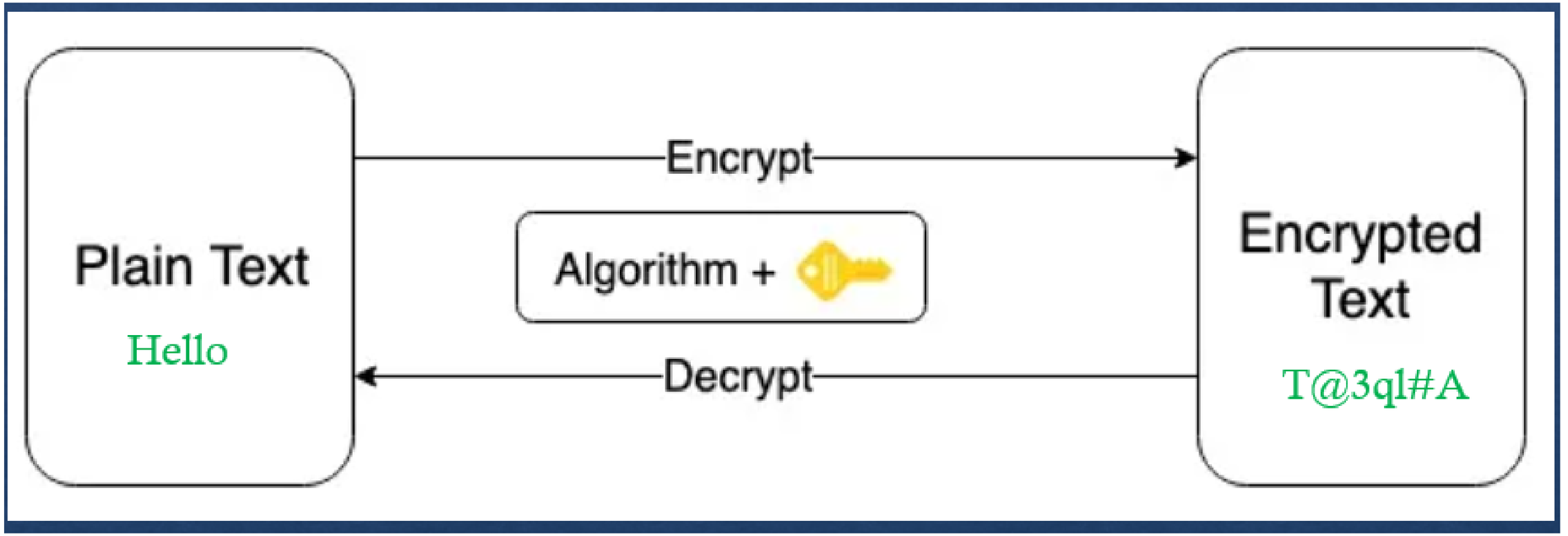
ENCRYPTION, HASHING AND DIGITAL SIGNATURE

Hiral Patel
@gisacouncil

Encryption

Encryption is the process of converting plaintext or data into a ciphertext using an algorithm and a key. This process makes the original data unreadable to anyone who doesn’t have the corresponding decryption key.

Data can be encrypted "at rest," when it is stored, or "in transit," while it is being transmitted somewhere else



