No.									

MANIPAL INSTITUTE OF TECHNOLOGY
(Constituent Institute of Manipal University)
MANIPAL-576104

SIXTH SEMESTER B.E.(CSE) DEGREE END SEMESTER EXAMINATION
MAY 2013
CRYPTOGRAPHY AND NETWORK SECURITY(CSE 324)
PROGRAM ELECTIVE 1
DATE: 13-05-2013

TIME: 3 HOURS MAX.MARKS: 50

Instructions to Candidates

- Answer **any FIVE** full questions.
- Missing data if any, may be suitably assumed

1A. Explain the following security mechanisms
(i)Traffic Padding (ii)Routing Control
(iii)Notarization (iv)Event Detection

1.B.Using the Playfair Cipher matrix given in Table Q.1.B , encrypt the message

Must see you over Cadogan West Coming at once

Table Q.1 (B)

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

1.C.Explain the Fiestel encryption and decryption techniques with neat diagrams.

1.D. What are stream ciphers? Show the encryption and decryption process of stream cipher generation using a peudorandom byte generator.

(2+2+4+2)

2.A.Explain the AES-128 key expansion algorithm with a neat diagram.

2.B. Explain the Triple DES encryption method that uses two keys and three keys. Discuss the known plain text attack on Triple DES with two keys.

2.C.Explain the Electronic Codebook Mode of operation of DES. What is the security deficiency of ECB and how is it overcome in CBC mode, explain.

(3+4+3)

3.A.Using Blum Blum Shub pseudorandom generator, generate the sequence given the following parameters: p=7, q=11, and initial seed=2. Find the period of the sequence

3.B.State and prove Fermat's Theorem.

3.C.Write the Diffie Hellman key exchange algorithm and show how is it susceptible to man in the middle attack.

(3+3+4)

4.A. Given the parameters, p=7, q=3, d=5, using RSA algorithm, find the public key e, sign and verify the message m=2.

4.B.Define a hash function. Explain the various steps in inducing birthday attack on the hash function.

4.C.What are Message Authentication codes. How are they computed? Explain how MAC could be used to provide the following functions

(i)Message Authentication.

(ii) Message Authentication and confidentiality: authentication tied to plaintext

(iii) Message Authentication and confidentiality: authentication tied to ciphertext.

(3+3+4)

5.A. What is replay attack? Explain how Anti replay mechanism is implemented in IPSecurity.

5.B. With necessary diagrams, show how key rings are used in PGP message generation and reception.

5.C.What is a computer virus? Explain the various phases that a virus undergoes during its lifetime

(3+4+3)

6.A.Explain any four parameters associated with SSL session state.

6.B.Give the format of ESP packet and explain the functions of each and every field.

6.C.Explain briefly the various approaches to intrusion detection

6.D What are Packet filtering firewalls? Explain. List any two limitations of Packet filtering firewalls

(2+3+3+2)