Homework-2

R11836401-Sasi Kumar Ede

# Ans)

The advantages and disadvantages of public-key cryptography include:

**Advantages:**

* + - Public-key cryptography, which does not require a shared secret key, makes key management simpler and more secure. The public key can be shared without restriction, whereas the private key can be kept a secret.
    - Improved Security Public-key cryptography is more secure than symmetric-key cryptography because it uses two keys and is therefore more challenging to crack. The private key is necessary to decode the message, therefore even if the public key is stolen, it cannot be used to do so.
    - Digital signatures give users a way to verify the authenticity and integrity of a message, and public-key cryptography makes them possible. Digital signatures are crucial for secure online authentication and transactions.

**Disadvantages:**

* Managing the distribution of public keys can be difficult in large organizations or on an international scale. Public keys must be verified for authenticity because a lost or fake public key could endanger the security of the system**.**
* It is possible that encryption and decryption will take longer with public-key cryptography because it is computationally more challenging than symmetric-key cryptography.
* **Key Length:** For public-key cryptography to be secure, longer keys are needed, which might result in larger messages and slower processing.

# Ans)

The attributes of Public-key encryptions are:

* + - **Security:** Public-key encryption is more secure than symmetric-key encryption because it prevents an attacker from using the public key to decode a message without the private key, even if they have it.
    - **Asymmetric:** Asymmetric means that the public key and the private key in public-key encryption are different but mathematically connected.
    - **Encryption and decryption:** A public key is used for encryption, and a private key is used for decryption, in public-key encryption. This allows for the encryption and decryption of communications.
    - **Key Management:** Public-key encryption eliminates the need for a shared secret key, making it easier to distribute and keep keys securely.
    - **Authentication:** By using public-key encryption for authentication, network and system access can be made secure.
    - **Non-repudiation:** Public-key encryption makes it hard for a sender to undo their actions once a communication has been encrypted and delivered using their private key.
    - Digital signatures can be created using public-key encryption and used to verify the authenticity and integrity of messages.

# Ans)

Public key encryption is a type of cryptography that encrypts and decrypts messages using a public key and a private key. The following are the general steps for public key encryption:

* + - **Key Generation:** Public key encryption begins with the production of a key pair that consists of a public key and a private key. Only the owner can decrypt messages that have been encrypted with the private key, which is kept secret. Anyone who wishes to send the key pair's owner an encrypted message can do so by using the public key.
    - **Encryption:** The recipient's public key must be acquired by the sender and used to encrypt a message using public key encryption. Plaintext is changed into ciphertext using the recipient's public key, which can only be decoded with the recipient's private key.
    - **Transmission:** The encrypted communication will subsequently be delivered to the recipient, either directly or through a network. As it is encrypted, anyone who intercepts the transmission won't be able to read it or change it.
    - **Decryption:** After receiving an encrypted communication, the recipient decrypts it using their private key. With the help of the recipient's private key, the ciphertext is decrypted and transformed back into the original plaintext message.

Ex:

This is an example of how public key encryption may be used:

A must reveal a secret to B. B has made the public key of a key pair—which consists of a private and a public key—available on a public key server. A receives B's public key and encrypts her conversation with it. By applying the encryption technique, A's plaintext message is transformed into ciphertext using B's public key, which can then only be decrypted using B's private key. A sends B an encrypted message, which B uses his private key to decrypt so he can view what is inside. In this situation, public key encryption provides a secure method for A and B to communicate secretly without fearing that someone else might eavesdrop or read it.

# Ans)

There are various types of public key cryptography algorithms. These five categories are frequently used:

* + - **Mathematical approach:** The mathematical techniques used by public key cryptography algorithms, such as lattice-based encryption, elliptic curve cryptography, or modular arithmetic, can be used to classify them.
    - **Key size:** The classification of these techniques may also be based on the size of the keys used by public key cryptography algorithms, which are often measured in bits. With keys of 2048 bits or more, RSA and DSA, for example, are often used.
    - The security level of public key cryptography techniques can be used to group them according to how difficult it is to decrypt data. The mathematical approach utilized, and the size of the key are usually used to determine the security level.
    - **Algorithm type:** RSA and ElGamal are examples of encryption algorithms. Other examples of public key cryptography techniques include signature algorithms (such as DSA and ECDSA).
    - **Application:** Public key cryptography techniques can also be divided into groups based on the sort of secure communication they are used for, such as digital signatures and SSL/TLS for secure communications and S/MIME and PGP for secure communications, respectively.