Decryption

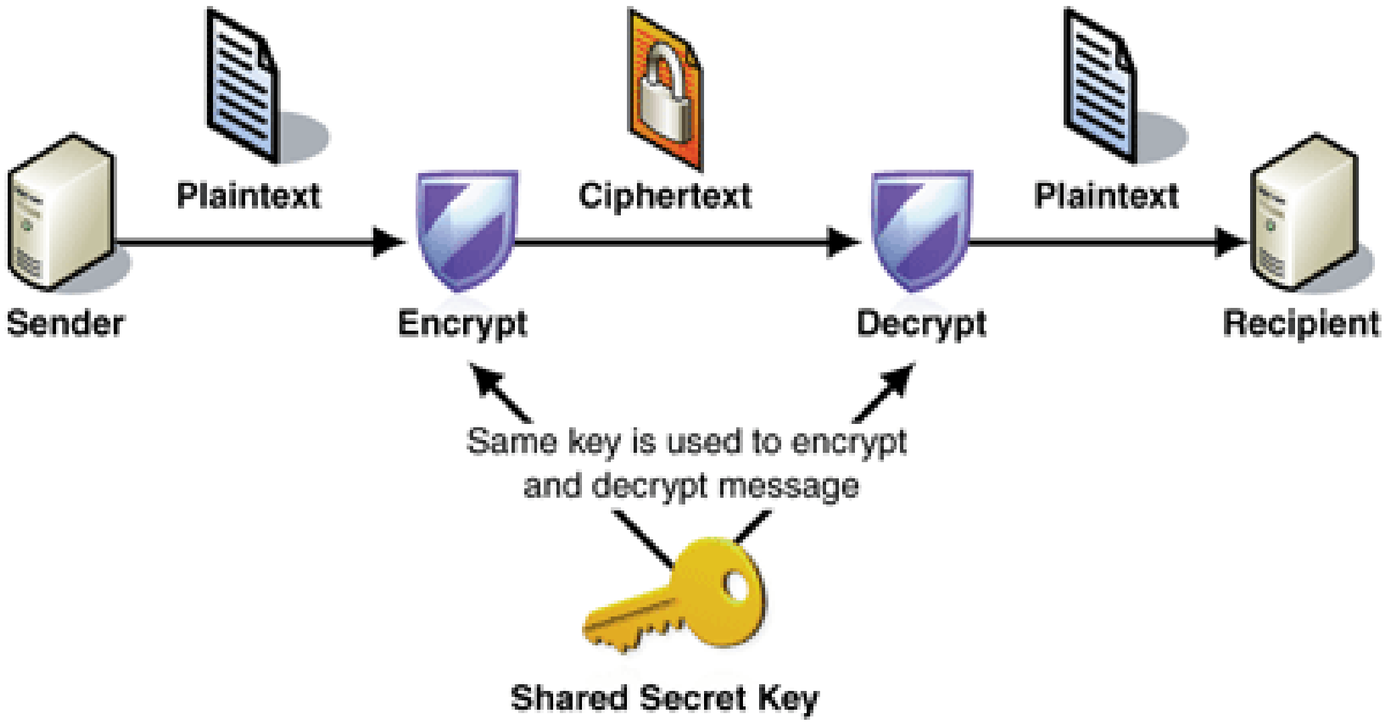
Decryption, on the other hand, is the process of converting the ciphertext back into its original plaintext form using the appropriate decryption key. Decryption reverses the encryption process, allowing authorized parties to access and read the original data.

Types of Encryptions

Mainly 2 types of Encryptions

1. Private or secret key encryption also called Symmetric key encryption
2. Public key encryption also called Asymmetric key encryption

