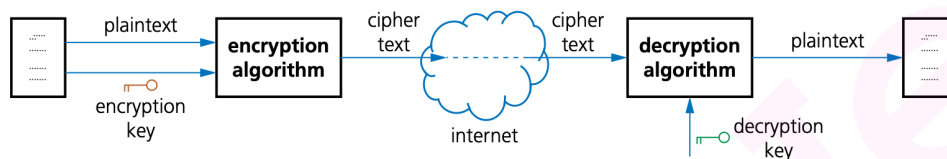


## 17. Security

### 17.1 Encryption, Encryption Protocols, and Digital Certificates

#### Definitions

- **Encryption** is the process of converting data into a coded form to prevent unauthorized access.
- **Plain text** is the original data to be sent. **Cipher text** is the result when plain texts have gone through an encryption algorithm.
- The process of encryption is shown in the diagram:



#### Why Encryption

- To keep data secure & information away from a hacker.
- Information needs to be impossible to understand by a 3rd party.
- Only authorized people with the key can understand the information.

#### Security Concerns of Encryption

1. **Confidentiality:** only intended recipient shall be able to decipher the data.
2. **Authenticity:** the need to identify who sent the data and verify that the sending source is legitimate.
3. **Integrity:** the data shall reach its destination without any changes.
4. **Non-repudiation:** neither the sender nor the recipient should be able to deny that they were part of the data transmission which just took place.

#### Symmetric Encryption

- Uses a **single key** to decrypt and encrypt data.
- This encryption key **must be shared** between the sender and the receiver.
  - This triggers the **key distribution problem**: the key itself may be intercepted by an eavesdropper/hacker when it's sent to recipients.
- However, sometimes the shared key doesn't need to be directly transmitted between the two parties.
  - The **Diffie-Hellman key exchange** allows two parties to independently compute the same secret key using public values and their private inputs.

#### Drawbacks

- Key as to be exchanged securely.
- Once compromised the key can decrypt both sent and received messages.
- Cannot ensure **non-repudiation** (proof of identity and origin of data).

## Asymmetric Encryption

- Uses a **public-private key** system to decrypt and encrypt data separately.

### Public and private keys

- **Public key:** a key that is openly shared and used to **encrypt** data.
- **Private key:** a secret key never transmitted anywhere.
  - It has a matching public key.
  - It is used to **decrypt** data that was encrypted with its matching public key.
- A fundamental principle lies in public-private key cryptography:

What one key encrypts, the other can decrypt.

### Process

1. Each party generates their own matching private-public key pair using an asymmetric encryption algorithm (e.g., RSA).
  - The matching pairs of keys are mathematically linked but cannot be derived from each other.
2. The **recipient** sends their **public key** to the **sender**.
3. The **sender encrypts** the message using the **recipient's public key**.
4. The **recipient decrypts** the message using **the recipient's private key**.

## Quantum Cryptography

- If interested in a specific algorithm, check out **BB84** ([Paper](#) & [Explanation](#)).

### Purpose

- Using the laws of **quantum mechanics** (properties of photons)
- ... To produce a virtually **unbreakable encryption system**.
- Easy to **detect eavesdropping**
- ... Because measuring a quantum state disturbs it.
- To protect security of data transmitted over fiber optic cables.
- To enable the use of **longer keys**.

### Benefits

- Provides security based on laws of physics rather than mathematical algorithms, so more secure → virtually unhackable.
- Eavesdropping can be detected easily.
- Longer keys can be used.
- The performance of quantum cryptography is continuously improved, making it suitable for most valuable government/industrial secrets.

### Drawbacks

- **High cost** of purchasing / maintaining equipment required.
- Currently only works over relative **short distances**.

- Polarization of light may be altered while traveling down fiber optic cables.
- Error rates are relatively high as the tech is still being developed.
- Allows criminals and terrorists to hide their communications.
- Lacks many vital features such as digital signature, certified mail, etc.

## Protocols

- Both **Secure Sockets Layer (SSL)** and **Transport Layer Security (TLS)** are cryptographic protocols to provide secure communication over a network.
  - They operate in the **transport layer** in the TCP/IP protocol.
- TLS is a modern successor based on SSL (replaced).

## Purposes

- The SSL and TLS protocols provide communications securely over the network
- ... They provide **encryption**.
- They enable two parties to identify and authenticate each other
- ... And communicate with **confidentiality** and **integrity**.

## Use Cases

- Online banking and all financial transactions (e.g., online commerce).
- Private communications in the internet (e.g., voice calls, private emails).
- Cloud storage facilities.

