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

Examination	**: First Sessional**	**Seat No.**	**: _____**
Date	**:29 /07/2013**	**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) Which two characteristics must exist if encryption algorithm is computationally Secure Encryption algorithm? [2]

(b) Draw the Simplified model of Conventional Encryption and its five ingredients. [2]

(c) State types of attack possible on encrypted message and what is to be known to cryptanalyst for those attack. [2]

(d) Encrypt following plain text using reil-fence technique. [2]

Plaintext : "I love my india and mera bharat mahan" with depth =2

(e) What is difference between end to end and link to link encryption. [2]

(f) State advantage of play-fair cipher over the mono-alphabetic cipher technique. [2]

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

(a) Explain Key Distribution Scenario with appropriate figure. [6]

(b) Explain key generation of S-DES with proper figure. [6]

(c) Encrypt following using play-fair cipher. [6]
plaintext : "Hello my dear students"
key : monarchy

Q.3 Attempt the following questions. [12]

(a) Draw which part of IP packet encrypted when packet pass from following level. [6]
1) application-level encryption
2) TCP-level encryption
3) Link-Level encryption

(b) Explain Pseudorandom Number Generators (PRNGs) and calculate it for $a=7, c=0, m=32$ $X_0=1$. [6]

OR

Q.3 Attempt the following questions. [12]

(a) Explain ANSI X9.17 PRNGs with proper figure and explanation. [6]

(b) Perform encryption using hill-cipher using following data: [6]

$$\text{Key} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

And plain text = "indian"