Assignment: 5

① Define authentication system. Illustrate the need of mutual authentication over one-way authentication with example.

⇒ Q.No.1 of Assignment 4.

② Define SSL protocol. Mention the services provided by PGP.

⇒ SSL (Secure Sockets Layer) is a cryptographic protocol designed to provide secure communication over a computer network. SSL has been deprecated in favor of TLS (Transport Layer Security) due to security vulnerabilities.

Service Provided by PGP (Preety Good Privacy)

PGP is an encryption program that provides security for emails, files and other communications. It uses a combination of symmetric and asymmetric encryption techniques.

Key services of PGP:

① Confidentiality
② Authentication
③ Integrity
④ Non-Repudiation
⑤ Key Management

③ Answer of Q.No.3

When we refer to SSL/TLS as a stack of pRotocols, we mean that it is not a single, monolithic protocol, but rather a collection of multiple protocols working together to provide secure communication. Each protocol within the stack has a specific role, such as negotiating encryption settings, authenticating parties, securely transmitting data, and ensuring data integrity.

The SSL/TLS stack consists of four main protocols:

① Handshake Protocol
② Record Protocol
③ Alert Protocol
④ Change Cipher Spec Protocol

How These Protocols Work Together in SSL / TLS:

① Handshake Protocol: Client & Server negotiate encryption settings
② Change Cipher Spec Protocol: Signals that encryption should begin
③ Record Protocol: Handles encrypted communication.
④ Alert Protocol: Reports errors and alerts.

⑦ Define Malware. Clarify and explain them.

⇒ Malware (Malicious Software) is any software designed to disrupt, damage, steal data, or gain unauthorized access to computer systems or networks. It is created by cybercriminals to exploit security vulnerabilities for various malicious purposes.
Malware can be classified based on its behavior and attack mechanisms. Some of them are:

Malware Type	How it Spreads	Effects
Virus	Needs a host file	Corrupts files, spreads via execution
Worm	Spreads via network	Consume bandwidth, slows system
Trojan	Disguised as software	Allows remote access, data theft
Ransomware	Sent via email, infected sites	Encrypts files, demands ransom
Spyware	Installed secretly	Steals user data.
Adware	Bundled with free software	Shows intrusive ads
Rootkit	Hidden in system files	Grants admin access to hackers
Botnet	Infected computers	Used for large-scale attacks
Keylogger	Hidden software/hardware	Records keystrokes, steals passwords.

⑧ Explain Types of trojans.

⇒ A Trojan Horse (Trojan) is a type of malware that disguises itself as legitimate software but once executed, grants unauthorized access or performs malicious actions on a system.

Trojan Types	Function	Effects
Backdoor	Provides remote access	Hackers control the system
Rootkit	Hides malicious activities	Maintains long-term access
Banker	Steals banking credentials	Financial fraud, identity theft
Ransom	Encrypts data, demand ransom	Data loss, financial extortion
Infostealer	Collects sensitive information	Identify theft, data leaks
Downloader	Installs more malware	System compromise, further infections
DDos	Launches DDos attacks	Server crashes, network disruption
SMS	Sends premium-rate SMS	High phone bills, SMS-based fraud
Fake Antivirus	Pretends to be antivirus software	Scams users for money
Game-Thief	Steals gaming accounts	loss of in-game assets

⑨ Explain types of virus

⇒ A computer virus is a malicious program that attaches itself to a legitimate file or software and spreads when executed. Viruses usually require human intervention (E.g. opening an infected file) to propagate.

