Basic Cryptography

- *Cryptography* — the science of secret writing.
- The prefix "crypt" means "hidden" and suffix graph means "writing".
- Cryptography basically means keeping information in secret or hidden.
- Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.
- Thus preventing unauthorized access to information.

Key: Replace every letter with 3rd successive letter

Cipher K NQYG CRRNGU

Benefits of Cryptography

1. **Privacy/confidentiality**: Ensuring that no one can read the message except the intended receiver.

2. **Authentication**: The process of proving one's identity.

3. **Integrity**: Assuring the receiver that the received message has not been altered in any way from the original.

4. **Non-repudiation**: A mechanism to prove that the sender really sent this message.

5. **Key exchange:** The method by which crypto keys are shared between sender and receiver.

Basic Terminology of Cryptography

1. **Plaintext:** This is the readable message or data that is fed into the algorithm as input.

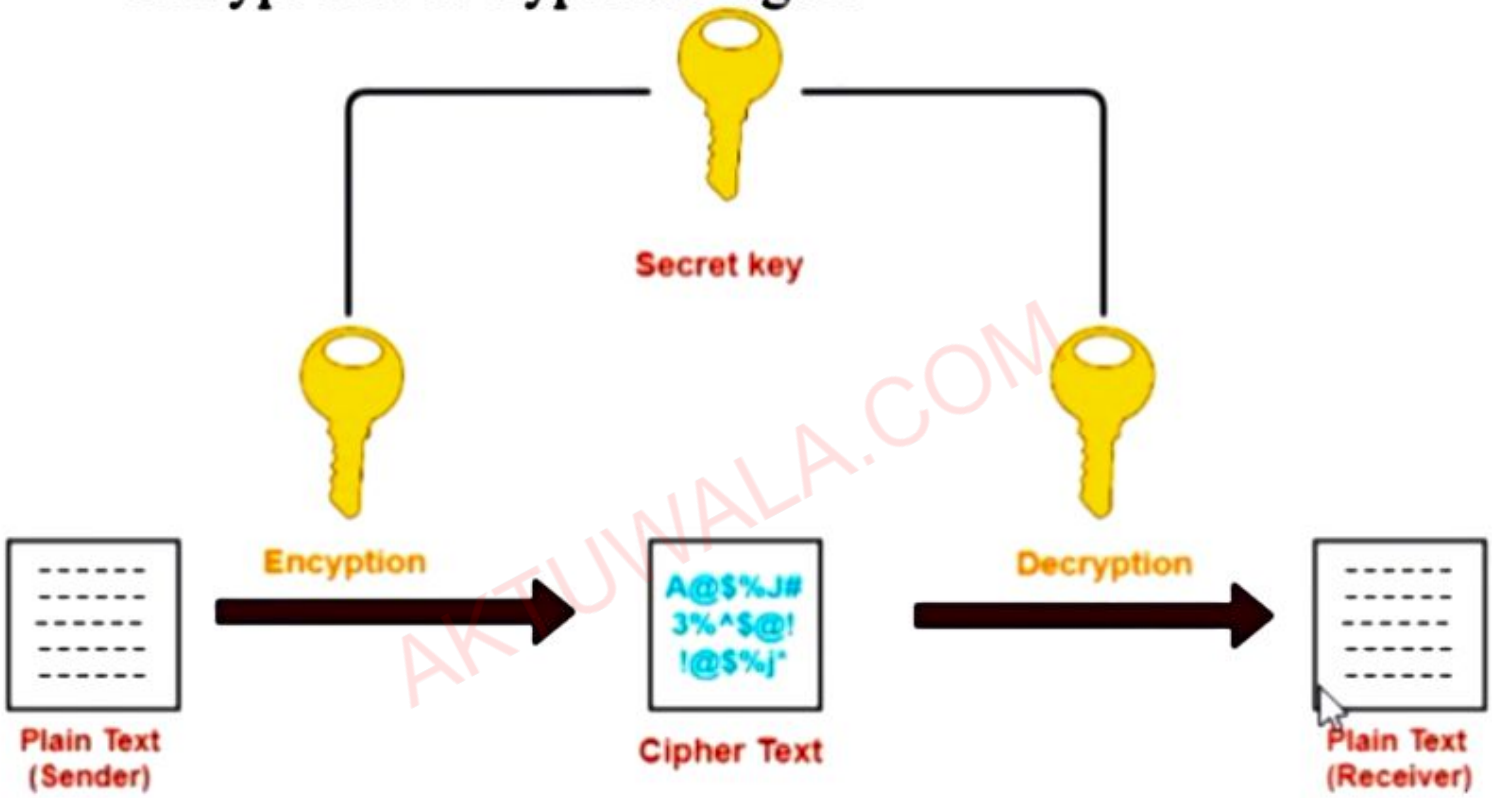
2. **Encryption algorithm:** The encryption algorithm performs various transformations on the plaintext.

3. **Public and private keys:** This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.

