DHARMSINH DESAI UNIVERSITY, NADIAD
FACULTY OF TECHNOLOGY
B.TECH. SEMESTER V [INFORMATION TECHNOLOGY]
SUBJECT: E- COMMERCE & E-SECURITY [IT-710]

Examination	**: First Sessional**	**Seat No.**	**: _____**
Date	**: 30/07/2017**	**Day**	**: Monday**
Time	**: 2:30 – 3:45**	**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.(No Marks Without Justification)

(a) Suppose that everyone in a group of 15 people wants to communicate secretly with the 14 others using symmetric key cryptographic system. The communication between any two persons should not be decodable by the others in the group. How many keys required in the system as a whole to satisfy the confidentiality requirement? **[2]**

(b) Give an example of polyalphabetic substitution cipher. **[1]**

(c) Which attack is very efficient against double DES? **[1]**

(d) Mention the type of attack for the statements given below (one word answer) : **[3]**
(I)An attacker sits between customer and Banker, and captures the information from the customer and retransmits to the banker by altering the information.
(II)An attack meant to shut down a machine or network, making it inaccessible to its intended users.
(III)An attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification.

(e) Give advantages of using One-Time Pad. **[1]**

(f) Define Non-Repudiation. **[1]**

(g) What is Traffic Padding? Why it is needed? **[1]**

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

Q.2 Attempt ***Any Two*** from the following questions.

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

(b) Encrypt the given plain text using hill cipher: **[6]**
plain text: "EFFECT"
Key matrix M = $\begin{vmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{vmatrix}$

(c) (I) Solve the following questions using playfair cipher: **[3]**
1. Construct a table for the Playfair Cipher with the keyword EFFECTIVENESS?
2. Encrypt the phrase: "protect your password".

(II) Generate at least 10 random numbers using PRNG's linear congruential method for the data given as : multiplier =5, constant=1, modulus=64 and seed=1. **[3]**

Q.3 (a) Find the cipher text of the plain text 0110 0001 using S-DES algorithm. **[8]**
Key: 11010 11001 ; 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: 4,3,1,2,2,3,4,1 ; P4: 2,4,1,3

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

(b) List and define security services by X.800. **[4]**

OR

Q.3 (a) Explain any three block cipher modes of operations with proper diagram. **[6]**

(b) Find the plain text for a cipher text "EOMNTSCKUEECWOLIYRXTTOERW" using double columnar transposition cipher with a key "LAYER". **[6]**