Private key/Symmetric key Encryption

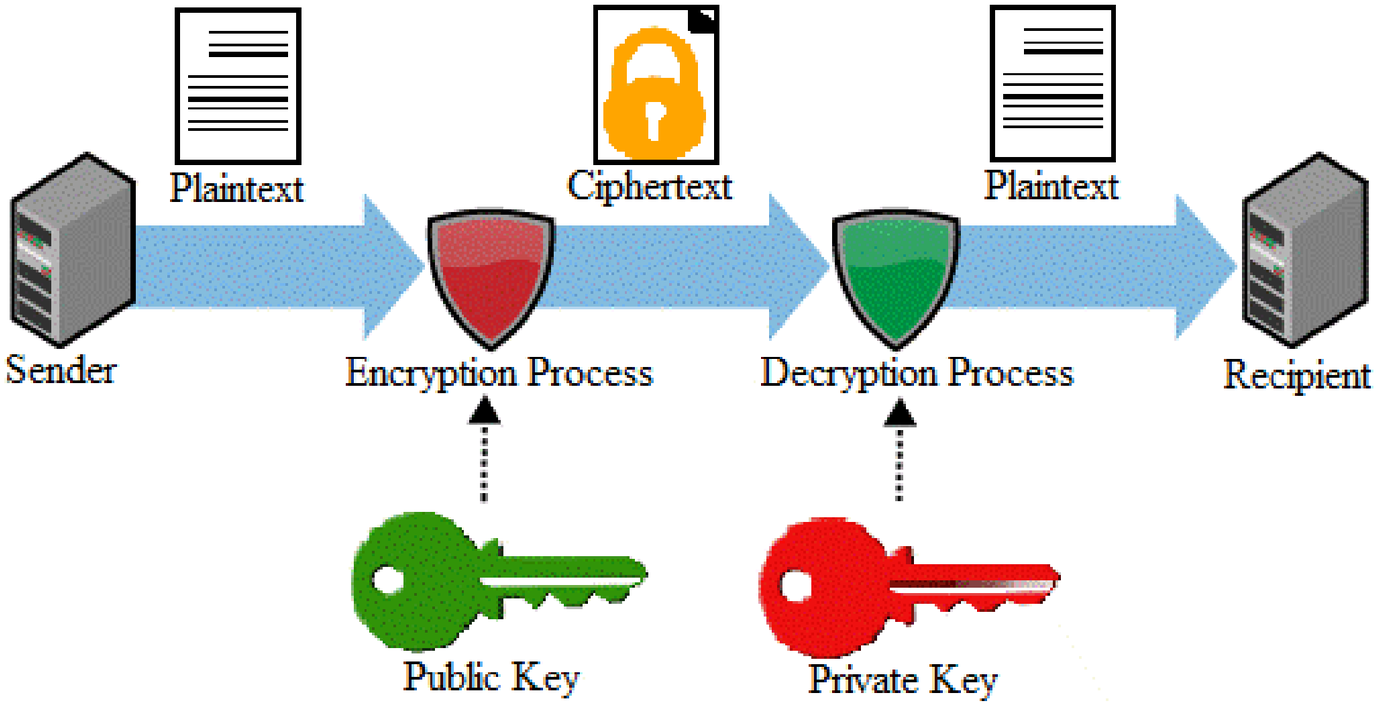


In Symmetric key encryption, the same key is used for both encryption and decryption. So it is faster and less expensive but the challenge is to share the same key securely between two parties. AES, DES, 3DES, Blowfish are some of the example of symmetric key encryption

Public key encryption/Asymmetric key encryption

In this type of Encryption, two different types of keys are used, one is public key and second is private key. Public key is available in public domain to everyone and private key is private to specific person. Message encrypted by private key can be decrypted by corresponding public key. It is slower and more expensive algorithm then symmetric key algorithm. But there is no challenge of sharing the key between two parties. RSA, Diffie-Hellman key exchange, Elliptic curve cryptography are the example of Asymmetric encryption.

Public key encryption/Asymmetric key encryption



In this mechanism 4 keys can take part in whole process.

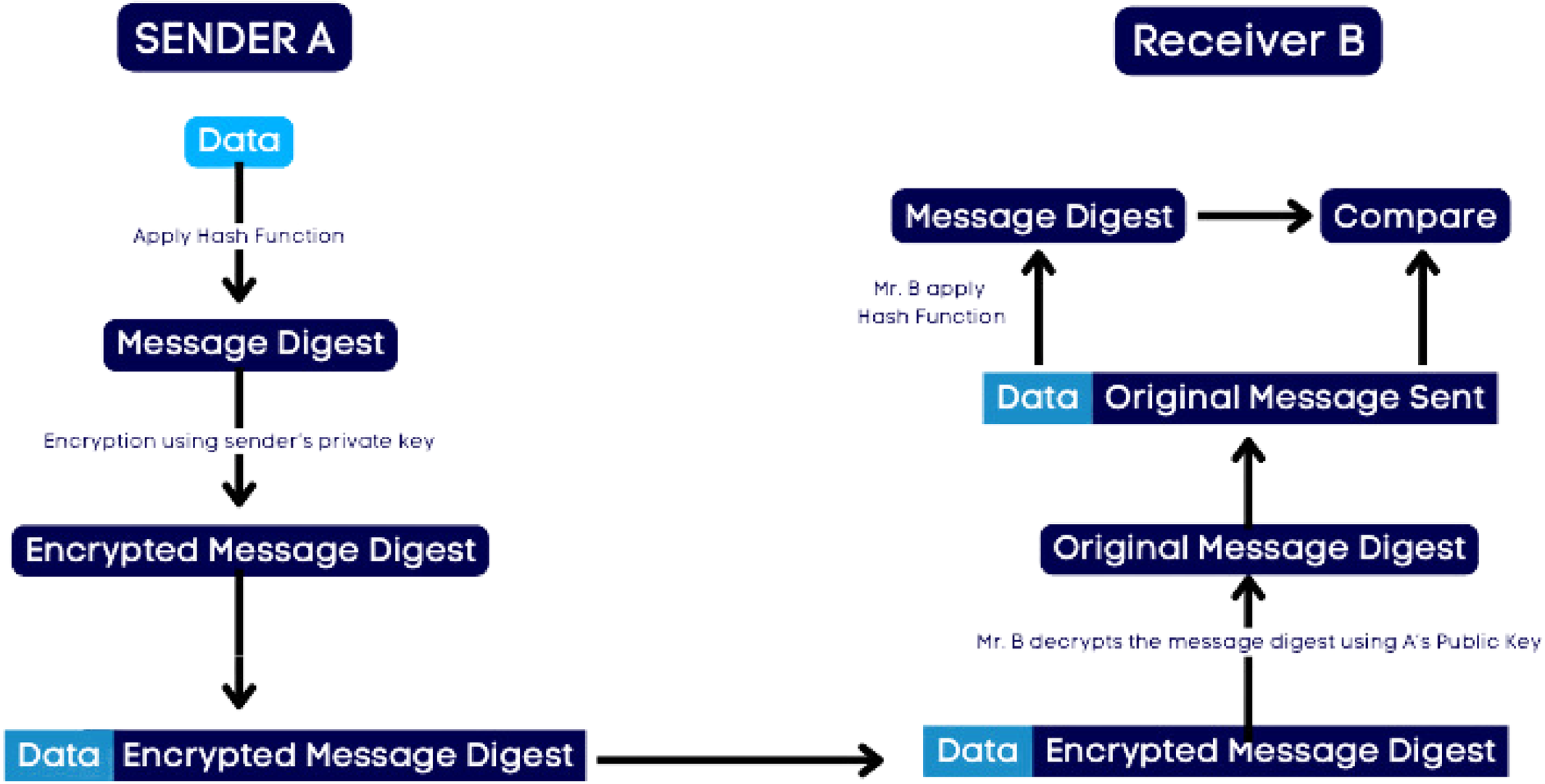
- **Sender's public key**
- **Sender's Private key**
- **Receiver's Public key**
- **Receiver's Private key**

