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

Examination	**:Block Exam**	**Seat No.**	**: _____**
Date	**: 27/10/2012**	**Day**	**: Saturday**
Time	**: 9:30 to 10:45**	**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) Draw the Model of Conventional Cryptosystem and write all its components [2]
(b) List out diffie - hellman requirement for public key cryptosystem. [2]
(c) List the selectors for SPD entry in IPSEC. [2]
(d) List two requirement using we can say key or algorithm is computationally secure [2]
(e) Importance of Dual signature. [2]
(f) Why we use diffie - hellman algorithm? [2]

Q.2 Attempt all of the following questions. **[12]**

(a) Draw and explain X.509 certificate with its fields. [6]

(b) Explain the process of Secure Electronic Transaction in Detail. [6]

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

(a) Explain following block cipher modes. Also state what is difference (operational) between given modes. [6]
   1) cipher feedback mode
   2) Electronic code book mode

(b) Find out cipher text for given problem using RSA. [6]
P=5,q=11,e=3,Message='I' (don't consider epos top).