**CCS354 NETWORK SECURITY**

**PART A**

**UNIT-I INTRODUCTION**

**1.What is public-key cryptography?**

Publickey cryptography uses two keys:

 a public key for encryption and a private key for decryption.

**2.Define conventional cryptography.**

Conventional cryptography uses a single key for both encryption and decryption.

**3.What are hash functions?**

Hash functions are algorithms that convert input data into a fixed-size string of characters, which uniquely represents the input.

**4.Explain digital signatures.**

Digital signatures are cryptographic signatures that authenticate the identity of the sender and ensure message integrity.

**5.What is the primary use of cryptography?**

Cryptography ensures secure communication and data protection by encrypting information.

**6.How does authentication differ from authorization?**

Authentication verifies the identity of a user, while authorization determines what resources the user can access.

**7.Describe the purpose of encryption.**

Encryption transforms data into an unreadable format to prevent unauthorized access.

**8.What is symmetric key encryption?**

Symmetric key encryption uses the same key for both encryption and decryption.

**9.Define public key.**

A public key is a cryptographic key that can be distributed openly and used to encrypt messages.

**10.What is a private key?**

A private key is a cryptographic key kept secret by its owner and used to decrypt messages.

**Unit II: Key Management and Authentication**

PART-A

**1.What are X.509 certificates?**

X.509 certificates authenticate the identity of entities and securely exchange public keys over a network.

**2.Explain symmetric key distribution.**

Symmetric key distribution is the process of securely exchanging a shared secret key between parties for encryption and decryption.

**3.What is a Public-Key Infrastructure (PKI)?**

PKI is a system for managing digital certificates and public-key encryption to ensure secure communication.

**4.Describe the role of Kerberos in user authentication**.

Kerberos uses secret key cryptography and a trusted third party to authenticate users in a network.

**5.What is remote user authentication?**

Remote user authentication verifies the identity of a user accessing a system from a remote location.

**6.Define asymmetric encryption.**

Asymmetric encryption uses a pair of keys (public and private) for encryption and decryption.

**7.What is a key distribution center (KDC)?**

A KDC is a trusted third party in Kerberos that issues tickets to prove user identities.

**8.Explain the principles of PKI.**

PKI uses digital certificates and a hierarchy of certificate authorities to authenticate identities and manage public keys.

**9.What is the purpose of digital certificates?**

Digital certificates verify the identity of entities and facilitate secure communication over networks.

**10.Describe the process of key management.**

Key management involves generating, distributing, storing, and revoking cryptographic keys to ensure secure communication.

**Unit III: Access Control and Security**

PART-A

**1.What is IP Security (IPsec)?**

IPsec provides protocols to secure IP communications by authenticating and encrypting each IP packet in a communication session.

**2.Describe the Secure Sockets Layer (SSL).**

SSL is a protocol for establishing authenticated and encrypted links between networked computers to ensure data integrity and privacy.

**3.What is network access control?**

Network access control regulates who can access a network and what resources they can use.

**4.Explain the Extensible Authentication Protocol (EAP).**

EAP is an authentication framework used in network access control to provide flexible authentication methods.

**5.What is IEEE 802.1X Port-Based Network Access Control?**

IEEE 802.1X is a standard for securing network access by authenticating devices connected to a LAN or WLAN.

**6.Describe Internet Key Exchange (IKE).**

IKE is a protocol used to establish secure and authenticated communication channels in IPsec.

**7.What is Transport Layer Security (TLS)?**

TLS is a protocol that ensures secure communication over a computer network, succeeding SSL.

**8.Explain HTTPS.**

HTTPS is a secure version of HTTP that uses SSL/TLS to encrypt data exchanged between a web server and a browser.

**9.What is Secure Shell (SSH)?**

SSH is a protocol for secure remote login and other secure network services over an unsecured network.

**10.Describe the role of a firewall.**

Firewalls monitor and control network traffic based on predetermined security rules, acting as a barrier between trusted and untrusted networks.

**Unit IV: Application Layer Security**

PART-A

**1.What is Pretty Good Privacy (PGP)?**

PGP is a data encryption and decryption program that provides cryptographic privacy and authentication for data communication, commonly used for securing emails.

**2.Explain S/MIME.**

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data to secure email communication.

**3.What is DomainKeys Identified Mail (DKIM)?**

DKIM is an email authentication method that allows the receiver to check if the email was sent by an authorized mail server.

**4.Describe mobile device security.**

Mobile device security involves protecting mobile devices from unauthorized access, malware, and data breaches to ensure user privacy and data integrity.

**5.What is wireless network security?**

Wireless network security protects wireless networks from unauthorized access and cyber threats through encryption and authentication methods.

**6.Explain the importance of application layer security.**

Application layer security protects applications from cyber threats by ensuring data integrity, confidentiality, and authentication at the application level.

**7.What is email encryption?**

Email encryption secures the content of email messages by converting them into an unreadable format that only the intended recipient can decrypt.

**8.Describe the role of digital signatures in email security.**

Digital signatures authenticate the sender's identity and ensure the integrity of the email content by providing a cryptographic signature.

**9.What is the significance of wireless network encryption?**

Wireless network encryption prevents unauthorized access to the network by encrypting data transmitted over the wireless connection.

**10.Explain the concept of secure email communication.**

Secure email communication involves encrypting email messages and verifying the sender's identity to protect the content from unauthorized access and tampering.

**Unit V: Security Practices**

PART-A

**1.What are firewalls?**

Firewalls are security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules.

**2.Describe intrusion detection systems (IDS).**

IDS are systems that monitor network traffic for suspicious activity and potential threats, alerting administrators to security incidents.

**3.What is password management?**

Password management involves the processes and tools used to create, store, and manage passwords to ensure strong and secure access credentials.

**4.Explain the characteristics of firewalls.**

Firewalls filter network traffic, enforce security policies, and protect networks from unauthorized access and cyber threats.

**5.What are the different types of firewalls?**

Types of firewalls include packet-filtering firewalls, stateful inspection firewalls, proxy firewalls, and next-generation firewalls (NGFW).

**6.Describe firewall basing.**

Firewall basing involves determining the physical and logical placement of firewalls within a network to maximize security and performance.

**7.What is blockchain technology?**

Blockchain technology is a decentralized digital ledger that records transactions across a network of computers, ensuring transparency, security, and immutability of data.

**8.Explain the concept of cloud security.**

Cloud security involves protecting data, applications, and services hosted in the cloud from cyber threats and ensuring compliance with security standards.

**9.What is IoT security?**

IoT security involves safeguarding Internet of Things (IoT) devices and networks from cyber threats to ensure data privacy and device integrity.

**10.Describe the role of intrusion detection in network security.**

Intrusion detection systems monitor network traffic for suspicious activity and potential threats, alerting administrators to security incidents to prevent breaches.