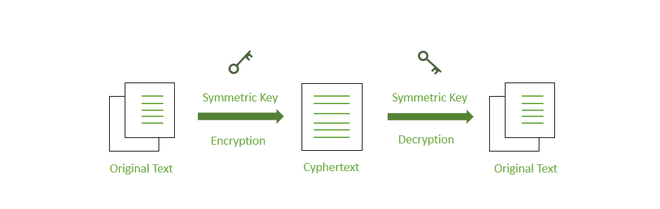
**Digital Signatures and Certificates:**

**Encryption** – Process of converting electronic data into another form, called ciphertext, which cannot be easily understood by anyone except the authorized parties.   
**Decryption**– The message is encrypted at the sender’s side using various encryption algorithms and decrypted at the receiver’s end with the help of the decryption algorithms.

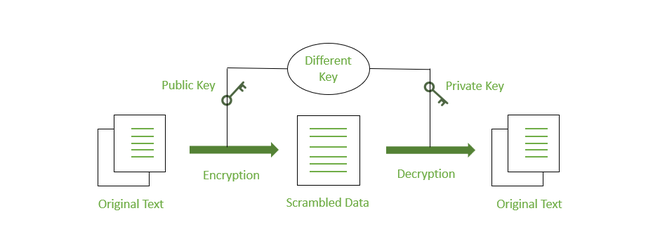
**Types of Encryption:**

**1. Symmetric Encryption**

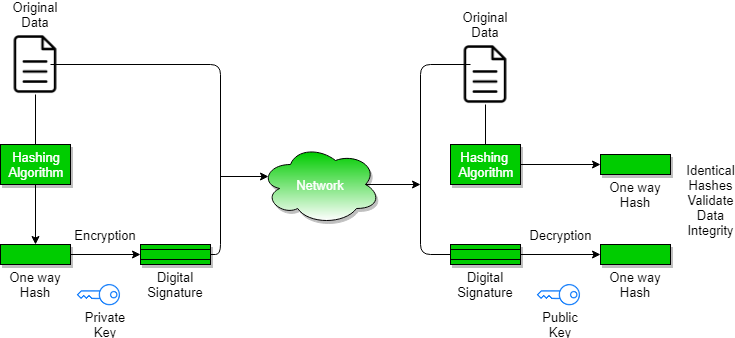
* Uses the same key for both encryption and decryption.
* The key must be securely shared and kept confidential, as it allows full access to the data.
* Example: AES (Advanced Encryption Standard) 

**2. Asymmetric Encryption (Public-Key Cryptography)**

* Utilizes a pair of keys:
  + **Public key**: Shared openly.
  + **Private key**: Kept secret by the owner.
* Encryption is done using one key, and decryption requires the other key in the pair.
* Offers enhanced security, as private keys are never shared.



**Diagram:**



**Digital Signature:**

A **digital signature** is a mathematical method used to ensure the authenticity and integrity of messages, software, or digital documents. It verifies that the message originates from a specific sender and has not been altered during transmission.

**Key Components of Digital Signatures:**

1. **Key Generation Algorithms**:
   * Generate a **private key** for signing and a corresponding **public key** for verification.
   * Ensure authenticity and prevent unauthorized data alteration during digital transactions.
2. **Signing Algorithms**:
   * Create a one-way hash of the data to be signed.
   * Encrypt the hash using the **private key** to produce the digital signature.
   * Encrypting the hash saves time, as hash values are shorter and faster to process.
3. **Signature Verification Algorithms**:
   * The verifier uses the **public key** and the received digital signature to calculate a value.
   * The same hash function is applied to the received data to generate a new hash value.
   * The signature is valid if the computed value matches the hash value; otherwise, it is invalid.

**Steps to Create and Verify a Digital Signature**

1. **Creating the Digital Signature**:
   * A **message digest** is generated by applying a hash function to the message.
     + Message Digest=Hash Function (Message)
   * The message digest is encrypted using the **private key** of the sender to form the digital signature.
     + Digital Signature=Encryption (Sender’s Private Key, Message Digest)
2. **Transmission**:
   * The message and the digital signature are sent together to the receiver.
     + Transmitted Data= Message + Digital Signature
3. **Verification by the Receiver**:
   * The receiver decrypts the digital signature using the **public key** of the sender. This ensures **authenticity**, as only the sender can encrypt the signature using their private key.
     + Decrypted Digest=Decryption (Sender’s Public Key, Digital Signature)
4. **Integrity Check**:
   * The receiver computes the message digest from the received message using the same hash function.
     + Computed Digest=Hash Function (Received Message)
   * The receiver compares the **decrypted digest** with the **computed digest**. If they match, the message's **integrity** is confirmed.

**Digital Certificate:**

A **digital certificate** is issued by a trusted third party, called a **Certificate Authority (CA)**, to verify the identity of an individual or entity. It links a public key to the certificate holder and helps establish trust between sender and receiver.

**Contents of a Digital Certificate:**

1. **Certificate Holder's Name**: Identifies the individual or entity associated with the certificate.
2. **Serial Number**: Uniquely identifies the certificate.
3. **Expiration Dates**: Specifies the validity period of the certificate.
4. **Public Key**: Enables decryption of messages and digital signatures.
5. **CA's Digital Signature**: Verifies the authenticity of the certificate.

**Advantages of Digital Certificates:**

1. **Network Security**: Forms part of a layered cybersecurity strategy, protecting against manipulation and man-in-the-middle attacks.
2. **Verification**: Restricts access to sensitive data by ensuring reliable identity verification at multiple endpoints.
3. **Buyer Success**: Demonstrates website reliability, supported by trusted Certificate Authorities (CAs), which builds consumer confidence.

**Disadvantages of Digital Certificates:**

1. **Phishing Attacks**: Attackers can create fake websites and obtain legitimate-looking certificates to deceive users into sharing sensitive data.
2. **Weak Encryption**: Older certificates may use outdated and less secure encryption algorithms, making them vulnerable to breaches.
3. **Misconfiguration**: Incorrectly configured certificates can expose websites and online interactions to attacks.