# Ans)

# Algorithms for RSA encryption and decoding

# Use the RSA encryption algorithm to convert the plaintext message M into an integer m, making ensuring that 0<=m<n.

# The ciphertext C should equal me mod n.

# Deliver the ciphertext C to the receiver.

# Decryption algorithm for RSA:

# Get the ciphertext C.

# Use the following formula to determine the plaintext message m = C^d mod n.

# Put the value m back into message M's plaintext format.

You should be aware that the RSA method uses a private key of the form d, n, where d is the decryption exponent, and a public key of the type e, n, where e is the encryption exponent and n is the modulus. While the modulus n and exponent e of encryption are made public, the decryption exponent d is maintained a secret.

The following procedures are normally used to produce the RSA key pair:

* + - Choose two very big prime numbers p and q.
    - Calculate by using n = p\*q.
    - phi(n) = (p-1)\*(q-1)., calculate the totient of n.
    - Choose an encryption exponent such that gcd(e, phi(n)) = 1 and 1 <e< phi(n).
    - Calculate the decryption exponent d such that it is the modular inverse of the value of e modulo phi (n).
    - The private key is {d, n}, while the public key is {e,n}.

After the key pair has been created, the techniques for encryption and decryption can be utilized to reliably encode and decode communications.

# Ans)

* + - **Attack through brute force:** Each conceivable private key can be tried by an attacker until they find the proper one. This attack can be stopped by using key sizes that are suitably large.
    - **Factorization attack:** An attacker could try factoring the modulus n to obtain the private key d. The attack is stopped by creating the modulus using large prime numbers.
    - **Attack based on timing:** The execution of RSA encryption or decryption can be timed by an attacker to get information about the private key. Constant-time algorithms can fend off this assault since they always finish a task in the same amount of time.
    - **Side-channel attack:** An attacker can measure the power consumption, electromagnetic emissions, or other side channels to find out more information about the private key. This attack can be stopped by using secure hardware or software solutions that prevent side-channel leakage.
    - **Attack using chosen ciphertexts:** An attacker can choose ciphertexts that must be decoded by the recipient to discover the private key. This attack can be stopped using message authentication codes and secure padding techniques.

To prevent these attacks and maintain system security, careful RSA encryption implementation is necessary. RSA should be used in conjunction with other encryption methods to increase system security even more.

# Ans)

Message authentication ensures that the intended recipient and not a forger delivered the message.

* The service used to provide message authentication is called a Message Authentication Code (MAC).
* Using a keyed hash function that includes the symmetric key shared by the sender and recipient, a MAC generates the digest.
  + - It demonstrates how a sender A authenticates a message using a keyed hash function and how a receiver B may check the message's validity.
    - This approach employs a symmetric key that both A and B share.
    - A creates a MAC using this symmetric key and a keyed hash function.
    - A then delivers the original message with this MAC to B.
    - The message and MAC are received by B, who isolates the message from the MAC.
    - B then generates a new MAC by using the same symmetric key and the same keyed hash function on the message.
    - B then contrasts the previously created MAC with the one sent by A.
    - If the two MACs match, A is the message's sender and that the message hasn't been altered.

# Ans)

**Digital Signatures:** The sender's identity and the veracity of a communication can be verified using a digital signature, a cryptographic technique. It entails employing a private key to encrypt the message's hash, which is delivered along with the message. The recipient can then use the corresponding public key to decrypt the hash and verify the message's authenticity.

**Message Authentication Codes (MACs):** The validity and integrity of a message can be verified using a MAC, a cryptographic technique. Using a secret key, it requires developing a unique code or tag for a communication that is sent along with the message. When comparing the code and the message to establish whether the message is authentic, the receiver might use the same key and algorithm.

**Public Key Infrastructure (PKI):** Public key encryption and digital certificates are managed by PKI, a group of technologies, protocols, and rules. It requires the use of a Certificate Authority (CA), a reliable third party, to issue digital certificates that confirm the sender's identity and ensure the message's legitimacy. After that, the recipient can verify the message's authenticity using the public key of the digital certificate.

**Hash Functions:** A message's unique, fixed-size representation is produced by a mathematical operation called a hash function. The message is input into the hash function, which generates a message digest or hash of a specified size. After that, the recipient can verify the integrity of the message by creating a hash of the received message using the same hash method and comparing it to the original hash.

# 2 Q.2. Short answer Questions

1. Asymmetric
2. two keys and an encryption algorithm
3. private key cryptography
4. Symmetric
5. integrity