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

Examination	**: External – Regular**	**Seat No.**	**: ________________**
Date	**: 22/11/2021**	**Day**	**: Monday**
Time	**: 1:30 hours**	**Max. Marks**	**: 30**

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.
5. Follow the following file name convention for uploading the document: **BTech_Semester_IDNo_SubjectCode_SubjectName.pdf**

SECTION – II

Q.1 Attempt *any three* following questions. [12]

(a) Explain how authentication and confidentiality are achieved using public key cryptography with appropriate diagram. **[4]**

(b) Draw & explain B2C e-Commerce of a customer buying cell phone from Amazon.com from his home or place of work. **[4]**

(c) What is block cipher modes of operations? Explain any two with appropriate diagram. **[4]**

(d) Mention and define the types of attack possible on RSA. **[4]**

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

Q.2 Attempt the following questions.

(a) Explain Handshake protocol of Secure Socket Layer. **[6]**

(b) Explain the Modular Exponentiation Algorithm. Using the same algorithm to compute a^b mod n for a=88, b=7 and n =187. **[6]**

(c) Consider a Diffie-Hellman key generation algorithm using which A and B wants to communicate securely. Let modulus q = 19 and alpha a=7 are the two global parameters. The private numbers chosen by A & B are Xa = 8 and Xb=10 respectively. Using the given data attempt the following questions: **[6]**

1) A’s key generation Ya
2) B’s key generation Yb
3) Shared secret keys of both A and B

OR

Q.2 Attempt the following questions.

(a) Explain Kerberos system with proper diagram. **[6]**

(b) Suppose the plain text is “COVID PANDEMIC”. Now transform the plain text into cipher text using the following procedure for Encryption: **[6]**

(1) Transform each of the letters in the plaintext alphabet to the corresponding integer in the range 0 to m-1(m is 26). 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).Given a= 7 and b = 1.

(3) Now transform the text obtained from step (2) using columnar transformation technique with keyword “VIRUS”.

(c) A certain application uses DES algorithm for securing the data. If the secure key is given as 11001 10011 Then Find out the cipher text for the plain text 1010 0110. Consider following information: **[6]**

P10: 5, 7, 9, 10, 8, 3, 1, 2, 4, 6
P8: 9, 7, 1, 8, 2, 3, 4, 6
IP: 2, 6, 4, 1, 8, 3, 7, 5
E/P: 4, 1, 2, 3, 1, 2, 4, 3
P4: 4 ,3 ,2 , 1

S0

	C0	C1	C2	C3
R0	0	1	2	3
R1	1	3	0	2
R2	3	2	1	0
R3	2	0	3	1

S1

	C0	C1	C2	C3
R0	1	3	2	1
R1	2	1	3	0
R2	3	0	1	2
R3	0	2	0	3