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

Examination	**:Second Sessional**	**Seat No.**	**: _____**
Date	**: 10/09/2012**	**Day**	**: Monday**
Time	**: 12:30 To 1:45**	**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 conventional Encryption and public key encryption [2]
(b) Write down requirements of public key cryptography given by Diffie-Hellman [2]
(c) Which are the counter-measures use to prevent timing attack? Explain in brief. [2]
(d) If A is prime root of B, what is the definition of prime root? Why we need it in Diffie-Hellman? [2]
(e) How does a "hash function" work? Explain in terms of how it provide authentication at receiver side. [2]
(f) Give the definitions for the following: [2]
    1. Weak collision resistance
    2. Strong collision resistance

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

(a) Draw the figure MD5 algorithm. Explain the logic in very brief steps. [6]

(b) Explain RSA algorithm in brief. And compute the public key and private key from the given data. [6]
P=3 , q=11, e=7,M=5

(c) Explain how we can achieve Confidentiality, Authentication and both using public key cryptography system. Explain it with appropriate diagrams. [6]

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

(a) Draw the diagrams of processing of single SHA-1 512-bit block and its Elementary operation. . Explain the logic in brief. [6]
(b) If user A have private key $X_A = 5$, User B have private key $X_B = 12$. Both have $\alpha = 7$ and $q = 6$. [6]

OR

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

(a) Explain with figure that how we can distribute public key using public-key authority. [6]
(b) Compare the following algorithms: [6]
    1) MD5 with SHA-1
    2) MD5 with MD4.