

**GUJARAT TECHNOLOGICAL UNIVERSITY**

**BE - SEMESTER- 6 EXAMINATION – Summer 2015**

**Subject Code: 160702**

**Date:04/05/2015**

**Subject Name : Information Security**

**Time:10.30AM-01.00PM**

**Total Marks: 70**

**Instructions:**

1. Attempt all questions.
2. Make suitable assumptions wherever necessary.
3. Figures to the right indicate full marks.

- Q.1 (a)**
- (i) Encrypt the message “Exam” using the Hill cipher with the key  $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ . **04**
- (ii) Write the subkey and S-Box generation in Blowfish. **03**
- (b)**
- (i) Explain cipher feedback mode of operation. **04**
- (ii) Given the seed to be 101355, generate first five bits of random number with the help of blum blum shub generator. **03**
- Q.2 (a)**
- (i) Perform encryption using the RSA algorithm. **04**  
p=3,q=11(two random numbers).  
e(encryption key)=7  
M(plaintext message)=5
- (ii) Evaluate Euler’s totient function  $\Phi(37)$ . **03**
- (b)** Explain Elliptic curve algorithm. **07**
- OR**
- (b)** Explain Diffie – Hellman key exchange. **07**
- Q.3 (a)** Explain the steps involved in International data encryption standard algorithm. **07**
- (b)** How message authentication code can be used to achieve message authentication and confidentiality? **07**
- OR**
- Q.3 (a)** Explain scheme for DES encryption. **07**
- (b)** Which techniques are used for the distribution of public keys? **07**
- Q.4 (a)**
- (i) Write the benefits of IPSec. **04**
- (ii) When an encryption scheme is said to be unconditionally secure and computationally secure? **03**
- (b)** Write cast -128 encryption algorithm. **07**
- OR**
- Q.4 (a)**
- (i) Write the properties of hash functions. **04**
- (ii) Explain the fields included in ESP(Encapsulating security payload) packet. **03**
- (b)** Explain pretty good privacy. **07**
- Q.5 (a)**
- (i) Why E-commerce transactions need security? **04**
- (ii) Explain the use of firewall. **03**
- (b)** Write MD5 algorithm. **07**

**OR**

**Q.5 (a)**

(i) Which type of substitution is called monoalphabetic substitution cipher? **01**

(ii) Which two principal methods are used in substitution ciphers to lessen the extent to which the structure of the plaintext survives in the ciphertext? **02**

(iii) Use playfair algorithm with key “monarchy” and encrypt the text “jazz”. **04**

**(b)** Define SSL session and SSL connection. Which parameters define session state and connection state. **07**

\*\*\*\*\*