Examination	:Third Sessional	Seat No.	: _____
Date	: 15/10/2012	Day	: Monday
Time	: 1 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) Define Security Association and which parameters are used to Uniquely identify SA? [2]

(b) List out Real world application of Kerberos (At least Four) [2]

(c) If user A and B are under different CA then What is the meaning of following [2]
statement and why this statement are required?
X1<<x2>>X2<<B>>
X2<<X1>> X1<<A>

(d) In Which layer SSL works ? List out three protocol for SSL. [2]

(e) Explain the process how to create Dual-Signature? [2]

(f) Give definition of the following [2]
    1) IP spoofing attack
    2) Tiny fragment attack

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

(a) Write down authentication dialogue of Kerberos Version 4 [6]

(b) Explain Handshake protocol in brief for SSL [6]

(c) Explain Types of Firewall with advantage and disadvantage. [6]

Q.3 Attempt the following questions. [12]

(a) Explain the process of Secure Electronic Transaction in Detail. [6]
[with proper figures]

(b) Draw Packet formats of IPV4 and IPV6 for tunnel mode and transport mode after [6]
applying the ESP Authentication and Encryption in IPSEC.

OR

Q.3 Attempt the following questions. [12]

(a) Draw the IPSEC AH Authentication mode header and explain how it provides Anti- [6]
replay service and Integrity Check Value

(b) Draw the E-commerce model for the following situation. [6]
Owner of the car Show room, when stock goes below the limit, want to get stock of
TATA-NANO car from regional distributor of TATA company .