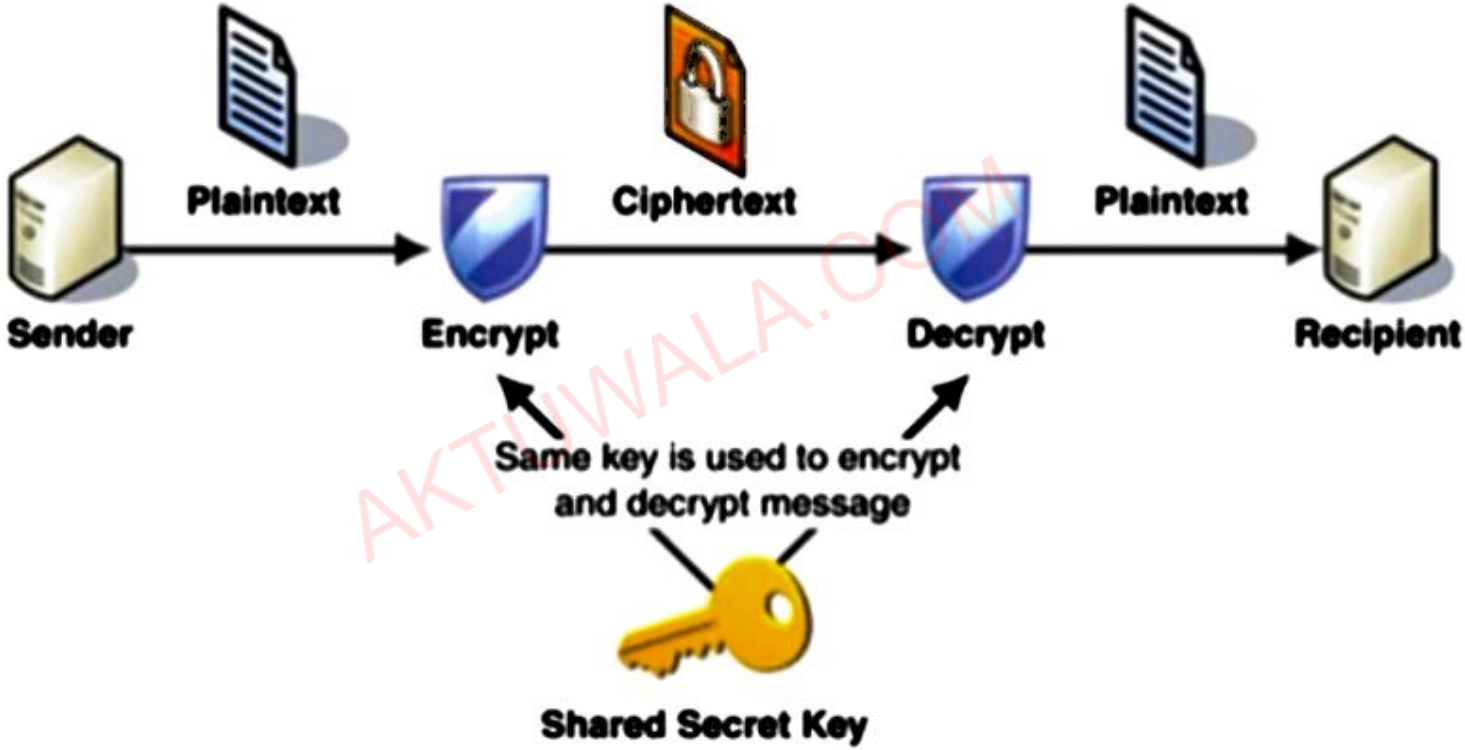
4. **Cipher text:** This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different cipher texts.

5. **Decryption algorithm:** This algorithm accepts the cipher text and the matching key and produces the original plaintext.

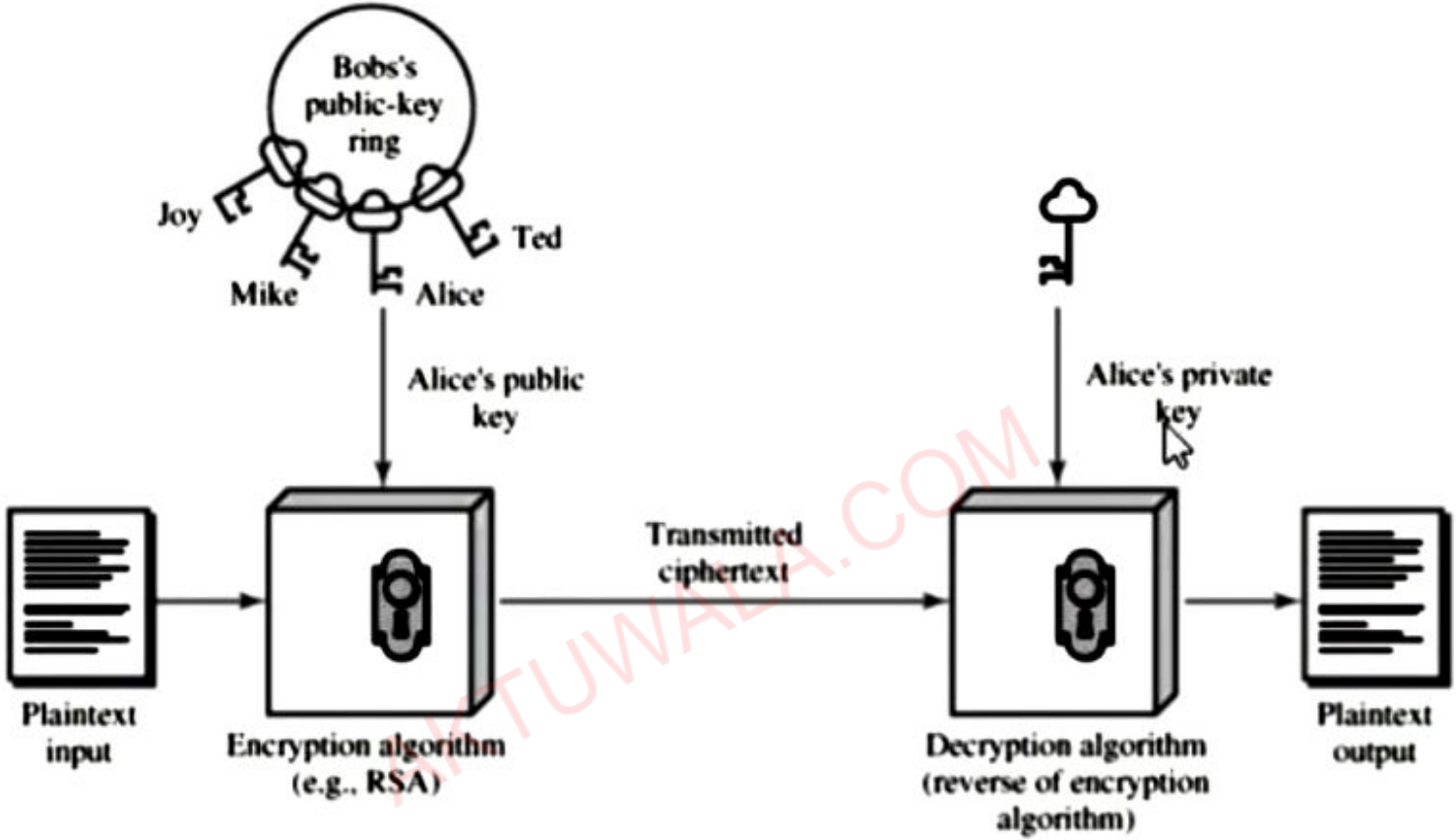
1. **Symmetric or Private Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages.



