



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

**Examination** : Third Sessional  
**Date** : 07/10/2014  
**Time** : 1:00 TO 2:15

**Seat No.** : \_\_\_\_\_  
**Day** : Monday Tuesday  
**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) If user A registered under x1 authority and user B registered under X2 C.A. then how they can exchange public key? [2]
- (b) Write down four application of Kerberos [2]
- (c) What is difference between tunnel mode and transport mode? [2]
- (d) List the conditions in which X.509 certificate get revoked? [2]
- (e) What is the use of alert protocol and cipher specification change protocol of SSL ? [2]
- (f) [12]

**Q.2 Attempt any two from the following questions.**

- (a) Explain Secure Electronic Transaction with appropriate figures. [6]
- (b) Explain Handshake protocol of Secure Socket Layer [6]
- (c) Explain Three way authentication using X.509 [6]

**Q.3 Attempt the following questions.**

[12]

- (a) Explain Kerberos Version 4 dialogue [6]
- (b) Draw the IPv4 and IP v6 packet format for tunnel mode and transport mode for ESP of IPSec. [6]

**OR**

**Q.3 Attempt the following questions.**

[12]

- (a) Draw the Business to Business e-commerce model. [6]
- (b) Draw and explain each and every field X.509 certificate format [6]