Cryptography

The word **cryptography** comes from the Greek words **κρυπτός (kryptós)**, meaning “hidden,” and **γράφειν (gráphein)**, meaning “writing.” Its original meaning is “secret writing.” Cryptography has evolved into a distinct field, primarily within computer science, that deals with creating encryption (secret codes) and their decryption (breaking these codes).

With the spread of **electronic communication**, three fundamental requirements for encryption methods to ensure secure Internet communication channels have emerged. These requirements are crucial to achieving secure communication.

Basic Requirements for a Secure Channel

1. **Confidentiality**: The content of messages should only be accessible to the communicating parties. No third party should be able to intercept and understand the message. This is achieved through encryption algorithms, which are designed to be difficult to reverse-engineer, efficient in computation, and easy to use. It’s essential to prove mathematically the limits of a given encryption method.

- **Example**: When using the internet, applications like email or messaging services encrypt the content of the message so that if an attacker intercepts it, they cannot read it without the correct decryption key.
- **Tools**: Various encryption algorithms like **AES (Advanced Encryption Standard)** or **RSA** are used to ensure confidentiality.

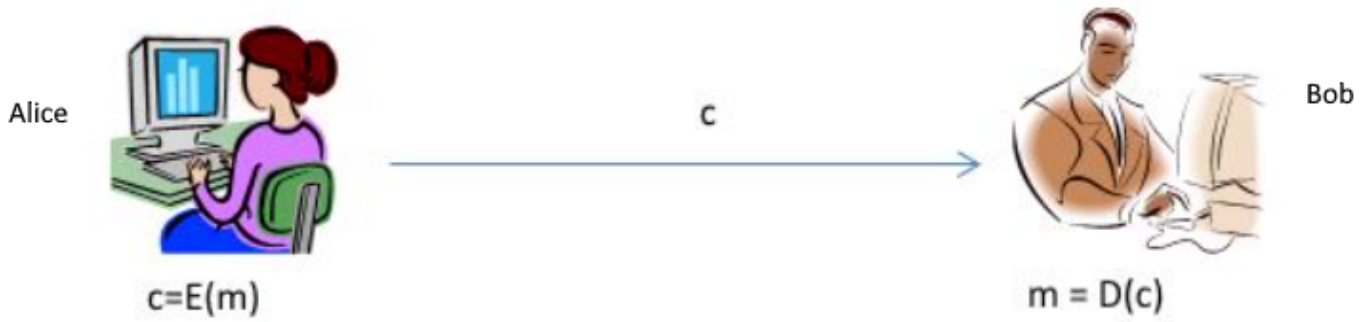
2. **Authenticity**: The communicating parties need to verify each other's identity, even if they have never met in person. This is crucial for secure internet transactions and communication with remote servers, which may be impossible to physically reach. Authentication ensures that a sender is indeed who they claim to be.

- **Example**: In online banking, users need to verify the authenticity of the bank’s website before they can securely communicate and transfer sensitive information.
- **Tools**: Authentication can be achieved using **certificates** issued by trusted authorities (Certification Authorities or CAs) and **public-key infrastructure (PKI)**.

3. **Integrity**: It must be ensured that the data exchanged between parties remains unchanged during transmission. Unauthorized changes or tampering with the data must be detectable. Integrity is often ensured through the use of **digital signatures**.

- **Example**: In the context of signing legal contracts online, the digital signature confirms that the document hasn't been altered since it was signed.
- **Tools**: **Hashing algorithms** and **digital signatures** ensure the integrity of messages and files. A digital signature binds a cryptographic hash of the document with the sender’s private key, making it evident if the data has been tampered with.

Basic communication model



Where Alice is the sender(A), Bob is the receiver (B),

m: message, c: encrypted message,

E(): encrypt function,

D(): decrypt function,

D() is the inverse function of E().