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

Examination	**: Third Sessional**	**Seat No.**	**: _____**
Date	**: 10/10/2016**	**Day**	**: Monday**
Time	**: 2:15 to 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) Which type of authentication should a company that has all computers in one domain use to ensure authentication of all clients and servers with the least administrative effort? Assume that all client computers run Windows XP Professional and all servers run Windows Server 2003. **[2]**
(1) Certificates (2) Preshared keys (3) Kerberos (4) MD5

(b) Which types of encryption protocols can be used to secure the authentication of computers using IPSec? **[2]**
(1) Kerberos (2) Certificates (3) SHA (4) MD5 (5) Digital Signature

(c) Explain Difference between tunnel mode and transport mode. **[2]**

(d) Why IPSec is important? Explain in brief. **[2]**

(e) What is the significance of Sequence Number in AH and ESP protocols? **[2]**

(f) What is SSL Session and SSL Connection? **[2]**

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

(a) Explain with proper diagram: Handshake protocol of Secure Socket Layer. **[6]**

(b) Explain any three types of firewalls in detail. **[6]**

(c) Explain SET with proper diagrams. **[6]**

Q.3 (a) Explain Kerberos. What are the limitations and benefits of Kerberos? **[6]**

(b) (i) What is the importance of dual signature? Explain with proper diagram. **[3]**
(ii) Draw and explain IPv4 and IPv6 packet format of ESP protocol. **[3}**

OR

Q.3 (a) Explain each and every field of X.509 certificate format. **[6]**

(b) (i) Briefly explain S/MIME functionality. **[3]**
(ii)What is Security Association? List out parameters that uniquely identify the Security Association. **[3]**