S.N	Classification of Viruses:	Function:
①	Boot Sector Virus	Infects boot sector
②	File Infector Virus	Attaches to executable files
③	Macro Virus	Infects macro-enabled documents
④	Polymorphic Virus	Changes code to evade detection
⑤	Metamorphic Virus	Rewrites its own code
⑥	Resident Virus	StepsStays in system memory
⑦	Non-Resident Virus	Infects files when executed
⑧	Multipartite Virus	Infects boot sectors & files
⑨	Overwrite Virus	Overwrites file content
⑩	Spacefiller Virus	Uses empty space in files
⑪	Web scripting Virus	Exploits web browser vulnerabilities

S.N	Effects	Spread Method
(1)	Prevents system from booting	Infected bootable media
(2)	Corrupts programs & system files	Email attachments, software download
(3)	Modifies documents, spread via email	Word, Excel files, email attachments
(4)	Hard to detect and remove	Infected files, phishing emails
(5)	Advanced & harder to detect	Infected downloads, attachments
(6)	Constanly infects files	USB drives, network connections
(7)	Does not stay in memory	Infected files, removable media
(8)	Spreads in multiple ways	Software downloads, bootable media
(9)	Destroys data permanently	Infected email attachments
(10)	Hard to detect	Infected executable files
(11)	Executes scripts, steals data	Malicious websites, infected ads

(10) Differentiate between Worm and Virus

⇒ Both worms and viruses are types of malware, but they differ in how they spread and operate:

Feature	Virus	Worm
Definition	A self-replicating malware that attaches to a legitimate file and requires human execution to spread.	A self-replicating malware that spreads automatically without user interaction.
Spreading Mechanism	Spreads when the infected file or program is executed.	Spreads across networks & systems automatically.
Dependence on Host	Requires a host file to infect	Doesn't need a host file; standalone
Propagation speed	Slower, as it needs user actions.	Faster, as it spreads via network vulnerabilities
Damage Type	Corrupts or modifies files & system data	Consumes system resources, causing slowdowns or crashes
Examples	ILOVEYOU Virus, CIH (Chernobyl)	Wannacry, Morris Worm
Prevention Method	Avoid running unknown files, use antivirus software, keep OS updated.	Use firewalls, update network security, disable unnecessary network services.

(12) What is PEP? explain. Compare PEP and PGP.

⇒ PEP stands for Privacy-Enhanced Mail (PEP). It is a set of standards developed to provide security features like confidentiality, message integrity, etc for email communication. It was designed to improve the security of email using encryption and digital signatures. However, it has not been widely adopted due to complexity and competing technologies.

Differences between PEP and PGP are:

Feature	PEP (Privacy-Enhanced Mail)	PGP (Pretty Good Privacy)
Purpose	Secure email communication	Secure email, files & communication
Encryption	Uses asymmetric encryption with public key infrastructure	Uses both symmetric and asymmetric encryption.
Authentication	Uses digital certificates (x.509)	Uses digital signature (Web of Trust)
Adoption	Limited adoption due to complexity.	Widely used & supported
Key Management	Relies on centralized certificate authorities (CAs)	Decentralized, uses a Web of Trust model
Complexity	More complex and requires CA for trust verification.	Easier to use with self-signed keys.

Answer of Q. No. 13

⇒ Connection: A connection in SSL/TLS is a single communication link between a client and a server. It is a transient, peer-to-peer communication channel that ensures secure data exchange.

Session: A session in SSL/TLS is a set of cryptographic security parameters that can be shared accross multiple connections. A session helps in reducing handshake overhead by reusing security parameters for multiple secure connections.

Yes, a session can include multiple connections. for eg: in HTTPS a brower can establish multiple parallel TCP connections to the same server using a single SSL/TLS session to improve performance.

Connection State Vs. Session State in SSL/TLS

Feature	Connection State	Session State
Definition	Represents the security parameters for a specific connection.	Represents shared security parameters accross multiple connections.
Scope	Specific to a single secure connection.	Can be reused for multiple connections.
Components	Includes encryption keys, MAC keys, sequence numbers, and cipher suite.	Includes session ID, cipher suite, master secret, and compression method.
Duration	Exists only for the duration of a connection.	Can persist and be resumed later using session resumption
Security Role	Ensures encryption and integrity of a single connection.	Allows efficient security management accross multiple connections.

Security features Applied to Each

1. Connection State Security features:
   - Encryption using session keys
   - Integrity checks using Message Authentication Codes
   - Sequence numbers to prevent replay attacks.
   - Each connection has a unique set of symmetric encryption keys
2. Session State Security features
   - Session resumption (reduces handshake overhead)
   - Secure negotiation of cryptographic parameters
   - Prevents frequent full handshakes, reducing CPU and latency overhead.