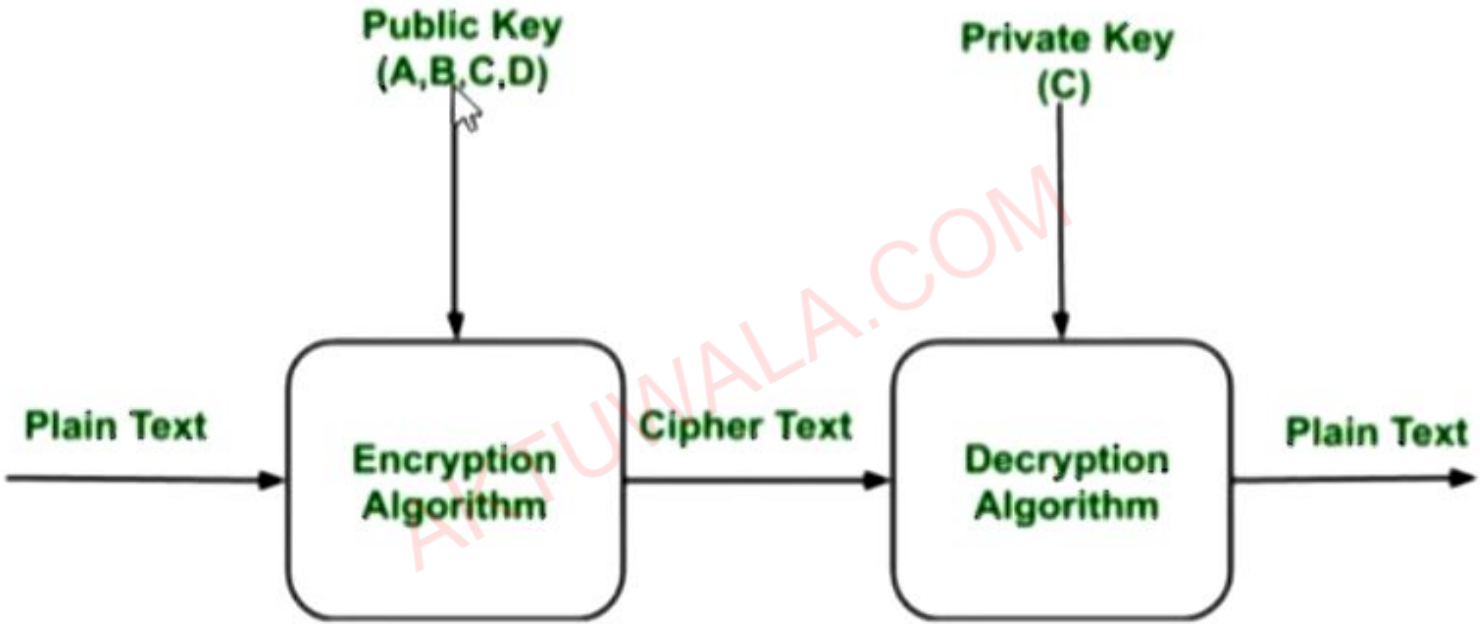
Symmetric Key Cryptography



2. **Asymmetric or Public Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.