Hashing

Hashing is a cryptographic technique used to transform input data of any size into a fixed-size string of characters, known as a hash value or hash code. The process of hashing involves applying a hash function to the input data, which produces a unique representation of that data. Hashing is irreversible encryption.

If Mr. A wants to confirm the integrity of the message not confidentiality then Mr. A will use hash function upon data and create a message digest. Then that message digest will be encrypted by using Mr. A’s private key. Mr. A will share that Data + encrypted Message digest with Mr. B. Now Mr. B will first decrypt the encrypted message digest with Mr. A’s public key and will get the original message digest. Mr. B then will apply the hash function on data and will create a message digest on his/her end and then will compare both message digests created by at B’s end and supplied by Mr. A. If both are matching then Mr. B can confirm that the message is not being altered by anyone and can confirm the integrity of the message.

Hashing


SENDER A
Data
Apply Hash Function
Message Digest
Encryption using sender's private key
Encrypted Message Digest
Data
Encrypted Message Digest
Receiver B
Message Digest
Compare
Mr. B apply
Hash Function
Data
Original Message Sent
Original Message Digest
Mr. B decrypts the message digest using A's Public Key
Data
Encrypted Message Digest

Digital Signature

Digital signature is the process to attach a digital code to the document to verify its content and sender’s identity. As an paper document, we take the signature of a person to verify that the document is shared by that person and validate the message from him. Same way, this can also be verified for electronic document using digital signature. Hashing technique is used to create a digital code.

How to achieve Confidentiality, Integrity, Authentication and Non-Repudiation Using these techniques

Confidentiality

Encrypt the message using receiver's public key and decrypt by using receiver's private key

Authentication, Integrity, Non-Repudiation

Create the Message digest/ Hash of the message
Encrypt the hash/message digest using sender's private key

Confidentiality, Authentication, Integrity, Non-Repudiation

For Confidentiality: message to be encrypted using receiver's public key
For Authentication/Non-Repudiation, Integrity:

1. Create the hash/message digest of the message
2. Encrypt the hash/message digest using sender's private key

Food for thought

Q-1 In Public key Encryption, the sender of the message is authenticated by:

A.Using the Receiver’s private key to encrypt the hash of the message and using the receiver’s public key to decrypt it

B.Using the sender’s public key to encrypt the hash of the message and using the sender’s private key to decrypt it

C.Using the sender’s private key to encrypt the hash of message and using the sender’s public key to decrypt it

D.Using the receiver’ public key to encrypt the hash message and using the receiver’s private key to decrypt it

Food for thought

Q-2 In Public key Encryption, How message confidentiality can be achieved?

A.Encryption is done by private key and decryption is done by public key

B.Encryption is done by public key and decryption is done by private key

C.Public keys are used to encrypt and decrypt the data

D.Private keys are used to encrypt and decrypt the data

Food for thought

Q-3 In Public key Encryption, How message Integrity can be achieved?

A.Hash of the message to be encrypted by sender’s private key and decryption is done by sender’s public key

B.Hash of the message to be encrypted by sender’s public key and decryption is done by sender’s private key

C.Hash of the message to be encrypted by receiver’s private key and decryption is done by receiver’s public key

D.Hash of the message to be encrypted by receiver’s public key and decryption is done by receiver’s private key

Food for thought

Q-4 Which one of the following cryptographic algorithms supports the goal of Non-repudiation?

A. Blowfish

B. DES

C. AES

D. RSA

Food for thought

Q-5 The basic difference between hashing and encryption is that hashing

A. Can not be reversed

B. Can be reversed

C. Concerned with security

D. Concerned with confidentiality

Food for thought

Q-6 Hiral has sent a message to krishna along with encrypted hash created using hiral's private key. This will ensure

A. Authenticity and Integrity

B. Authenticity and Confidentiality

C. Integrity and Privacy

D. Privacy and Non-Repudiation

COMMENT YOUR ANSWERS

FOLLOW MY LINKEDIN FOR MORE CONTENT