Security In Distributed Systems

1. Write the steps of the RSA Algorithm. Illustrate with an example given P=3 & Q=11.

2. Analyze the following uses of Cryptography with suitable scenarios:
a) Secrecy and Integrity b) Authentication

Secrecy and Integrity

- Cryptography is used to maintain the secrecy and integrity of information whenever it is exposed to potential attacks.
- It maintains the secrecy of the encrypted message as long as the decryption key is not compromised.
- It also maintains the integrity of the encrypted information, provided that some redundant information such as a checksum is included and checked.

Scenario:

Secret communication with a shared secret key:
Alice wishes to send some information secretly to Bob. Alice and Bob share a secret key KAB.

- Alice uses KAB and an agreed encryption function E(KAB, M) to encrypt and send any number of messages {Mi}KAB to Bob.
- Bob decrypts the encrypted messages using the corresponding decryption function D(KAB, M).

Authentication

- Cryptography is used in support of mechanisms for authenticating communication between pairs of principals.

- **Key** is known only to two parties.

Scenario:

Bob has a public/private key pair <KBpub, KBpriv>

- Alice obtains a certificate that was signed by a trusted authority stating Bob's public key Kbpub.
- Alice creates a new shared key KAB, encrypts it using Kbpub using a public-key algorithm, and sends the result to Bob.
- Bob uses the corresponding private key KBpriv to decrypt it.

3. Discuss asymmetric (public/private key pair-based) cryptography technique and how it can be used in supporting security in distributed systems.

When a public/private key pair is used, one-way functions are exploited in another way. The feasibility of a public-key scheme was proposed as a cryptographic method that eliminates the need for trust between communicating parties. The basis for all public-key schemes is the existence of a trap-door function. A trap-door function is a one-way function with a secret exit- it is easy to compute in one direction but infeasible to compute its reverse unless the secret is known.

The pair of keys needed for asymmetric algorithms are derived from a common root. The derivation of the pair of keys from the root is a one-way function. In the case of the RSA algorithm, the large numbers are multiplied together, this computation takes only a few seconds, even for very large primes used. The resulting product, N, is computationally infeasible to derive the original multiplicands.

One of the pair of keys is used for encryption. For RSA the encryption procedure obscures the plaintext by treating each block as a binary number and raising it to the power of key, modulo N. The resulting number is the corresponding ciphertext block. The size of N and at least one of the pair of keys is much larger than the safe key size for symmetric keys to ensure that N is not factorizable. For this reason, the potential attacks on RSA are small, its resistance to attacks depends on the infeasibility of factorizing N.

4. What is a distributed denial-of-service attack and how does it work?

Distributed denial-of-service attacks target websites and online services. The aim is to overwhelm them with more traffic than the server or network can accommodate. The goal is to render the website or service inoperable. Flooding a channel or other resource with messages in order to deny access to others.

Botnets

- The primary way a DDoS is accomplished is through a network of remotely controlled, hacked computers or bots. These are often referred to as “zombie computers.”
- They form what is known as a “botnet” or network of bots. These are used to flood targeted websites, servers, and networks with more data than they can accommodate.
- The botnets may send more connection requests than a server can handle or send overwhelming amounts of data that exceed the bandwidth capabilities of the targeted victim.
- Botnets can range from thousands to millions of computers controlled by cybercriminals. Cybercriminals use botnets for a variety of purposes, including sending spam and forms of malware such as ransomware.

5. What is the goal of security? List the three broad classes of security threats?

Classes of Threats

- **Leakage:** Refers to the acquisition of information by unauthorized recipients.
- **Tampering:** Refers to the unauthorized alteration of information.
- **Vandalism:** Refers to interference with the proper operation of a system without gain to the perpetrator.

6. What is cryptography? What is the use of it?

Cryptography

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Uses

- Secrecy and Integrity
- Authentication

💡 Same as Answer 2

7. Write a note on digital signature.

- Cryptography is used to implement a mechanism known as a digital signature.
- This is similar to the conventional signature, verifying to a third party that a message or a document is an unaltered copy of one produced by the signer.
- This can be achieved by encrypting the message called a digest – using a key that is known only to the signer.
- A digest is a fixed-length value computed by applying a secure digest function.
- The resulting encrypted digest acts as a signature that accompanies the message.
- The originator generates a signature with their private key, and the signature can be decrypted by any recipient using the corresponding public key.