(14) What is certificate and why are certificates needed in public key cryptography?

⇒ A certificate in public key cryptography is a digitally signed document that binds a public key to a specific entity. It is issued by a Certificate Authority (CA) and serves as a means of verifying the authenticity of the entity holding the corresponding private key.
Certificates address key challenges in public key cryptography, such as trust and authentication. Their main purposes include:

① Authentication
② Trust Establishment
③ Integrity and security
④ Encryption in Secure Communication

(15) Explain the structure of X.509 certificate.

⇒ An X.509 certificate is a digital certificate format widely used in SSL/TLS, email encryption, and digital signatures. It follows the ITU-T X.509 standard and contains various fields that help verify the authencity and integrity of the certificate.
An X.509 certificate is encoded in ASN.1 (Abstract Syntax Notation One) and commonly represented in PEM (Base64) or DER (binary) format. It consists of three main parts:

① Certificate Information (Main body of the certificate)
② Signature Algorithm (Defines the algorithm used for signing the certificate)
③ Digital Signature (Cryptographic signature from the certificate Authority)

Fields in an X.509 Certificate

Below are the key fields in an X.509 v3 certificate, which is the most commonly used version:

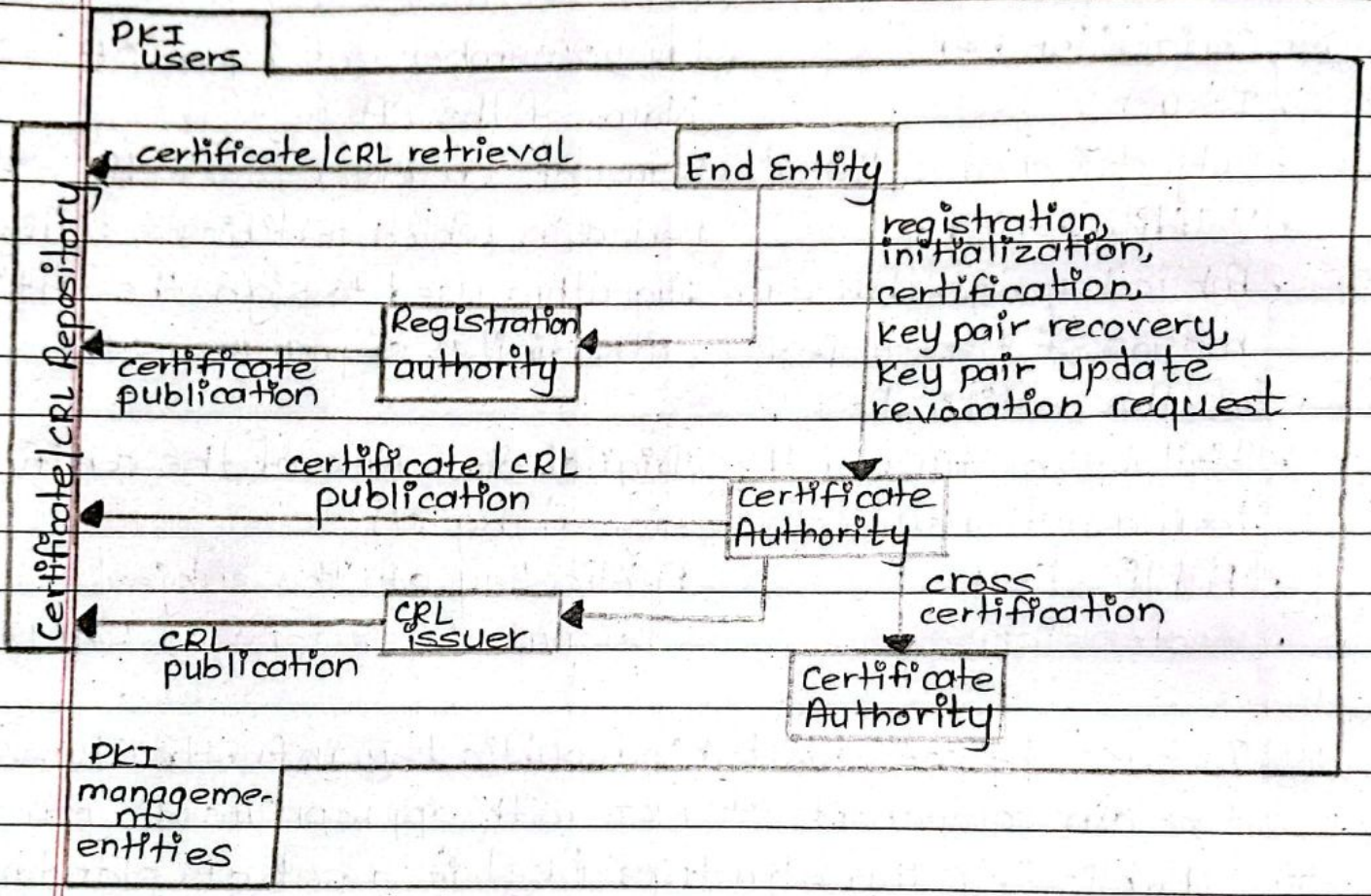
Field	Purpose
• Version Number	Most certificates use X.509 version 3
• Serial Number	Unique number set by a CA
• Issuer	Name of the CA
• Subject issued certificate	Name of a receiver of certificate
• Validity period	Period in which certificate will valid
• Public-key algorithm information of the subject of the certificate	Algorithm used to sign the certificate with digital signature
• Digital Signature of the issuing authority	Digital signature of the certificate signed by CA
• Public Key	Public key of the subject
• Extension	Optional Extensions (eg. Key Usage)

