DHARMSINH DESAI UNIVERSITY, NADIAD
FACULTY OF TECHNOLOGY
B.TECH. SEMESTER VII [Information Technology]
SUBJECT: (IT 710) E-Commerce & E-Security

Examination	**:Second Sessional**	**Seat No.**	**: ________________**
Date	**: 31/08/2015**	**Day**	**:Monday**
Time	**: 1:00 TO 2:15**	**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. [12]

(a) Write down requirements of public key cryptosystem proposed by Diffie-hellman [2]

(b) Write down difference between public key cryptosystem and private key cryptosystem. [2]

(c) Write a difference between MD 5 and SHA -1 [2]

(d) Explain timing attack on RSA and write method to resolve it. [2]

(e) Write and briefly explain different ways of distribution of public key. [2]

(f) Write down the application of public key cryptosystem. [2]

Q.2 Attempt any two from the following questions. [12]

(a) Write an algorithm of RSA and compute Cipher text using following data [6]
P=11, q=13 e=11 and M=7

(b) Explain how public key cryptosystem use to achieve confidentiality, authentication, authentication and confidentiality both. [6]

(c) Write a key distribution scenario using public key authority with proper figure. [6]

Q.3 Attempt the following questions. [12]

(a) Explain SHA-1 with appropriate figures. [6]

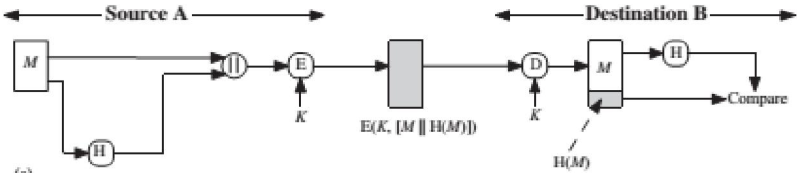
(b) Calculate the secret key using diffie –hellman key generation algorithm. [6]
$\alpha = 7$, q=71, X_A=5 , X_B=12

OR

Q.3 Attempt the following questions. [12]

(a) Explain message digest algorithm which generate 128 bits of message digest with proper figure. [6]

(b) [6]



Explain step by step process done by above figure.
Which are the security requirements achieved by above figure.