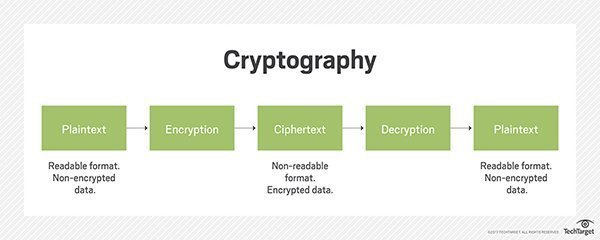
**Practical-1**

**Cryptography:**

Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher

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 his or her 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



**Asymmetric key cryptography:**

Asymmetric[cryptography](https://searchsecurity.techtarget.com/definition/cryptography), also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the [public key](https://searchsecurity.techtarget.com/definition/public-key). The other key in the pair is kept secret; it is called the [private key](https://searchsecurity.techtarget.com/definition/private-key). Either of the keys can be used to[encrypt](https://searchsecurity.techtarget.com/definition/encryption)a message; the opposite key from the one used to encrypt the message is used for decryption.

Many protocols like [SSH](https://searchsecurity.techtarget.com/definition/Secure-Shell), [OpenPGP](https://whatis.techtarget.com/definition/OpenPGP), [S/MIME](https://whatis.techtarget.com/definition/S-MIME-Secure-Multi-Purpose-Internet-Mail-Extensions), and SSL/TLS rely on asymmetric cryptography for encryption and [digital signature](https://searchsecurity.techtarget.com/definition/digital-signature) functions.

Every user in this system needs to have a pair of dissimilar keys, **private key** and **public key**. These keys are mathematically related − when one key is used for encryption, the other can decrypt the ciphertext back to the original plaintext.

* It requires to put the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called **Public Key Encryption**.
* Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is a strength of this scheme.
* When *Host1* needs to send data to *Host2,* he obtains the public key of *Host2* from repository, encrypts the data, and transmits.
* *Host2* uses his private key to extract the plaintext.

### **Symmetric Key Cryptography:**

The encryption process where **same keys are used for encrypting and decrypting** the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is referred to as **symmetric cryptography**.

A few well-known examples of symmetric key encryption methods are − Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

* Persons using symmetric key encryption must share a common key prior to exchange of information.
* Keys are recommended to be changed regularly to prevent any attack on the system.
* A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.

### **Challenge of Symmetric Key Cryptosystem**

There are two restrictive challenges of employing symmetric key cryptography.

* **Key establishment**− Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.
* **Trust Issue**− Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver ‘trust’ each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed.

These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer. These limitations of symmetric key encryption gave rise to asymmetric key encryption schemes.

## **Relation between Encryption scheme**

A summary of basic key properties of two types of cryptosystems is given below −

|  |  |  |
| --- | --- | --- |
|  | Symmetric Cryptosystems | Public Key Cryptosystems |
| **Relation between Keys** | Same | Different, but mathematically related |
| Encryption Key | Symmetric | Public |
| Decryption Key | Symmetric | Private |

[**Reference**](https://www.tutorialspoint.com/cryptography/cryptosystems.htm)

<https://www.tutorialspoint.com/cryptography/cryptosystems.htm>

<https://searchsecurity.techtarget.com/definition/cryptography>

https://searchsecurity.techtarget.com/definition/asymmetric-cryptography