(a) Encryption

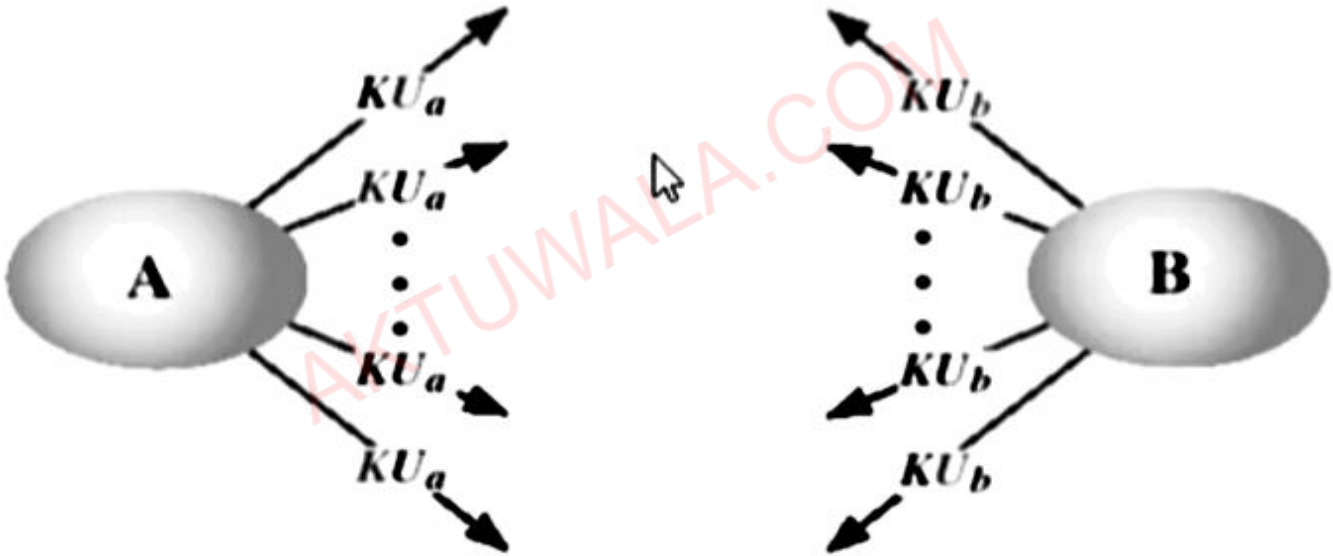


Public key distribution

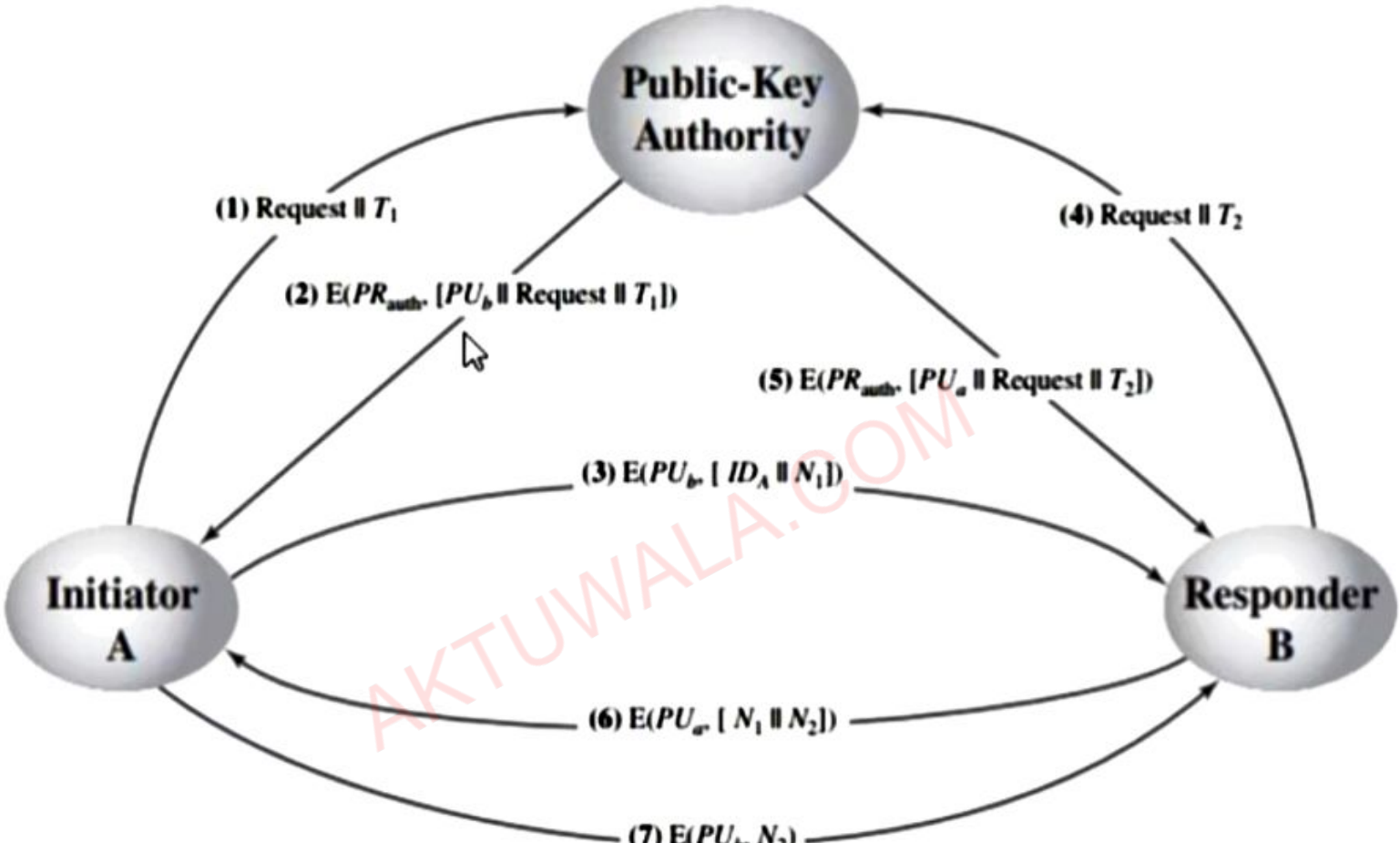
In public key cryptography, everyone has access to everyone's public key, public keys are available to the public.:

- Public announcement
- Publicly available directory (trusted center)
- Public-key authority (controlled trusted center)
- Public-key certificates

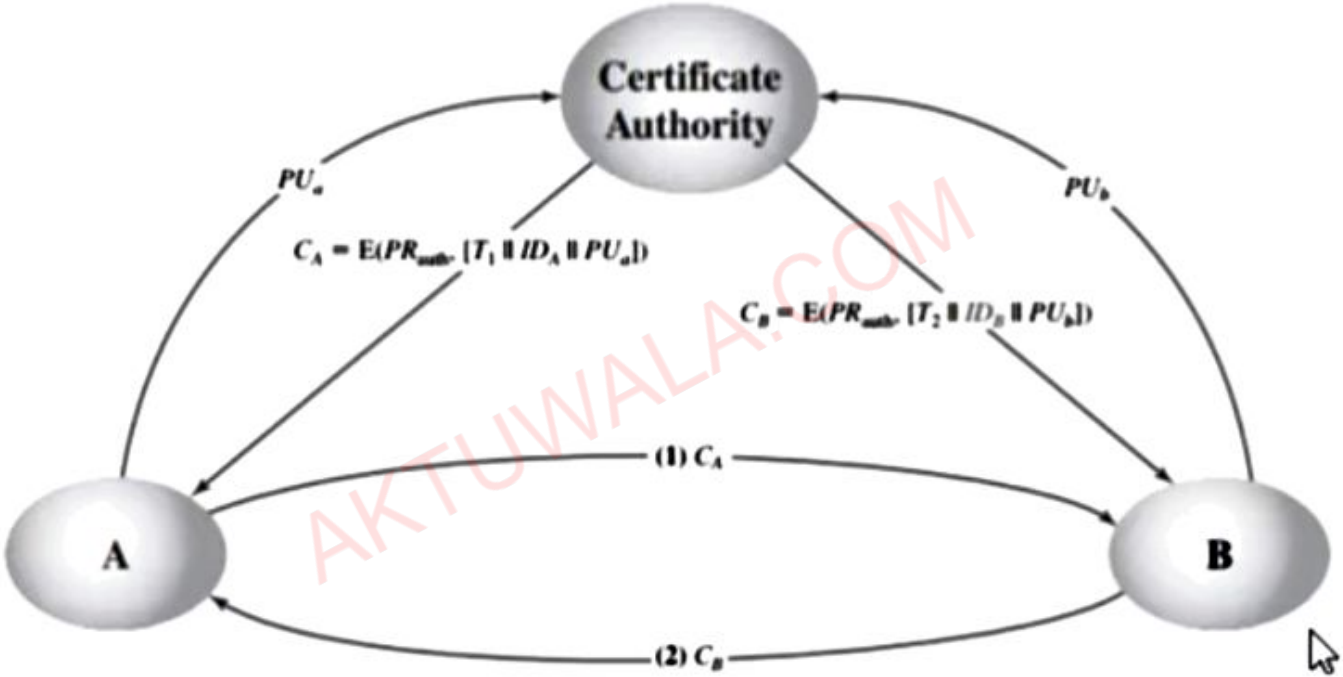
1. Public Announcement -



2. Publicly available directory (trusted center) -

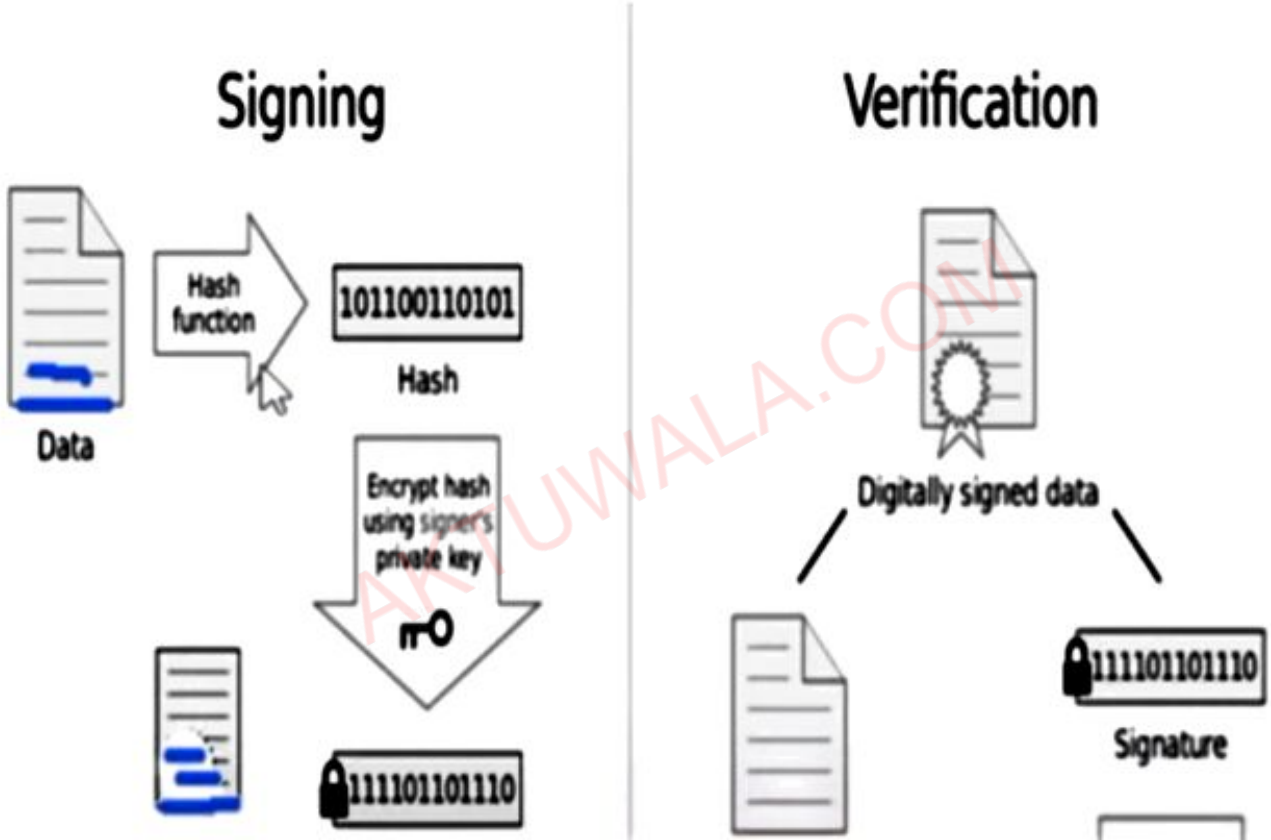


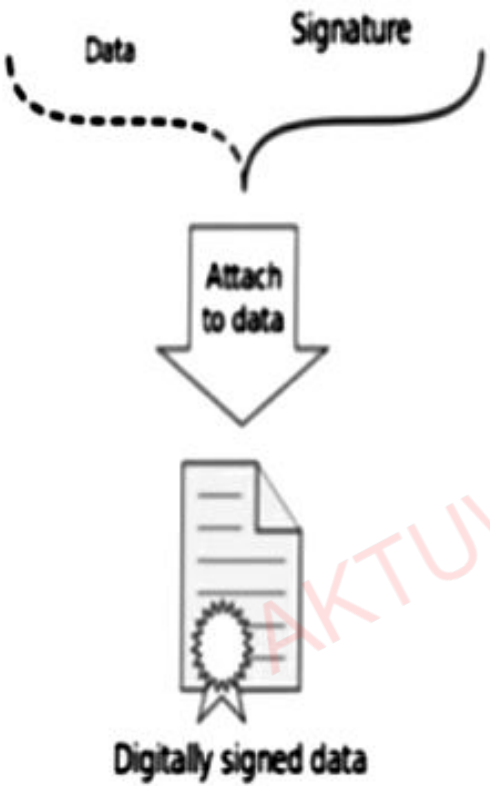
4. Public Key Certificates -

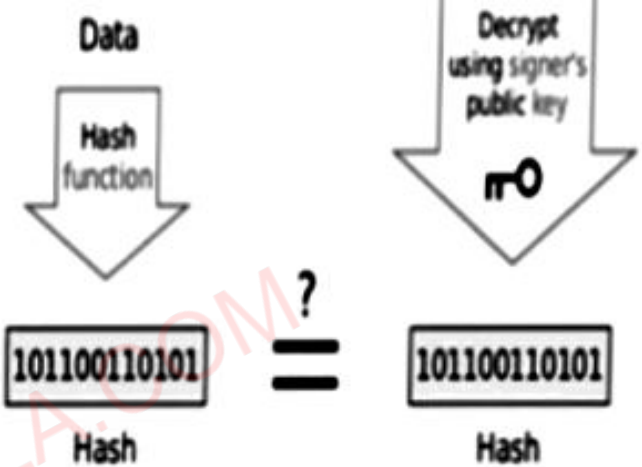


Digital Signature

1) As similar to handwritten signature or stamped seal
2) Mathematical technique
3) Used for authenticity and integrity of a message
4) Provide security to digital document.
5) Solve the problem of tampering


Signing
Hash function
101100110101
Hash
Data
Encrypt hash using signer's private key
1111011101110
Verification
Digitally signed data
1111011101110
Signature





If the hashes are equal, the signature is valid.

Real World Protocols

Following are the Real world protocols:

1. SSL Architecture
2. S/MIME OR Email security certificates - Secure/ Multipurpose Internet Mail Extensions
3. PGP-Pretty Good Privacy
4. SET-Secure Electronic Transaction
5. IP security (IPSec)

1. **SSL Architecture** - Secure Socket Layer (SSL) provide security to the data that is transferred between web browser and server.

Secure Socket Layer Protocols:

