Reg. No:……

Name:…….

Eighth Semester B.Tech Degree Examination,May 2017

(2013 Scheme)

13.801 CRYPTOGRAPHY AND NETWORK SECURITY (R)

Time : 3 Hours **Max.Marks :100**

PART-A

Answer ***all***questions, each question carries *four* marks.

1. What is the purpose of the S-boxes in DES? How the S-box is indexed in DES?
2. What is the difference between direct and arbitrated digital signature?
3. What are the functions of S/MIME?
4. List out the services provided by IPsec?
5. What is the function of Handshake protocol in SSL?

PART- B

Answer **any one full** questions from **each** module

Module-I

6. a)Using this Playfair matrix:

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

Encrypt this message:
"Meet me at the toga party" (5 Marks)

b) Explain any three Block cipher modes of operation in DES (15 marks)

OR

7 a) Illustrate the IDEA algorithm in detail (10 marks)

b) Explain the Key expansion in AES algorithm with a neat sketch? (10 marks)

Module-II

8 a)Explain in detail the RSA algorithm? (8 marks)

b)Perform encryption and decryption using the RSA algorithm for thefollowing:

$p = 3$; $q = 11$, $e = 7$;$M = 5$ (7 marks)

c) What is the difference between a message authentication code and a one-way hash function? (5 marks)

OR

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

1.Show that 2 is aprimitive root of 11

2. If user A has public key $Y_A = 9$, what is A's private key X_A ?

3.If user B has public key $Y_B = 3$, what is secret key K shared with A ?

(10 marks)

b)List four general categories of schemes for the distribution of public keys. (4 marks)

c) What are the requirements of a digital signature? (6 marks)

Module -III

10 a) What are the five principal services provided by PGP? (10 Marks)

b) Discuss the major security services provided by AH and ESP (10 Marks)

OR

11 a)What is the differences between transport and tunnel mode operation? (5 marks)

b)Explain the two security protocols provided by IPsec? (15 Marks)

Module –IV

12 a)What is the difference between an SSL connection and an SSL session? (5 marks)

b)Explain the operation of SSL Record Protocol? (15 marks)

OR

13 a)Explain the construction of dual signature in Secure Electronic Transaction? (10 marks)

b)Describe the different types of firewalls (10 marks)