**Cryptography**

**Cryptography** is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols that prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security. Secure Communication refers to the scenario where the message or data shared between two parties can’t be accessed by an adversary. In Cryptography, an Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security. Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

1. **Confidentiality** refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.
2. **Data integrity** refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.
3. **Authentication** is the process of making sure that the piece of data being claimed by the user belongs to it.
4. **Non-repudiation** refers to the ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

Consider two parties Alice and Bob. Now, Alice wants to send a message m to Bob over a secure channel. So, what happens is as follows. The sender’s message or sometimes called the Plaintext, is converted into an unreadable form using a Key k. The resultant text obtained is called the Ciphertext. This process is known as Encryption. At the time of received, the Ciphertext is converted back into the plaintext using the same Key k, so that it can be read by the receiver. This process is known as Decryption.

Alice (Sender) Bob (Receiver)

C = E (m, k) ----> m = D (C, k)

Here, C refers to the Ciphertext while E and D are the Encryption and Decryption algorithms respectively. Let’s consider the case of Caesar Cipher or Shift Cipher as an example. As the name suggests, in Caesar’s Cipher each character in a word is replaced by another character under some defined rules. Thus, if A is replaced by D, B by E and so on. Then, each character in the word would be shifted by a position of 3.

**Types of Cryptography:**

There are several types of cryptography, each with its own unique features and applications. Some of the most common types of cryptography include:

**1. Symmetric-key cryptography:** This type of cryptography involves the use of a single key to encrypt and decrypt data. Both the sender and receiver use the same key, which must be kept secret to maintain the security of the communication.

**2. Asymmetric-key cryptography:**Asymmetric-key cryptography, also known as public-key cryptography, uses a pair of keys – a public key and a private key – to encrypt and decrypt data. The public key is available to anyone, while the private key is kept secret by the owner.

**Hash functions:** A hash function is a mathematical algorithm that converts data of any size into a fixed-size output. Hash functions are often used to verify the integrity of data and ensure that it has not been tampered with.

**Applications of Cryptography:**

Cryptography has a wide range of applications in modern-day communication, including:

* **Secure online transactions:**Cryptography is used to secure online transactions, such as online banking and e-commerce, by encrypting sensitive data and protecting it from unauthorized access.
* **Digital signatures:**Digital signatures are used to verify the authenticity and integrity of digital documents and ensure that they have not been tampered with.
* **Password protection:**Passwords are often encrypted using cryptographic algorithms to protect them from being stolen or intercepted.

Military and intelligence applications: Cryptography is widely used in military and intelligence applications to protect classified information and communications.

**Challenges of Cryptography:**

While cryptography is a powerful tool for securing information, it also presents several challenges, including:

* **Key management**: Cryptography relies on the use of keys, which must be managed carefully to maintain the security of the communication.
* **Quantum computing:**The development of quantum computing poses a potential threat to current cryptographic algorithms, which may become vulnerable to attacks.
* **Human error:** Cryptography is only as strong as its weakest link, and human error can easily compromise the security of a communication.