

GUJARAT TECHNOLOGICAL UNIVERSITY
BE – SEMESTER – VI EXAMINATION – WINTER 2015

Subject Code:160702**Date:17/12/ 2015****Subject Name: Information Security****Time:2:30pm to 5:00pm****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) 07**
- (i) Define the term – confusion, diffusion.
- (ii) Use Hill cipher to encrypt the text DEF. The key to be used is
- $$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 8 & 7 \end{bmatrix}.$$
- (b) 07**
- (i) The encryption algorithm to be used is RSA. Given two prime numbers 11 and 3 and public key (e) is 3. Calculate the decryption key and Calculate the ciphertext if the given plaintext is 7.
- (ii) What is MIME and S/MIME?
- Q.2 (a) 07**
- (i) Using playfair cipher encrypt the plaintext “Why, don’t you?”. Use the key “keyword”.
- (ii) How Encryption is done in blowfish? Include calculation of function in explanation.
- (b) 07**
- Write the general format of PGP(pretty good privacy) message.
- OR**
- (b) 07**
- Define pseudorandom number generators. Explain Linear congruential generators and blum blum shub generator.
- Q.3 (a) 07**
- What is the difference between passive and active security threats? List and briefly define categories of passive and active security attacks.
- (b) 07**
- (i) Explain the key expansion algorithm used in RC5.
- (ii) Apply Euclid’s algorithm and find greatest common divisor of 28,42.
- OR**
- Q.3 (a) 07**
- Explain single round of DES algorithm.
- (b) 07**
- (i) Explain the feistel structure used in cast-128?
- (ii) What four requirements were defined for Kerberos?
- Q.4 (a) 07**
- Define the term cryptanalysis. Explain various types of cryptanalytic attacks.
- (b) 07**
- What parameters identify an SA(security association) and what parameters characterize the nature of SA(security association)?
- OR**
- Q.4 (a) 07**
- In symmetric encryption, Describe the ways in which key distribution can be achieved between two parties A and B?

- (b) Describe MD5 message digest algorithm. **07**
)
- Q.5** (a) What is a dual signature? Explain in detail the following transactions supported by SET(secure electronic transaction) **07**
(i) Purchase request
(ii) Payment authorization
- (b) **07**
) (i) What characteristics are needed in a secure hash function?
(ii) Give examples of replay attacks. List three general approaches for dealing with replay attacks.
- OR**
- Q.5** (a) Define – SSL session and SSL connection. Which parameters are used to define SSL state and SSL connection? **07**
- (b) **07**
) (i) What is the purpose of X.509 standard?
(ii) How following can be achieved with message authentication code(MAC)?
a. Message authentication
b. Message authentication and confidentiality