(16) Describe the concepts behind public key infrastructure. Explain components of PKI with appropriate diagram.

⇒ Public Key Infrastructure (PKI) is a set of standards, procedures, software, and people for implementing authentication using public key cryptography. It is used to request, install, configure, manage and revoke digital certificates. PKI offers authentication via digital certificates, and these digital certificates are signed and provided by certificate authorities.

It is made up of four major pieces: the certificate that represent the authentication token; the CA that holds the ultimate decision on subject authentication; the registratio

authority (RA) that accepts and processes certificate signing requests on behalf of end users; and the LightWeight Directory Access Protocol (LDAP) directories that hold publicly avaible certificate Information.



(17) What are the possible phases that a virus can go through, during its lifecyle?

⇒ A computer virus typically goes through four main phases during its lifecyle:

① Dormant phase (Optional): The virus remains inactive within the system. It waits for specific condition to activate.

② Propagation phase: The virus replicates itself by infecting files, programs or systems.

③ Triggering phase: The virus activates based on specific

conditions.

④ Execution Phase (Payload Delievery): The virus carries out its malicious intent, which could include :- Data corruption, System disruption, Opening backdoors for hackers, etc.

⑱ How rabbits and bacterium can be malicious to a secure system?

⇒ A rabbit (also called fork bomb) is a type of denial-of-serivice (DoS) attack that continuously spawns processes, consuming CPU and memory resources until the system crashes or becomes unresponsive. It harms a secure system by:

(i) Exhausting system resources (CPU, memory)
(ii) Causing system slowdown or complete crash.
(iii) ~~fan~~ evading detection by appearing as a normal process.

A bacterium is a type of malware that self-replicates aggressively but does not necessarily cause direct harm beyond resource consumption. It harms a secure system by:

(i) Consuming storage space by continuously replicating itself.
(ii) Slowing down system performance by using disk I/O.
(iii) leading to disk failure if left unchanged.

⑳ How many layers are in the TCP/IP protocol suite for internet communications? Name the layers. Name some of the protocols in each layer.

