences between conventional encryption and public-key encryption techniques
4. Find all the primitive roots of 10.
5. What are the possible ways to attack on hash functions?
6. Give the purpose of ticket granting server in Kerberos?
7. What is the role of ISAKMP in IPSec?
8. In PGP message format, what is the purpose of leading two octets of message digest?
9. What type of information does a typical packet filtering router use?
10. List the primary factors of security in a wireless environment.

Part – B
(5*16 = 80 marks)

11. a. (i) Discuss the block cipher modes of operation and give the advantages and disadvantages. (6)
(ii) How man-in-middle attack is performed over Diffie-Hellman key exchange algorithm? (10)

12 a. Discuss briefly about the Advanced Encryption Standard. (16)

(OR)

b. Discuss the algorithm developed by Rivest, Shamir and Adleman for implementing public key encryption. (16)

13 a.(i) Discuss briefly about the HMAC algorithm with the design objectives and security issues. (8)
(ii) State and prove Euler's theorem? Give the algorithm for finding out the multiplicative inverse of a number. (8)

(OR)

b. (i) Briefly explain the Digital Signature algorithm. (8)
(ii) Discuss about any two authentication protocols. (8)

14 a. Discuss briefly about the PGP used for E-mail security. (16)

(OR)

b. Discuss briefly about IP security architecture. (16)

15 a. Discuss briefly about the viruses and related threats in system security. (16)

(OR)

b. Discuss in detail about the wireless LAN security factors. (16)