BE/INSEM/APR - 587
B.E. (Computer) (Semester - II)
410251: INFORMATION & CYBER SECURITY
(2015 Pattern)

Time : 1 Hour]

[Max. Marks : 30

Instructions to the candidates :

1) *Answer Q1 or Q2, Q3 or Q4, Q5 or Q6.*

2) *Figures to the right side indicate full marks.*

3) *Assume suitable data, if necessary.*

Q1) a) Define Cryptography, Encrytion, Decryption, Plain text, Cipher text & Cryptanalyst. **[5]**

b) What are different security policies? Explain. **[5]**

OR

Q2) a) Explain Passive and Active attacks with examples. **[5]**

b) What is Cryptanalysis? Explain various Cryptanalysis technique. **[5]**

Q3) a) Write short note on Electronic code book. **[5]**

b) Use Playfail Cipher to encrypt the message "Weliveina world full of beauty". Use key 'ANOTHER'. **[5]**

OR

Q4) a) Explain DES Algorithm with diagram. **[5]**

b) Explain simple columnar techniques with multiple rounds. **[5]**

P.T.O.

Q5) a) What is HMAC? Discuss different objectives of HMAC. Explain HMAC in brief. **[5]**

b) Use RSA algorithm to encrypt plaintext "3" use following parameters $p = 11$, $q = 3$, $e = 13$. **[5]**

OR

Q6) a) Explain operation of MDS Message digest algorithm. **[5]**

b) Explain Elliptic curve Cryptography in detail. **[5]**

✳ ✳ ✳