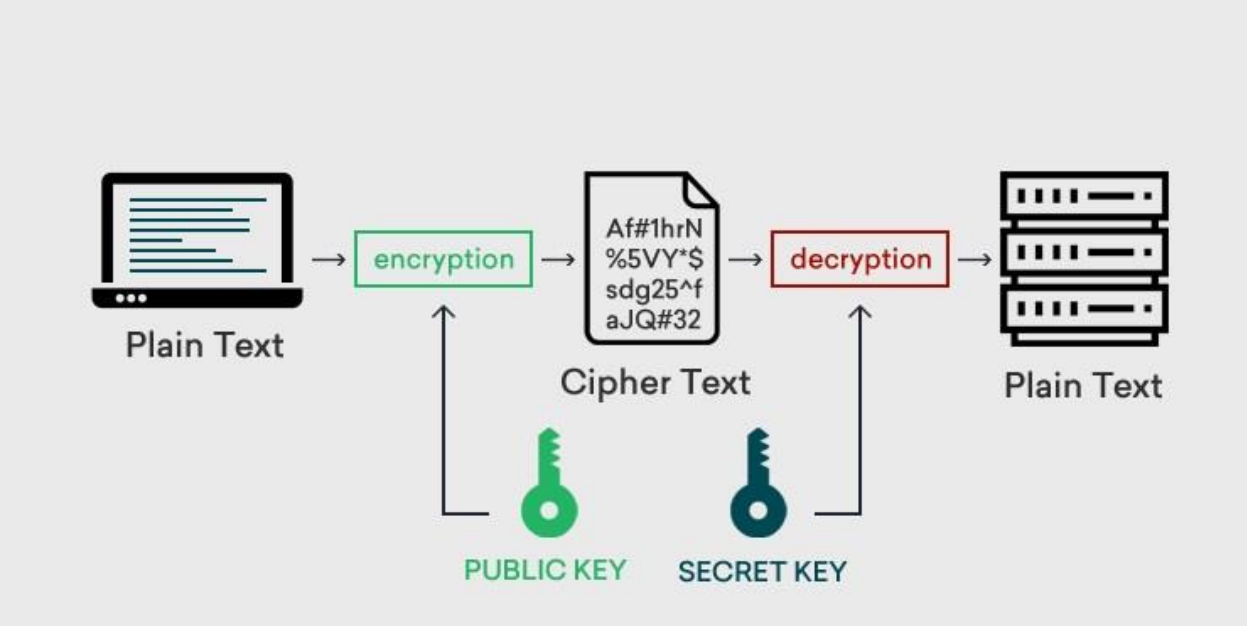
Encryption

Data encryption is the process of converting readable information (plaintext) into an unreadable format (ciphertext) to protect it from unauthorized access. It is a method of preserving data confidentiality by transforming it into ciphertext, which can only be decoded using a unique decryption key produced at the time of the encryption or before it. The conversion of plaintext into ciphertext is known as encryption.



By using encryption keys and mathematical algorithms, the data is scrambled so that anyone intercepting it without the proper key cannot understand the contents.

When the intended recipient receives the encrypted data, they use the matching decryption key to return it to its original, readable form. This approach ensures that sensitive information such as personal details, financial data, or confidential communications remains secure as it travels over networks or is stored on devices.

Key Objectives of Encryption

1. Data Confidentiality

- **Meaning**: Only the intended receiver can read the information.
- **How**: Data is scrambled into ciphertext, so even if a hacker intercepts it, they cannot understand it without the key.
- **Example**: When you log into online banking, your username and password are encrypted so only the bank's server can read them.

---

2. Data Integrity

- **Meaning**: Ensures that data is not changed, modified, or tampered with during storage or transmission.
- **How**: If encrypted data is altered, it becomes corrupted and unreadable during decryption. Integrity checks (like hashes, digital signatures) are also used.
- **Example**: If someone tries to modify an encrypted exam paper while it is being sent online, the decryption process will fail, showing that tampering happened.

---

3. Authentication

- **Meaning**: Verifies the identity of the sender or receiver.

- **How**: Encryption is often combined with **digital certificates** or **keys** to confirm that the communication is from a genuine source.
- **Example**: When you visit a website with HTTPS, your browser checks the site's SSL/TLS certificate (which uses encryption) to make sure it's really the official site, not a fake one.

---

4. Non-Repudiation

- **Meaning**: The sender cannot deny sending the data, and the receiver cannot deny receiving it.
- **How**: Achieved using **digital signatures and encryption**. A digital signature is unique to the sender, so they cannot later claim "I never sent this."
- **Example**: In online contracts, once you digitally sign a document, encryption ensures you cannot deny signing it later.

---

5. Privacy & Trust

- **Privacy:** Encryption ensures that personal or sensitive data (like chats, emails, passwords, medical reports, or bank details) cannot be read by anyone except the intended person. This keeps your private life safe from hackers, spies, or unauthorized access.
- **Trust:** When people know their data is secure, they feel confident using online services. For example, customers trust online banking, shopping, and digital payments only because encryption protects their money and identity.

💡 **Example:**

- **WhatsApp uses end-to-end encryption →** only you and your friend can read the messages.
- **Banks use SSL/TLS encryption (HTTPS) →** protects login and transactions, so you trust the bank's website.