⇒ The TCP/IP protocol suite consists of four layer for internet communications. The layers and some associated protocols are:-

① Application layer: It provides network services to applications, enabling user interaction with the network.
Protocols: HTTP, HTTPS, FTP, SMTP, POP3, DNS

② Transport layer: It provides reliable or connectionless data transport between devices. Protocols: TCP, UDP

③ Internet layer: It handles addressing, packet forwarding, and routing. Protocols: IP (IPv4, IPv6), ICMP, ARP, IGMP

④ Network Access layer (Link layer): It defines hardware addressing and how data is physically transmitted over network media. Protocols: Ethernet, Wi-Fi, PPP, MAC

(22) What is certificate and why are certificates needed in public key cryptography.

⇒ ~~A certificate in public key~~ Q. No. 14

(26) What is the role of the SSL Record Protocol in SSL/TLS?

⇒ The SSL Record Protocol is a fundamental component of the the SSL/TLS suite. It operates at the Transport Layer and is responsible for securely transmitting data between applications over a network. Functions of the SSL Record protocols are:

① Fragmentation - Breaks application data into smaller chunks.
② Compression - Reduces data size before encryption
③ Message Authentication - Adds a MAC to ensure data integrity
④ Encryption - Encrypts the data using symmetric encryption
⑤ Encapsulation - Wraps the encrypted data into SSL/TLS records before transmission
⑥ Decryption and Integrity Check - On the receiving end, decrypts and verifies the MAC to detect tampering.

(27) Define PKI Trust Model.

⇒ A Public Key Infrastructure (PKI) Trust Model defines how trust is established and managed in a public key cryptography system. It determines how entities verify and authenticate digital certificates to ensure secure communication and data integrity.

Importance of PKI Trust Model:

(i) Ensures authentication, confidentiality, and integrity of digital communications.

(ii) Prevents man-in-the-middle (Mit·M) attacks and certificate spoofing.

(iii) Enables secure web browsing, email encryption, digital signatures, and VPNs.

(28) What are the services provided by IPSec?

⇒ IPSec is a security protocol suite that ensures secure communication over IP networks. It provides the following key services:

(i) Access Control - To prevent an unauthorized access to the resource.

(ii) Connectionless integrity - to give an assurance that the traffic received has not been modified in any way.

(iii) Confidentiality - to ensure that Internet traffic is not examined by non-authorized parties.

(iv) Authentication - to verify the identity of communicating parties using protocols like Authentication Header (AH) and Internet Key Exchange (IKE)

(v) Replay protection - to guarantee that each packet exchanged bet' two parties is different.

(29) What is meant by intrusion detection system? Differentiate IPS and IDS:

⇒ An Intrusion Detection System (IDS) is a security solution that monitors network traffic or system activities for suspicious behavior, unauthorized access, or potential cyber threats. It alerts administrators when an attack or anomaly is detected but does not take direct action to block it.

Differences between IPS and IDS are:

feature	Intrusion Detection System (IDS)	Intrusion Prevention System (IPS)
function	Detects and alerts about security threats	Detects threats and actively blocks them
Response	Passive (generates alerts but does not intervene)	Active (prevents malicious activity)
Placement	Monitors network traffic but does not sit-in-line.	Sits in-line betⁿ sender and receiver to block threats
Action on threats	Logs and reports suspicious activity.	Blocks, drops, or modifies malicious packets.
Example Tools	Snort (IDS mode), Suricata, OSSEC	Snort (IPS mode, Cisco FirePOWER
Use case	Suitable for monitoring and analysis	Suitable for real-time threat prevention.

(30) What is meant by intruder? Explain its types.

⇒ An intruder is an a unauthorized entity that attempts to gain access to a system, network, or data with malicious intent. Intruders exploit vulnerabilities to steal, modify, or disrupt information.

Types of Intruders:

(1) Masquerader (Outside Attacker)

- An external attacker who pretends to be an authorized

user to gain access.
- Example: Hackers using stolen credentials to log into a system

② Misfeasor (Insider Attacker)
- An authorized user who misuses their privileges to perform malicious activities.
- Example: An employee leaking confidential data or abusing system access.

③ Clandestine User (Advanced Attacker)
- A highly skilled intruder who bypasses security controls and remains undetected.
- Example: A hacker modifying system logs to erase tracks of their attacks.