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

Examination	**: First Sessional**	**Seat No.**	**: _____**
Date	**: 01/08/2016**	**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) Define: 1) Nonrepudiation 2) Masquerade. **[2]**
(b) What is/are drawback of substitution ciphers? **[2]**
(c) Differentiate link encryption & end-to-end encryption. **[2]**
(d) What is the advantage of Advance Encryption Standard? **[2]**
(e) What are the differences between AES & DES? **[2]**
(f) What are cryptanalysis and cryptography? **[2]**

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

(a) List and briefly define categories of active and passive security attacks. **[6]**
(b) Explain S DES algorithm with diagram. **[6]**
(c) (a) Cryptanalyze the following message that was encrypted using columnar transposition: ABEEESWHTTRE. **[3]**
(b) How many possible keys does the playfair cipher have? Ignore the fact that some keys might produce identical encryption result. Express your answer as an approximate power of 2. **[3]**

Q.3 (a) List and briefly define categories of security services. **[6]**
(b) Encrypt the message "SPRING" using the Hill cipher with the key [9 4 5 7] (matrix form: a11= 9, a12 = 4, a21= 5, a22= 7). Show your calculations. **[6]**

OR

Q.3 (a) Explain block cipher modes of operations. **[6]**
(b) Using Playfair matrix : **[6]**

M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

Encrypt this message: BEYOND THE OBVIOUS.