HIMA SUTARIA

160470107058

VVPEC CE SEM-7

Lab manual

Information and network Security

Contents

[Introduction to Information And Network Security: 1](#_Toc12345730)

# 

# Introduction to Information And Network Security:

**What is 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. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing."

Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.

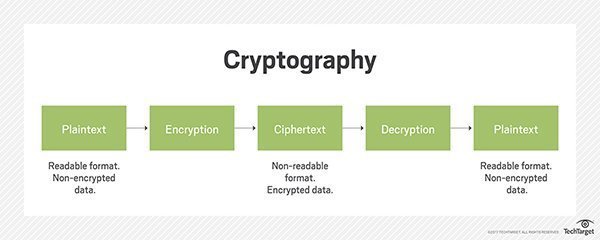
Cryptography also allows senders and receivers to authenticate each other through the use of key pairs. There are various types of algorithms for encryption, some common algorithms include:

• Secret Key Cryptography (SKC): Here only one key is used for both encryption and decryption. This type of encryption is also referred to as symmetric encryption.

• Public Key Cryptography (PKC): Here two keys are used. This type of encryption is also called asymmetric encryption. One key is the public key that anyone can access. The other key is the private key, and only the owner can access it. The sender encrypts the information using the receiver’s public key. The receiver decrypts the message using his/her private key.

**Following objects of cryptography:**

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. **Authentication**: the sender and receiver can confirm each other's identity and the origin/destination of the information.

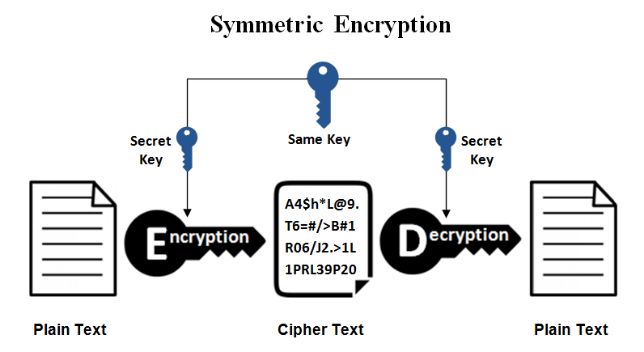


**What is Symmetric & Asymmetric Cryptography?**

Cryptography is classified into symmetric cryptography and asymmetric cryptography.

**SYMMETRIC CRYPTOGRAPHY**

It involves usage of one secret key along with encryption and decryption algorithms which help in securing the contents of the message. The strength of symmetric key cryptography depends upon the number of key bits. It is relatively faster than asymmetric key cryptography. There arises a key distribution problem as the key has to be transferred from the sender to receiver through a secure channel.



**Advantages**

• Very fast encryption and decryption of a message

• The bigger the code of the key, the greater the safety

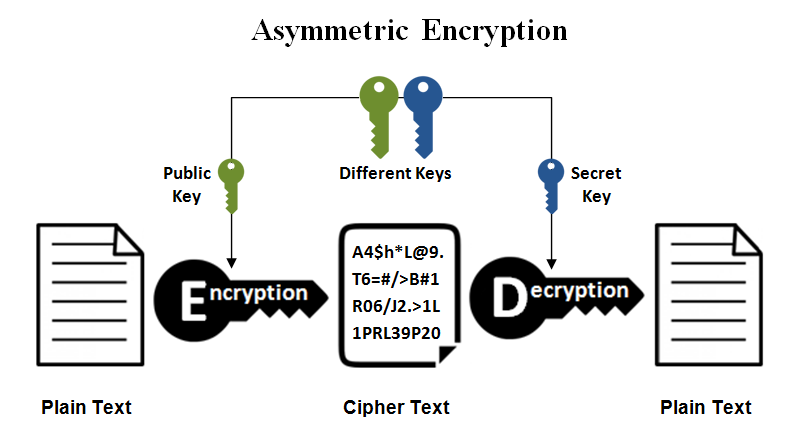
**Disadvantages**

• Exchange of the key: It must be ensured that the key to encryption, will be enchanged via a secure channel. However, in practice this can be really difficult.

• The number of the keys that are required: For each pair of participants that wish to enchange encrypted messages, a new key is required.

**ASYMMETRIC CRYPTOGRAPHY**

It is also known as public key cryptography because it involves usage of a public key along with secret key. It solves the problem of key distribution as both parties uses different keys for encryption/decryption. It is not feasible to use for decrypting bulk messages as it is very slow compared to symmetric key cryptography.

****

**Advantages**

* The private key does not need to be transmitted via a secure channel in order for the encryption to be successful
* There is the possibility of an electronic signature(digital signature)

**Disadvantages**

* The high cost to encrypt and decrypt messages(much slower compared to symmetric encryption)

**Difference Between Symmetric and Asymmetric Encryption**

* Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetrical encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.
* Symmetric encryption is an old technique while asymmetric encryption is relatively new.
* Asymmetric encryption was introduced to complement the inherent problem of the need to share the key in symmetrical encryption model, eliminating the need to share the key by using a pair of public-private keys.
* Asymmetric encryption takes relatively more time than the symmetric encryption.

**References:**

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

<https://www.geeksforgeeks.org/cryptography-introduction-to-crypto-terminologies/>

<http://www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf>

<https://greengarageblog.org/8-pros-and-cons-of-asymmetric-encryption>