Terna Engineering College, Nerul
Question Bank (Cryptography and System Security)
Class: TE; Department: Computer Science;

Q. no.	Questions
i)	Explain IPSec protocol in detail. Also, write about the applications and advantages of IPSec.
ii)	Describe challenge-response based authentication
iii)	Give detailed explanation on entity authentication with its types and example.
iv)	Describe various types of firewalls with example.
v)	Discuss various attacks on digital signatures and the methods by which they can be overcome?
vi)	What are the different components of an Intrusion Detection System?
vii)	Explain Boot Sector Virus in detail.
viii)	What is the purpose of a digital signature in a digital certificate, and how does the RSA-based signature algorithm work?
ix)	Explain the handshake protocol in SSL?
x)	What are the different types of viruses and worms? How do they propagate?
xi)	Discuss the need for Email Security. How does PGP achieve confidentiality and authentication in emails?
xii)	Explain the different types of SQL injections? Discuss mitigation techniques for SQL injection.
xiii)	Explain ARP spoofing in detail with example.
xiv)	Explain DOS and DDOS attack? Explain how it is launched.
xv)	How is security achieved in transport and tunnel modes of IPSec? What are security associations?
xvi)	What is ICMP flood attack? Explain in detail.
xvii)	Discuss layer wise TCP/IP vulnerabilities.
xviii)	What is a buffer overflow in C? Why gets () is bad?
xix)	Differentiate between SQL injection and buffer overflow.