- **SSL record protocol** - SSL Record provide two services to SSL connection

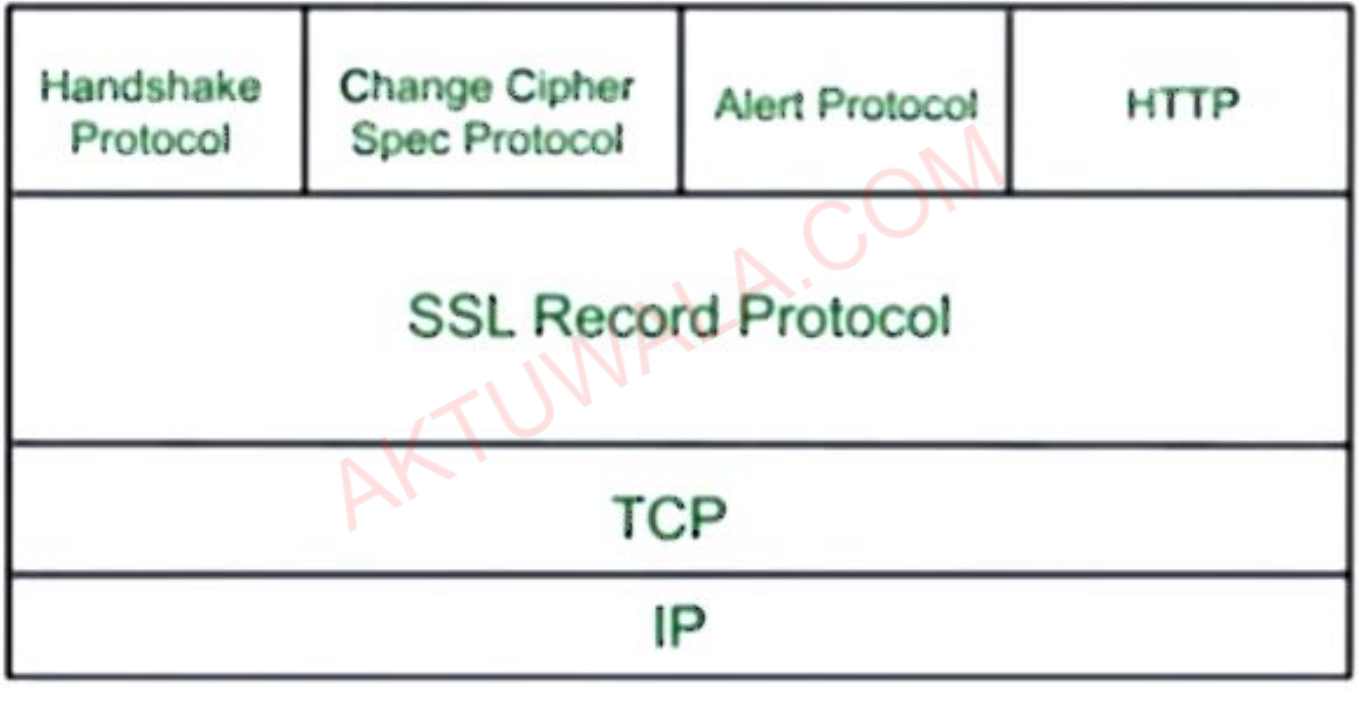
a) Confidentiality

b) Message Integrity

- **Handshake protocol** - Handshake Protocol is used to establish sessions. This protocol allow

client and server to authenticate each other by sending a series of messages to each other

- **Change-cipher protocol** - This protocol uses SSL record protocol. Change-cipher protocol consists of single message which is 1 byte in length and can have only one value. This protocol purpose is to cause the pending state to be copied into current state.
- **Alert protocol**- This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contain 2 bytes.



S/MIME OR Email security certificates –

(Secure/ Multipurpose Internet Mail Extensions)

S/MIME keeps your emails protected during transition. S/MIME uses cryptography to digitally sign and encrypt your email to prevent interception from any unauthorized person.

Email certificates, also known as SMIME certificates, are digital certificates that can be used to sign and encrypt email messages. When you encrypt an email using an email certificate, only the person that you sent it to can decrypt and read the email.

The recipient can also be sure that the email hasn't been changed in any way.

S/MIME includes two security features:

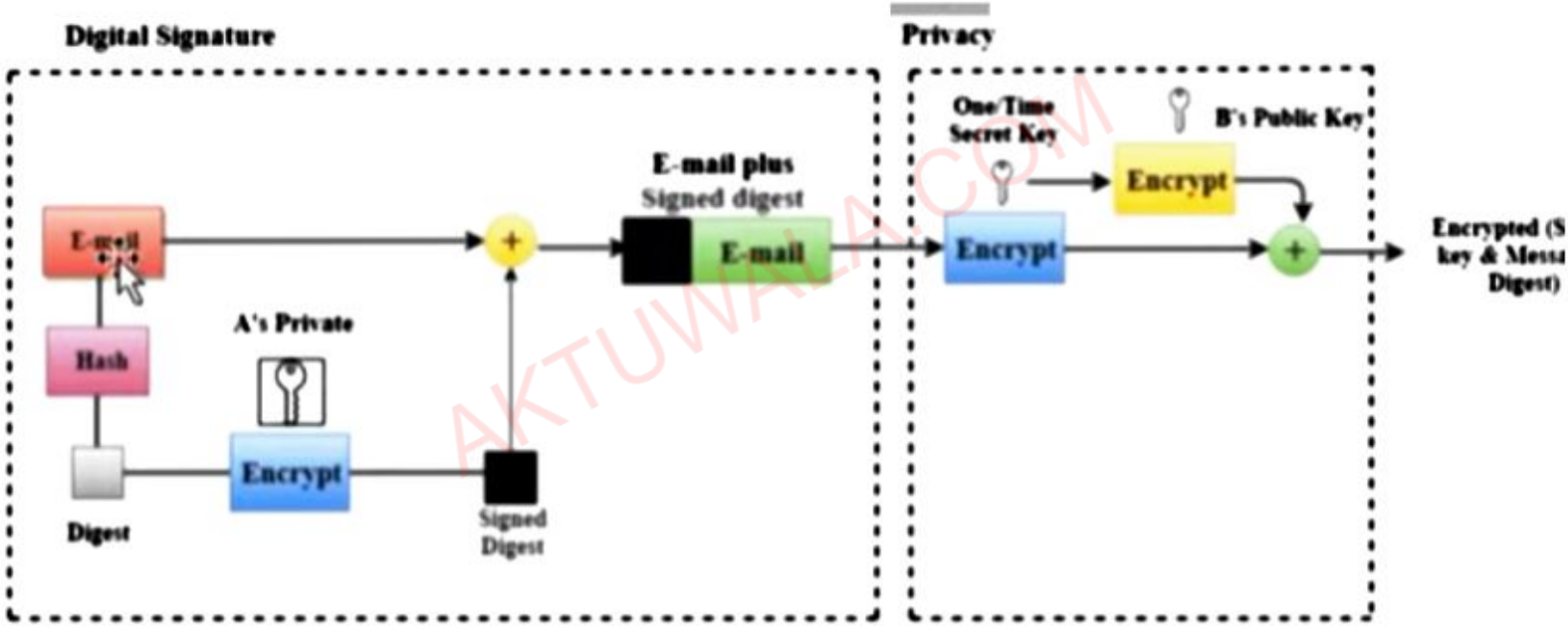
- **Email Encryption** - It encrypts the content of the email sent between two S/MIME enabled users to make it unreadable to anyone other than the intended recipient.

