DHARMSINH DESAI UNIVERSITY, NADIAD
FACULTY OF TECHNOLOGY
B.TECH. SEMESTER VII [Information Technology]
SUBJECT: (IT IT 710) E-COMMERCE AND E-SECURITY

Examination	**:Second Sessional**	**Seat No.**	**:** _____
Date	**: 02/09/2013**	**Day**	**:Monday**
Time	**:** 1:00 to 2:15	**Max. Marks**	**: 36**

INSTRUCTIONS:
1. Figures to the right indicate maximum marks for that question.
2. The symbols used carry their usual meanings.
3. Assume suitable data, if required & mention them clearly.
4. Draw neat sketches wherever necessary.

Q.1 Do as directed. **[12]**

(a) What is the difference between session key and master key? [2]

(b) What is difference between the public key cryptosystem and conventional cryptosystem? [2]

(c) How cryptography is different than message digest , explain with appropriate example [2]

(d) Show that 2 is a primitive root of 11. [2]

(e) If Sender sends message encrypted with [2]
   (1) His Private Key
   (2) Receiver's Public Key
   Then these different encryption techniques provide which facility? Consider each case separately. (Hint : consider Authentication and Confidentiality)

(f) What is difference between MD5 and SHA-1 [2]

Q.2 Attempt any two from the following questions. **[12]**

(a) Explain the algorithm to compute $a^b \bmod n$ for a=88, b=7, n=187. [6]

(b) Describe Diffe Hellman Key Exchange Algorithm [6]

(c) Perform Encryption and Decryption using the RSA algorithm for the following: [6]
   p=3
   q=10
   e=7
   M=5

Q.3 Attempt the following questions. **[12]**

(a) Explain Key Distribution using Public Key Authority with appropriate figure [6]

(b) Explain MD5 message authentication technique with appropriate figure [6]

OR

Q.3 Attempt the following questions. **[12]**

(a) Explain SHA-1 message authentication technique. [6]

(b) Describe how to achieve secrecy, authentication and both using Public key cryptosystem with appropriate figure. [6]