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

Examination	**: Second Sessional**	**Seat No.**	**: _____**
Date	**: 09/10/2017**	**Day**	**: Monday**
Time	**: 1:15 to 2:30**	**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) In tunnel mode IPSec protects the **[2]**
(i) Entire packet (ii) IP Header (iii) IP Payload (iv) None of the mentioned

(b) Which two types of encryption protocols can be used to secure the authentication of computers using IPSec? **[2]**
(i) Kerberos (ii) Certificates (iii) SHA (iv) MD5

(c) In which layer SSL works? List out three protocols of SSL. **[2]**
(d) What is the significance of Sequence Number in IPSec protocols? **[2]**
(e) What is SSL Session and SSL Connection? **[2]**
(f) List out parameters that uniquely identify the Security Association. **[2]**

Q.2 Attempt ***Any Two*** from the following questions.

(a) What is the importance of dual signature? Explain with proper diagram. **[6]**

(b) Draw IPv4 and IPv6 packet format for tunnel mode and transport mode of AH protocol. **[6]**

(c) What is Kerberos? Write down Kerberos version 4 dialogues. **[6]**

Q.3 (a) Explain Handshake protocol of Secure Socket Layer. **[6]**

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

OR

Q.3 (a) Explain SET with proper diagrams. **[6]**

(b) Draw and explain header format of ESP protocol. **[6]**