Seat No.: ________ Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VI • EXAMINATION – SUMMER 2013

Subject Code: 160702 **Date: 27-05-2013**

Subject Name: Information Security

Time: 10.30 am - 01.00 pm **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) Define the types of cryptanalytic attacks. Which cryptnalytic attack can occur on RSA algorithm? **04**

(ii) Is playfair cipher monoalphabetic cipher? Justify. Construct a playfair matrix with the key ñmoonmissionò and encrypt the message ñgreetò. **03**

(b) What is the difference between fiestel structure of Blowfish and cast-128? Explain the fiestel structure of Blowfish and cast-128. **07**

Q.2 **(a)** (i) What is a pseudorandom number? Selection of which values are critical in developing a good linear congruential generatos. **04**

(ii) Calculate ciphertext in case of RSA if p=3,q=11,e=3,M=5. **03**

(b) Explain four passes of MD5 message digest algorithm. **07**

OR

(b) Explain the operation of secure hash algorithm on 512 bit block. **07**

Q.3 **(a)** (i) Write two properties of prime numbers. **04**

(ii) Explain Eulerôs totient function. **03**

(b) (i) What is included in authorization request sent by merchant to the payment gateway in case of E-commerce transaction? **04**

(ii) Which tasks are performed by payment gateway in E-commerce transaction? **03**

OR

Q.3 **(a)** (i) Describe the three operations used by International Data Encryption Algorithm. **04**

(ii) Is message authentication code same as encryption? How message authentication can be done by message authentication code? **03**

(b) (i) Explain packet filtering router in case of firewall. **04**

(ii) What type of verification is provided by trusted system? **03**

Q.4 **(a)** What is a nonce in key distribution scenario? Explain the key distribution scenario if A wishes to establish logical connection with B. A and B both have a master key which they share with itself and key distribution center. **07**

(b) Explain the pseudorandom function used by Transport layer security. **07**

OR

Q.4 **(a)** Write Diffie Hellman key exchange algorithm. Explain man-in-the middle attack on this Diffie Hellman key exchange. **07**

(b) Explain the secure socket layer handshake protocol action. **07**

Q.5 **(a)** What does authentication header provide in case of IP security?Explain the various fields in Authentication Header. **07**

(b) Explain the functions provided by S/MIME . **07**

OR

Q.5 **(a)** How encapsulating security payload help in IP security? Explain various fields in Encapsulating security payload packet. **07**

(b) What steps sending PGP(pretty good privacy) perform? Explain PGP message generation. **07**