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

Examination	**: Second Sessional**	**Seat No.**	**: _____**
Date	**: 06/09/2016**	**Day**	**: Tuesday**
Time	**: 2:15 – 3:30**	**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) Using public key cryptography, X adds a digital signature P to message M, encrypts < M, P >, and sends it to Y, where it is decrypted. Which sequences of keys are used for these operations? [2]

(b) If we want to compute W_{58} in SHA-1 then which words are taken into consideration and how to get W_{58} ? [2]

(c) Write the differences between MD5 and SHA-1.(At least 4) [2]

(d) If X is prime root of Y, What is the definition of prime root? Why we need it in Diffie-Hellman? [2]

(e) Define: (i) Weak collision resistance (ii) Strong collision resistance. [2]

(f) Which are the counter measures we can take to overcome the timing attack on RSA? [2]

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

(a) Explain RSA algorithm in brief. And compute public key and private key from following data: p=7, q=13, e=5 and d=29. [6]

(b) Explain birthday attack. Give step by step explanation. [6]

(c) Explain all techniques of arbitrated digital signature. [6]

Q.3 (a) Consider a Diffie-Hellman scheme with a common prime q=11 and primitive root a=2. [6]

(i) Show that 2 is a primitive root of 11.

(ii) If user A uses public key Y_A =9, what is A's private key X_A?

(iii) If user B uses public key Y_B =3, what is the shared secret key K?

(b) Explain and draw all needed diagrams of message digest algorithm which generates 160 bit message digest, explain the logic in brief with its elementary operations. [6]

OR

Q.3 (a) Compute 7^{560} mod 561 using a^b mod n method. [6]

(b) How confidentiality, authentication, confidentiality and authentication are achieved using public key cryptography with proper figure and explanation. [6]