## Secure Sockets Layer (SSL)

1. An application initiates an SSL connection and becomes the **client**.
2. Another application which receives the connection becomes the **server**.
3. Each new session begins with a **handshake**:
  - The **client** sends *supported SSL version*, a *random number*, and a *list of supported cipher suites* to the server.
  - The **server** responds with its *chosen cipher suites*, a *random number*, and its **digital certificate** which includes the server's **public key**.
  - The **client** verifies the server's digital certificate and obtains the public key.
  - The **client** generates a **pre-master secret**, encrypts it using the server's public key, and sends it to the server.
  - Both the **client** and the **server** compute a **symmetric session key** using random values from both parties and the pre-master secret.
  - Both parties send a "Finished" message encrypted with the **session key**.
4. All later communication is encrypted and decrypted using the **symmetric session key**.

## Transport Layer Security (TLS)

- While SSL typically only supports RSA, TLS is more **extensible** in key algorithms.
  - It supports more modern & secure algorithms like ECDHE.
- In SSL, if the server's private key is hacked, all past communication is leaked.

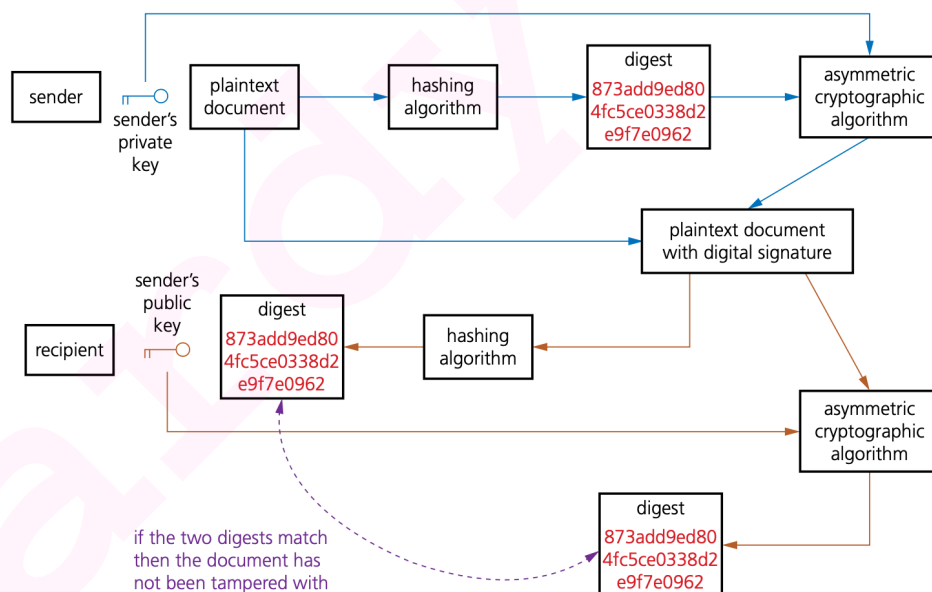
- In TLS, each session has its own private key, and hence even if long-term keys are lost, past sessions remain secure.
- Both TLS and SSL include two layers: **record protocol** and **handshake protocol**.
- Both TLS and SSL utilize **session catching**: a mechanism to reuse **cryptographic session parameters** so that the client and the server don't need to perform the handshaking protocol every time.

## Digital Signatures

- **Digital signatures** are digital codes used to ensure **authenticity**, **integrity** and **non-repudiation**.
- Digital signatures are commonly produced from **digital certificates**. Below describes another way digital signatures can be created.

### Mechanism

1. The sender **hashes** the plain text to produce a **digest** (e.g., using SHA-256).
2. They **encrypt** the hash using their **private key**.
3. The **encrypted hash** becomes the **digital signature**.
4. The recipient:
  - Hashes the received plain text.
  - **Decrypts** the digital signature using the sender's public key.
  - **Compares** the two hashes to confirm authenticity and integrity.



## Digital Certificates

- **Digital Certificates** are electronic "documents" used to prove the online identity of a website or an individual.
- They contain (i) a **public key** and (ii) **information identifying the owner of the certificate and the issuer**.

### Process to Acquire a Digital Certificate

1. The organization requests a certificate from a **Certificate Authority (CA)**.
2. The organization may send their **public key** to CA.

3. The organization gathers all the information required by the CA in order to obtain their certificate, which includes information to prove their identity.
4. The CA **verifies** the organization's identity.
5. The CA issues the certificate including the organization's public key (and other information).