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

Examination	**: Second Sessional**	**Seat No.**	**: _____**
Date	**: 01/04/2014**	**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) Write down difference between public key cryptography and Conventional Cryptography [at least four steps] [2]
(b) Explain Requirements for public key cryptography? [2]
(c) Explain Applications of public key cryptography? [2]
(d) Which are the counter measures we can take to overcome the Timing Attack on RSA? [2]
(e) Write down difference between MD5 and SHA 1 [2]
(f) If I want to compute W_{67} for SHA 1 then which words are taken in to consideration and how to get W_{67}? [2]

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

(a) How Confidentiality, Authentication, Confidentiality and Authentication are achieved using Public Key Cryptography with proper figure and explanation. [6]

(b) Compute 7^{560} mod 561 using a^b mod n method. [6]

(c) Explain types of attack possible on RSA algorithm [6]

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

(a) Explain Hash Function which has generated 128 bit message digest with proper figures and explanations. [6]

(b) Write down RSA algorithm and compute public key and private key using following data: [6]
p =11 , q= 3 , e=7

OR

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

(a) Explain Hash Function which use four 32 bit buffer registers for generating message digest with proper figures and explanations. [6]

(b) Explain Diffie-Hellman algorithm and compute only public key and private key using following data: [6]
$\alpha = 23$ and $q=5$
$X_A = 6$ and $X_B = 15$