(Pages : 2) **B – 2669**

Reg. No. : .....

Name : .....

Eighth Semester B.Tech. Degree Examination, December 2016
(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. List out some general approaches to attack a conventional encryption scheme.
2. Differentiate between polyalphabetic and monoalphabetic cipher.
3. How one-time pad offers complete security ? What are the difficulties of using one-time pad ?
4. Differentiate between diffusion and confusion.
5. Show that DES decryption is, in fact, the inverse of DES encryption.
6. What are the properties of Hash function ?
7. What are the factors which determine the security of elliptic curve cryptography ?
8. Compare two modes of IPSec.
9. PGP compresses the messages after applying the signature but before encryption. Justify your answer.
10. Compare and contrast existential and selective forgery.

PART – B

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

Module – I

11. Explain different substitution techniques used in cryptography. **20**

OR

12. a) Describe block cipher design principles. **10**

    b) What are the factors determining the strength of DES ? **10**

P.T.O.

Module – II

13. a) In the Diffie-Hellman protocol, what happens if x and y have the same value ? that is, Alice and Bob have accidently chosen the same number ? Do the session keys calculated by Alice and Bob have the same value ? Use an example to prove your claims. **10**

b) Briefly describe secure hash algorithm. **10**

OR

14. 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**

Module – III

15. a) Explain Transport Layer Security. **10**

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

OR

16. a) Briefly describe Pretty Good Privacy for e-mail security. **10**

b) Describe how secure electronic transaction is done. **5**

c) What is the significance of Encrypted tunnels in Transport layer security ? **5**