DHARMSINH DESAI UNIVERSITY, NADIAD
FACULTY OF TECHNOLOGY
B.TECH. SEMESTER V [INFORMATION TECHNOLOGY]
SUBJECT: E- COMMERCE & E-SECURITY

Examination	**: First Sessional**	**Seat No.**	**: _____**
Date	**: 31/07/2017**	**Day**	**: Monday**
Time	**:**	**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.(No Marks Without Justification)

(a) If EK(P)denotes an encryption of the plaintext block P with the key K by the block cipher E, then the cipher Output FeedBack (OFB) mode of operation can be described with the following equations: **[2]**
(i) Ci = EK(Ci-1 XOR Pi XOR Oi), Oi = Ci, C-1 = IV
(ii) Ci = Pi XOR Oi, Oi = EK(Oi-1), O-1 = IV
(iii) Ci = EK(Pi), Oi = EK(Oi-1)
(iv) Ci = Ci-1 XOR EK(Pi), C-1 = IV
(v) Ci = Pi XOR EK(i)

(b) Define: 1) Nonrepudiation 2) Masquerade. **[2]**

(c) Which attack is very efficient against Double-DES? **[2]**

(d) Differentiate link encryption & end-to-end encryption. **[2]**

(e) Encrypt the following using transposition cipher where key is: 1342 **[2]**
Plain Text is: I LOVE MY COUNTRY.

(f) What are cryptanalysis and cryptography? **[2]**

Q.2 Attempt ***Any Two*** from the following questions. **[12]**

(a) Explain key distribution scenario with proper figure and step by step explanation. **[6]**

(b) Explain Pseudorandom Number Generators (PRNGs) and calculate it for a=5, c=1, m=64, X_0=1. **[6]**

(c) Encrypt the given message using the Hill cipher: **[6]**
Plain text: puzzle
Key:

$$\begin{pmatrix} 8 & 9 & 5 \\ 6 & 2 & 3 \\ 1 & 4 & 7 \end{pmatrix}$$

Q.3 (a) Find the cipher text of the plain text 0010 1000 using S-DES algorithm. **[8]**
Key: 11000 11110 ; P10: 3,5,2,7,4,10,1,9,8,6 ; P8: 6,3,7,4,8,5,10,9 ;
IP: 2,6,3,1,4,8,5,7 ; E/P: 4,1,2,3,2,3,4,1 ; P4: 2,4,3,1

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

(Note: Generate Key1 by 1 shift and Key2 by total 2 shifts)

(b) List and briefly define categories of active and passive security attacks. **[4]**

OR

Q.3 (a) Explain block cipher modes of operations. **[6]**

(b) Solve the following questions using playfair cipher: **[6]**
1. Construct a table for the Playfair Cipher with the keyword EFFECTIVENESS?
2. Encrypt the phrase: “EXAMFORINFORMATIONSECURITY”
3. Decrypt the sequence: “PQFVCKFUFBGMUFYSTIKZKAGWWG”