



Reg. No. :

Name :

**Eighth Semester B.Tech. Degree Examination, April 2016
(2008 Scheme)**

CRYPTOGRAPHY AND NETWORK SECURITY (R)

Time : 3 Hours

Total Marks : 100

PART – A

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

I. 1) Using the following play air matrix, encrypt the message :

CRYPTO IS THE BEST

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

- 2) Define a state in AES. How many states are there in each version of AES ?
- 3) Using the Vigenère cipher, encrypt the word “explanation” using the key LEG.
- 4) What is steganography ?
- 5) Perform encryption using RSA algorithm $p = 5, q = 11, e = 3, M = 9$.
- 6) What are the properties for hash function which is used in cryptographic algorithms ?
- 7) Briefly describe about the Secure Hash Algorithm.
- 8) What are the applications of IPsec. ?
- 9) Explain message digest creation in SHA-512.
- 10) Show how public keys can be distributed using public key certificates ?



PART – B

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

Module – I

- II. a) In a cipher, S-boxes can be either static or dynamic. The parameters in a static S-box do not depend on the key. State some advantages and some disadvantages of static and dynamic S-boxes. Are the S-boxes (substitution tables) in AES static or dynamic ? **10**
- b) Describe Mixcolumn transformation of AES. **10**

OR

- III. a) What is the difference between a block cipher and a stream cipher ? **6**
- b) Use a Hill cipher to encipher the message "We live in an insecure world". Use the following key :

$$K = \begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$$

7

- c) Encrypt the message "this is an exercise" using one of the following ciphers. Ignore the space between words. Decrypt the message to get the original plaintext.
- i) Additive cipher with key = 20
- ii) Multiplicative cipher with key = 15
- iii) Affine cipher with key = (15, 20). **7**

Module – II

- IV. a) Explain Diffie-Hellman key exchange algorithm. What is its main drawback ? **12**
- b) Define elliptic curve and explain their application in cryptography. **8**

OR

- V. a) Elaborate the significance of message authentication code. What ensures the security of MAC ? **12**
- b) Explain the general idea behind DSS scheme. **8**

Module – III

- VI. a) How is confidentiality and authenticity provided using PGP ? **10**
- b) Explain about IPSec in detail. **10**

OR

- VII. a) Explain the significance of transport layer security. **5**
- b) What are the key features of secure electronic transaction ? **5**
- c) What are the different types of firewalls ? Explain. **10**