- **Digital Signature** - It digitally signs the emails sent between two S/MIME enabled users to eliminate any risk of spoofing.

PGP-Pretty Good Privacy

- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP uses a digital signature.
- PGP uses a combination of secret key encryption and public key encryption to provide privacy.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.

- PGP uses a digital signature.
- PGP uses a combination of secret key encryption and public key encryption to provide privacy.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm.



SET-Secure Electronic Transaction

Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario.

SET is not some system that enables payment but it is a security protocol applied on those payments.

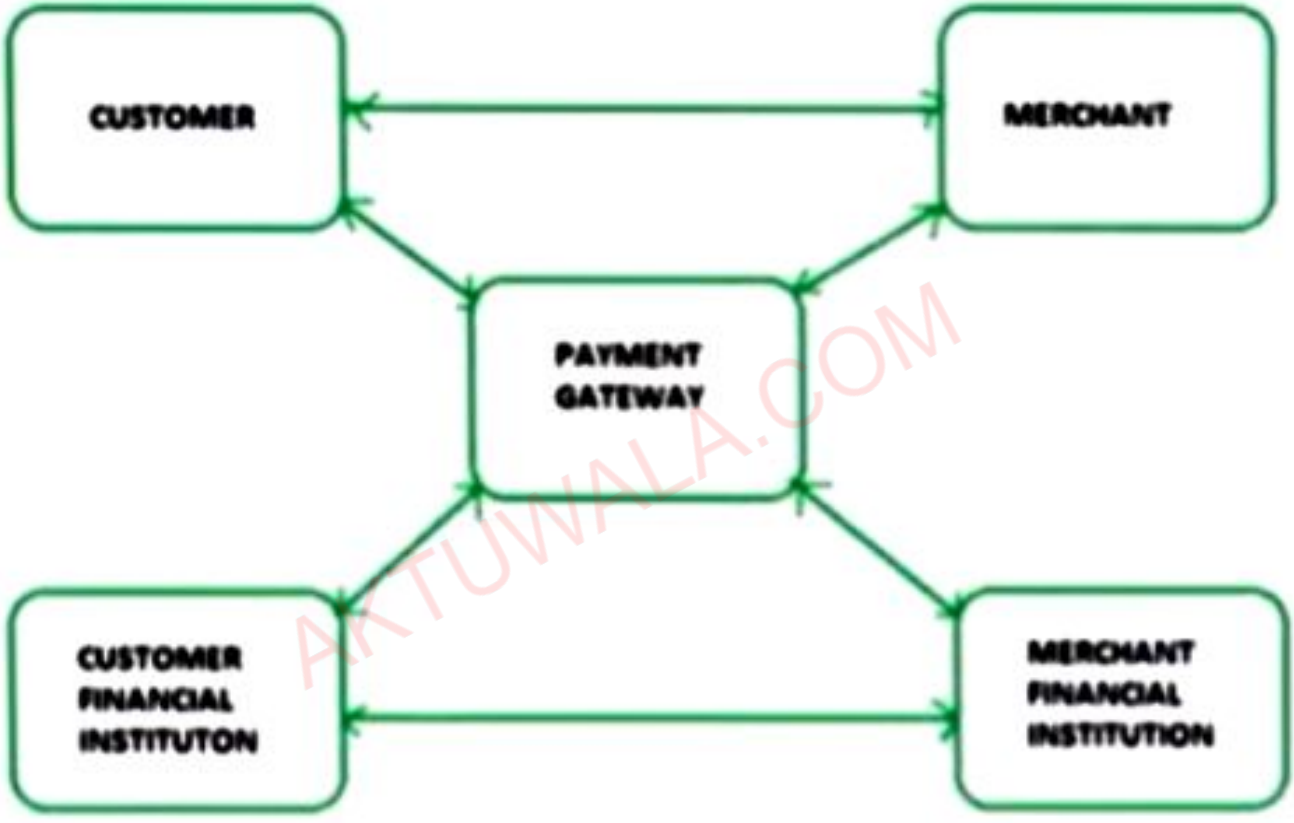
It uses different encryption and hashing techniques to secure payments over internet done through credit cards.

SET protocol was supported in development by major

security protocol applied on those payments.

It uses different encryption and hashing techniques to secure payments over internet done through credit cards.

SET protocol was supported in development by major organizations like Visa, MasterCard, Microsoft which provided its Secure Transaction Technology (STT) and Netscape which provided technology of Secure Socket Layer (SSL).



Advantages of digital signatures

- **Saves time**
- **Cost savings**
- **Workflow efficiency**
- **Better customer experience**
- **Security**
- **Legal validity**
- **Business efficiency**