Cyber Forensics

(CS-552)

Assignment--2

1. Analyze how is the Security Association used in the following parameters:

(a) Security Policy Database
(b) Security Association Database
(c) Transport Mode SA
(d) Tunnel Mode SA

2. Explain in detail about SSL Handshaking Protocol between a Server and Client Connection with an appropriate diagram.

3. Explain S/MIME and the general syntax it uses to support different content types.

4. What is PGP? What key size is allowed in PGP? How does PGP provide encryption and authentication?

5. Draw the OSCAR framework for network forensics methodology and explain the steps involved.

6. A company named 'Alpha' has noticed many suspicious entries and IP addresses while observing the log records. Further, some clients have reported that they have been receiving a message prompt, redirecting them to a payment gateway that does not look genuine. You are now the forensic investigator. Explain:

(a) How will you ascertain if malware activity has been taken place or malware is present in the systems?
(b) How will you disinfect malware-affected machines?
(c) How will you ensure that the malware activity has been not spread to all other systems in the network?
(d) Perform forensic investigation and trace the causes for the incidents.