mishil dobariya

160470107013

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:

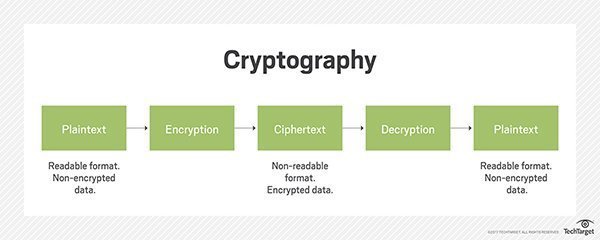
**What is Cryptography?**

Cryptography is a method of protecting information and communications through the use of secret key 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 is closely related to the disciplines of [cryptology](https://searchsecurity.techtarget.com/definition/cryptology) and [cryptanalysis](https://searchsecurity.techtarget.com/definition/cryptanalysis). It includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling [plaintext](https://searchsecurity.techtarget.com/definition/plaintext) (ordinary text, sometimes referred to as cleartext) into [ciphertext](https://whatis.techtarget.com/definition/ciphertext) (a process called [encryption](https://searchsecurity.techtarget.com/definition/encryption)), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

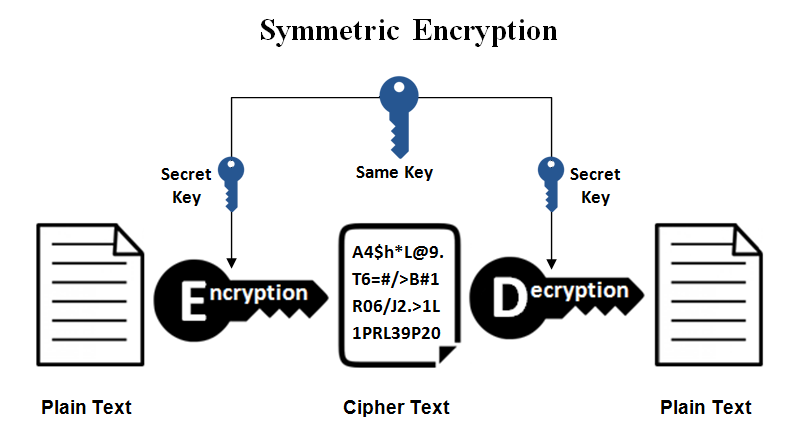
**Following objects of cryptography:**

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?**

**Symmetric key 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.

****

**Pros of Symmetric key cryptography:**

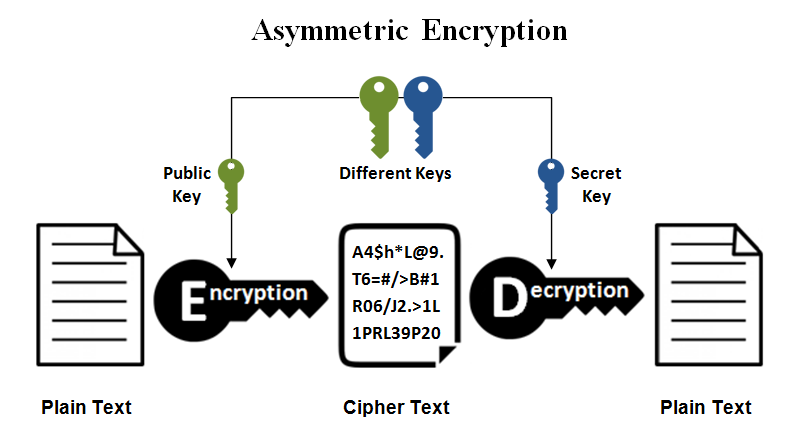
* A symmetric cryptography is faster.
* In Symmetric Cryptography, encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted. Since there is no key transmitted with the data, the chances of data being decrypted are null.
* A symmetric cryptosystem uses password authentication to prove the receiver’s identity.
* A system only which possesses the secret key can decrypt a message.

**Cons of Symmetric key cryptography:**

* Sharing the Key
* More Damage if Compromised

**Assymetric key 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.

****

**Pros of Asymmetric key cryptography:**

* In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem.
* The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone.
* Can provide digital signatures that can be repudiated

**Cons of Asymmetric key cryptography:**

* **It is a slow process.**
* **It risks loss of private key, which may be irreparable.**

**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>