(Pages : 3) **K – 5600**

Reg. No. : .....

Name : .....

Eighth Semester B.Tech. Degree Examination, February 2021.

(2013 Scheme)

13.801 : CRYPTOGRAPHY AND NETWORK SECURITY (R)

Time : 3 Hours Max. Marks : 100

PART – A

Answer All Questions, Each Question carries 4 marks

1. Discuss Symmetric Cipher model
2. Encrypt the message "ATTACK POSSIBLE" using Caesar cipher assuming a suitable key.
3. State Fermat's theorem and Euler theorem and prove it using the values a=7 and p=13
4. What are the functions of S/MIME?
5. What are the limitations of firewalls?

PART – B

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

Module – I

6. (a) Explain how substitution and permutation techniques used in Feistal structure. **10**

   (b) Discuss the use of Feistal Structure in DES and strength of DES. **10**

OR

7. (a) What are the different block Cipher modes of operation in DES? 10

(b) Illustrate IDEA algorithm. 10

Module – II

8. (a) What are the ingredients of Public key Cryptosystem? 8

(b) Discuss SHA with block diagram and write SHA algorithm. 12

OR

9. (a) Explain Diffie-Hellman key exchange 5

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

(i) Show that 2 is a primitive root of 11 4

(ii) If user A has public key $Y_A = 7$ what is the private key X_A of A 5

(iii) If user B has $Y_B = 5$ compute the key that is exchanged. 6

Module – III

10. (a) What are the security services provided by ESP and AH? 10

(b) What are basic features of PGP? 10

OR

11. (a) Explain IPSec Architecture. 10

(b) Explain transport and tunnel mode of IPSec. 10

Module – IV

12. (a) Explain Encrypted tunnels. **12**

(b) Explain secure electronic transaction. **8**

OR

13. (a) Explain SSL record Protocol. **10**

(b) What are the capabilities of firewall? **5**

(c) Compare packet filters and application level gateway. **5**