Cryptography and Network Security

Assignment

-Samarth Goel

23124092

1. What is cryptography, and how does it contribute to network security?

Cryptography is the branch of computer science and mathematics that focuses on securing information and communication using algorithms and keys. It involves techniques such as encryption, decryption, hashing, and digital signatures to protect data from unauthorized access. In a networked environment, data is constantly transmitted over public and potentially insecure channels, making cryptography essential for protecting sensitive information.

Cryptography contributes to network security by ensuring confidentiality, which prevents unauthorized users from reading data. It also ensures integrity, meaning that any unauthorized modification of data during transmission can be detected. Authentication is another important contribution, as cryptographic mechanisms verify the identities of communicating entities. Finally, cryptography provides non-repudiation, ensuring that a sender cannot deny sending a message. Together, these services protect networks against attacks such as eavesdropping, data tampering, impersonation, and replay attacks.

2. How do symmetric-key and asymmetric-key cryptography differ, and where are they used in secure networks?

Symmetric-key cryptography uses a single secret key that is shared between the sender and the receiver. The same key is used for both encryption and decryption, which makes symmetric algorithms very fast and efficient. However, the main drawback of symmetric-key cryptography is the secure distribution and management of the secret key. If the key is intercepted, the security of the entire communication is compromised. Common examples of symmetric-key algorithms include AES and DES. Symmetric encryption is widely used in secure networks for encrypting large volumes of data, such as in VPNs and disk encryption.

Asymmetric-key cryptography, also known as public-key cryptography, uses a pair of mathematically related keys: a public key and a private key. The public key can be freely shared, while the private key is kept secret by the owner. Data encrypted with one key can only be decrypted with the other, which makes asymmetric cryptography suitable for secure key exchange and authentication. Although asymmetric algorithms are slower than symmetric ones, they solve the key distribution problem. Examples include RSA and Elliptic Curve Cryptography (ECC). In secure networks, asymmetric cryptography is mainly used during initial authentication, digital signatures, and secure key exchange mechanisms such as those used in SSL/TLS.

3. What is the role of hash functions and digital signatures in ensuring data integrity and authentication?

Hash functions are cryptographic algorithms that take an input of arbitrary length and produce a fixed-length output known as a hash value or message digest. These functions are designed to be one-way, meaning that it is computationally infeasible to retrieve the original message from the hash. Even a small change in the input data results in a significantly different hash value. Because of these properties, hash functions are widely used to ensure data integrity. If the received hash does not match the recomputed hash, it indicates that the data has been altered during transmission.

Digital signatures combine hash functions with asymmetric cryptography. In a digital signature process, the sender first computes a hash of the message and then encrypts the hash using their private key. The receiver decrypts the signature using the sender's public key and compares the hash with a newly computed hash of the received message. This process ensures authentication of the sender, integrity of the message, and non-repudiation. Digital signatures are extensively used in secure emails, software distribution, online banking, and electronic documents.

4. How does SSL/TLS use cryptographic techniques to secure data transmission over networks?

SSL/TLS is a security protocol designed to provide secure communication between a client and a server over a network. It uses a combination of cryptographic techniques to achieve security goals. During the SSL/TLS handshake phase, asymmetric cryptography is used to authenticate the server and, in some cases, the client. The server presents a digital certificate issued by a trusted Certificate Authority, which allows the client to verify the server's identity.

After authentication, SSL/TLS securely establishes a symmetric session key using public-key cryptography. This session key is then used for encrypting the actual data exchanged between the client and server, as symmetric encryption is much faster and efficient. Additionally, hash functions and message authentication codes are used to ensure data integrity during transmission. By combining these cryptographic techniques, SSL/TLS ensures confidentiality, integrity, and authentication for applications such as HTTPS, online transactions, and secure email services.

5. What is Public Key Infrastructure (PKI), and how does it support secure network authentication and key management?

Public Key Infrastructure (PKI) is a comprehensive framework used to manage public-key encryption and digital certificates in a secure manner. It consists of hardware, software, policies, and procedures that work together to create, distribute, manage, and revoke digital certificates. A central component of PKI is the Certificate Authority (CA), which is responsible for issuing digital certificates that bind a public key to an entity's identity.

PKI supports secure network authentication by enabling users, devices, and servers to verify each other's identities using digital certificates. It also facilitates secure key management by ensuring that public keys are distributed safely and private keys remain confidential. Certificate revocation mechanisms, such as Certificate Revocation Lists (CRLs), help maintain trust by invalidating compromised or expired certificates. PKI is widely used in SSL/TLS, secure email systems, virtual private networks, and enterprise security solutions to establish trust in large-scale networks.