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

Examination:	**Second Sessional**		
Date:	**6/9/2021**	**Time:**	**1:15 to 2:30 (45 mins for descriptive exam)**

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:2	Attempt ***Any Two*** from the following questions.	[8]
(a)	Consider the following scheme by which B encrypts a message for A. 1. A chooses two large primes P and Q that are also relatively prime to (P1) and (Q1). 2. A publishes N = PQ as its public key. 3. A calculates P' and Q' such that PP'= 1 (mod Q1) and QQ'= 1 (mod P1). 4. B encrypts message M as C = M^N mod N. 5. A finds M by solving M =$C^{P'}$ (mod Q) and M = $C^{Q'}$ (mod P). i) Describe how this scheme works. ii) How does it differ from RSA? iii) Is there any particular advantage to RSA compared to this scheme?	[4]
(b)	Summarize the Diffie-Hellman key exchange algorithm. Compute private and shared secret key if a=23, q=5, Xa=6 and Ya=15.	[4]
(c)	Draw and explain compression function of SHA-1.	[4]

Q:3 (a)	Explain how public key cryptosystem use to achieve confidentiality, authentication, authentication and confidentiality both.	[6]
(b)	What is timing attack in RSA?	[2]
	OR	

Q:3 (a)	Draw and explain key distribution scenario using public key authority with proper figure.	[6]
(b)	How would you differentiate MD5 with SHA1.	[2]