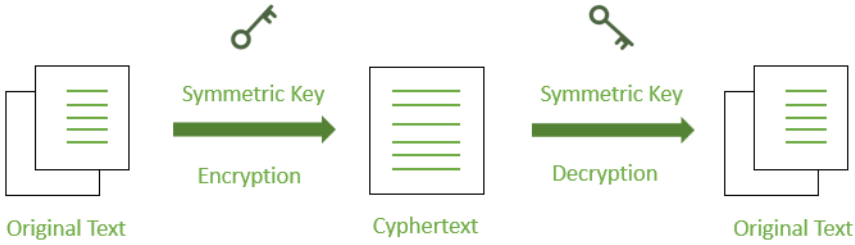
How Encryption Works (Step by Step)

Let's imagine you send a secret message "HELLO" to your friend:

1. **Input (Plaintext)** → "HELLO".
2. **Encryption Algorithm** → applies a set of mathematical rules.
3. **Key** → tells the algorithm how to scramble the text.
    - Example: Caesar Cipher (Shift by +3).
    - HELLO → KHOOR.
4. **Output (Ciphertext)** → "KHOOR".
5. Friend receives "KHOOR" and uses the **decryption key** (-3).
6. Decryption → "HELLO" again.

Types of Encryption

1.Symmetric Encryption:



1. Original Text (Plaintext)

This is the actual readable data (like a message, password, or file).
Example: "HELLO WORLD".

---

2. Encryption Process

- The **encryption algorithm** scrambles the plaintext into unreadable form.
- A **symmetric key** (single secret key) is used.
- Without the key, the ciphertext looks like random garbage.

👉 Example: "HELLO WORLD" → "X9@#L20Z".

---

3. Ciphertext

- This is the scrambled, unreadable output.
- It can be safely transmitted over the internet.
- Even if a hacker steals it, they cannot read it without the key.

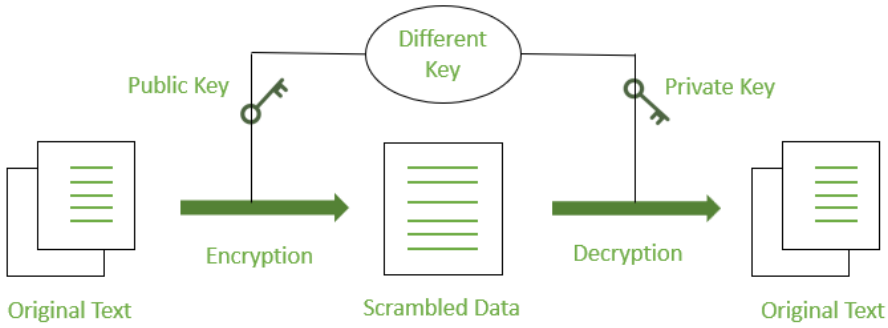
---

4. Decryption Process

- The same **symmetric key** is used again.
- Decryption algorithm converts ciphertext back into the original text.
- Only the sender and receiver (who both have the key) can understand the message.

👉 Example: "X9@#L20Z" → "HELLO WORLD".

2.Asymmetric Encryption:



1. Original Text (Plaintext)

This is the normal readable data (e.g., "HELLO FRIEND").

---

2. Encryption with Public Key

- A **public key** is used to encrypt the plaintext.
- Public key is **not secret** → it can be shared openly with anyone.
- Once encrypted, the data becomes **scrambled data (ciphertext)**.
- However, this ciphertext **can only be decrypted by the matching private key**.

👉 Example: "HELLO FRIEND" → "8dj#X!92Zk@".

---

3. Scrambled Data (Ciphertext)

- This looks like random characters.
- Safe to transmit over the internet, because even if hackers intercept it, they **cannot decrypt it** without the private key.

---

4. Decryption with Private Key

- The receiver uses their **private key** to decrypt the scrambled data.
- Private key is **kept secret** and never shared.
- Only the holder of the private key can read the original text.

👉 Example: "8dj#X!92Zk@" → "HELLO FRIEND".

Advantages of Encryption

1. **Data Confidentiality**

- Protects sensitive information (like passwords, bank details, medical records) from unauthorized access.

2. **Data Integrity**
    - Ensures data is not modified during transmission or storage. Any tampering is detected.
3. **Authentication**
    - Confirms the identity of the sender or receiver using encryption with digital certificates.
4. **Non-Repudiation**
    - Prevents a sender from denying they sent a message (using digital signatures).
5. **Privacy Protection**
    - Keeps personal communications (chats, emails, calls) private.
6. **Builds Trust in Digital Services**
    - People confidently use online banking, shopping, and digital payments because encryption protects them.

Disadvantages of Encryption

1. **Key Management Problems**
    - If the encryption key is lost, the data becomes permanently inaccessible.
2. **Performance Issues**

- Strong encryption can slow down systems because it requires high processing power.

3. **Complexity**
    - Implementing and managing encryption systems can be complicated.
4. **Cost**
    - Advanced encryption systems, hardware, and key management can be expensive.

5. **False Sense of Security**
    - Encryption protects data, but it doesn’t prevent hacking, phishing, or malware attacks.
6. **Potential for Misuse**
    - Criminals can also use encryption to hide illegal activities from authorities.