R

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

Examination	:Block Sessional	Seat No.	: ______________
Date	: 16/10/2014	Day	:Thursday
Time	: 11 to 12:15	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) What is the use of alert protocol and cipher specification change protocol of SSL ? [2]

(b) Explain reil fence cipher technique [2]

(c) Explain requirements of public key algorithms [2]

(d) List the conditions in which X.509 certificate get revoked? [2]

(e) Explain Dual signature [2]

(f) What is difference between conventional and public key encryption [2]

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

(a) Explain S-DES key Generation [6]

(b) Explain Handshake protocol of Secure Socket Layer [6]

(c) Explain how can we achieved authentication , authorization and secrecy using public key algorithm [6]

Q.3 Attempt the following questions. **[12]**

(a) Explain Diffie hellman algorithm [6]

(b) Explain Key Distribution center (KDC) scenario [6]

OR

Q.3 Attempt the following questions. **[12]**

(a) Explain RSA algorithm with appropriate example [6]

(b) Draw and explain each and every field X.509 certificate format [6]