(Pages : 2) **7672**

Reg. No. : .....

Name : .....

Eighth Semester B.Tech. Degree Examination, November 2015
(2008 Scheme)
08.803 : CRYPTOGRAPHY AND NETWORK SECURITY (R)

Time : 3 Hours Max. Marks : 100

PART – A

Answer **all** questions. **Each** question carries **4** marks.

1. Compare differential and linear cryptanalysis.
2. Distinguish between stream cipher and block cipher.
3. Define a trapdoor one way function and explain its use in asymmetric key cryptography.
4. What is double DES ? What kind of attack on double DES makes it useless ?
5. What is the difference between a MAC and a hash function ?
6. Show that Diffie-Hellman key exchange is insecure against man-in-the middle attack.
7. Explain how Bob finds out what cryptographic algorithms Alice has used when he receives a PGP message from her.
8. Compare Transport mode ESP and tunnel mode ESP.
9. List the security services provided by a digital signature.
10. What are the encrypted tunnels ? **(10×4=40 Marks)**

P.T.O.

PART – B

Answer **one full** question from **each** Module. **Each full** question carries **20** marks.

Module – I

11. a) Explain different transposition techniques used in cryptography. **10**

    b) List and briefly define types of cryptanalytic attackes based on what is known to the attacker. **10**

OR

12. Explain AES encryption algorithm and its security. **20**

Module – II

13. a) Alice wants to send a message to Bob. Alice wants Bob to be able to ensure that the message did not change in transit. Briefly outline the cryptographic steps that Alice and Bob must follow to ensure the integrity of the message by creating and verifying a MAC. **10**

    b) Consider a Diffie-Hellman scheme with a common prime q = 11 and primitive root $\alpha = 2$

    i) If User A has public key $Y_A = 9$, what is A's private key X_A.

    ii) If User B has public key $Y_B = 3$, what is the shared secret key, shared with A. **10**

14. a) What is the smallest value of a valid encryption key and the corresponding decryption key for an RSA modulus 143 ? **10**

    b) Describe Digital Signature Standards. **10**

Module – III

15. a) Explain Secure Socket Layer Protocol. **10**

    b) Describe different types of firewalls. **10**

OR

16. a) Describe S/MIME used for e-mail security. **10**

    b) How Encapsulating Security Payload (ESP) provide confidentiality and authentication ? **10**