Cryptography

Cryptography is the technique of securing information and communications through use of codes so that only those persons for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information.
The prefix “crypt” means “hidden” and the suffix graphy means “writing”.
Cryptography is necessary when communicating over any untrusted medium which includes just about any network , particularly the internet.

Modern cryptography concerns itself with the following four objectives:

1. **Confidentiality.** The information cannot be understood by anyone for whom it was unintended.
2. **Integrity.**The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
3. **Non-repudiation.** The creator/sender of the information cannot deny at a later stage their intentions in the creation or transmission of the information.
4. **Authentication.** The sender and receiver can confirm each other's identity and the origin/destination of the information.

Plain Text:- Any communication in the language that you and I speak that is human language , takes the form of Plain Text.

Plaintext can refer to anything which humans can understand and/or relate to. This may be as simple as English sentences, a script, or Java code. If you can make sense of what is written, then it is in plaintext.

Ciphertext, or encrypted text, is a series of randomized letters and numbers which humans cannot make any sense of.

Plaintext: This is a plaintext.

Ciphertext: Aopz pz h wshpualea.

Example

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.

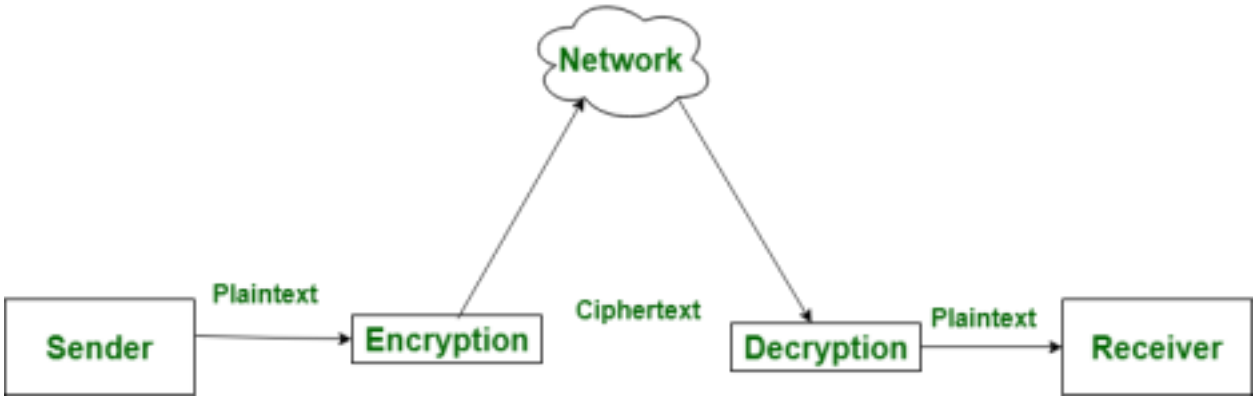
The sender's message or sometimes called the Plaintext, is converted into an unreadable form using a Key k. The resultant text obtained is called the Ciphertext. This process is known as Encryption. At the time of receival, the Ciphertext is converted back into the plaintext using the same Key k, so 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.

Encryption and Decryption

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Whereas **Decryption** is the process of converting meaningless message (Ciphertext) into its original form (Plaintext).



Encryption: Encryption means that the sender converts the original information into another form and sends the unintelligible message over the network.

Decryption: Decryption reverses the Encryption process in order to transform the message back to the original form.

Difference Between Encryption and Decryption -

S.No	Encryption	Decryption
1.	It is a method of transforming a plain or clear text into ciphertext using a key.	It is a method of transforming ciphertext into plain or clear text.
2.	Process of encryption takes place at the sender's end.	Process of decryption takes place at the receiver's end.
3.	The encrypted data is called Ciphertext.	Decrypted data is called Plain text.
4.	A public key or secret key is used in the process of Encryption.	A secret key or private key is used in the process of Decryption.
5.	In encryption the sender sends the data once it is encrypted.	In decryption, the receiver decodes the data once it is received.