DHARMSINH DESAI UNIVERSITY, NADIAD
FACULTY OF TECHNOLOGY
B.TECH. SEMESTER V [INFORMATION TECHNOLOGY]
SUBJECT: E- COMMERCE & E-SECURITY [IT-718]

Examination	**: First Sessional**	**Seat No.**	**: _____**
Date	**: 29/07/2019**	**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) What should be the minimum length of an encryption or decryption secret key in a cryptosystem that cannot be cracked by brute-force means within a reasonable period of time? **[1]**
(A) 32 bits (B) 56 bits (C) 64 bits (D) 128 bits

(b) Which of the following cryptosystems, if implemented properly, is impenetrable? **[1]**
(A) Substitution Cryptosystem (B) Vigenere Cryptosystem
(B) transposition Cryptosystem (D) One-time pad

(c) Which cipher is commonly used in network-based symmetric cryptographic applications? **[1]**
(A) Linear cipher (B) Block cipher (C) Permutation cipher (D) Stream cipher

(d) Which cipher encrypts a digital data stream one bit or one byte at a time? **[1]**
(A) Product cipher (B) Block cipher (C) Key cipher (D) Stream cipher

(e) How many rounds a Data Encryption Standard (DES) system has with an initial and final permutation block? **[1]**

(f) For what purpose Cryptanalysis is used? **[1]**

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

(h) List out the steps of AES algorithm. **[2]**

(i) What is meet in middle attack? **[2]**

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

(a) (i)List and briefly define categories of attacks. **[3]**
(ii)Consider following algorithm for Encryption: **[3]**

1)Transform each of the letters in the plaintext alphabet to the corresponding integer in the range 0 to m-1. Consider this integer as "x".
2)With this done, the encryption process for each letter is given by:
E(x) = (ax+b) mod m. Note: where a and b are the key for the cipher and m is number of alphabets.Using the using the key a= 5, b = 8 transform the plain text "MARCH" into cipher text.

(b) (i) Describe the scheme given in figure:1. **[6]**
(ii)Compare this scheme with the centralised key distribution traditional scheme along with the pros and cons.

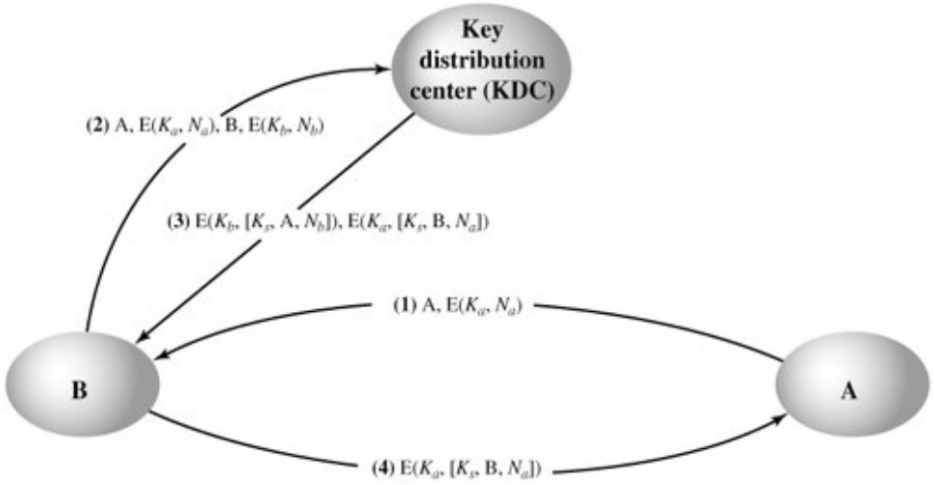

Figure:1

(c) (i) Describe ANSI X9.17 PRNG pseudorandom number generation scheme with neat diagram. **[3]**

(ii) Generate at least 10 random numbers using PRNG's linear congruential method for the data given as : multiplier =5, constant=1, modulus=32 and seed=1. **[3]**

Q.3 (a) Find the cipher text of the plain text 1111 1111 using S-DES algorithm.
Key: 11111 11111 ;
P10: 3,5,2,7,4,10,1,9,8,6 ; **[8]**
P8: 6,3,7,4,8,5,10,9 ;
IP: 2,6,3,1,4,8,5,7 ;
E/P: 4,3,2,1,1,2,3,4 ;
P4: 1,3,4,2

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

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

OR

Q.3 (a) Solve the following using hill cipher: **[8]**
(i) Encrypt the plain text: “cryptography”
(ii)Decrypt the cipher text: “DZYNAG”
Key matrix M = | 1 2 3 |
| 0 1 4 |
| 5 6 0 |

(b) Explain any two block cipher mode of operation technique with proper figure. **[4]**
