MIHIR SHUKLA

160470107054

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?**

To maintain the privacy and security of confidential and sensitive information there is a need of approaches which enhances the level of information security.[1]

The word "cryptography" is derived from the Greek kryptos, meaning hidden.[2]

Cryptography is the art and science of fabricating methods or algorithms that allow transmission of data in a secure manner by transforming the readable and understand-able data into irrational and unfathomable data in such a way that only the intended person is able to retrieve the exact original data from the data being transmitted.[1]

The conversion of data into a secret code for transmission over a public **network**. Today, most **cryptography** is digital, and the original text ("plaintext") is turned into a coded equivalent called "ciphertext" via an **encryption** algorithm.[3]

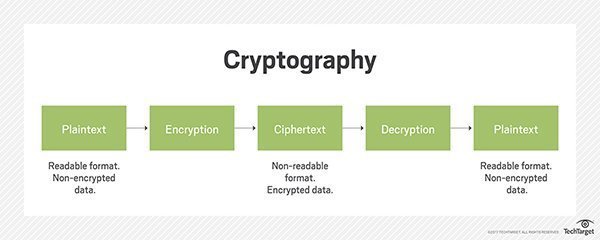


Figure-1 Cryptography

**Types of Cryptography**

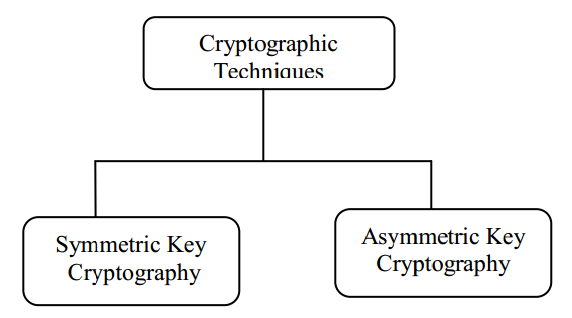


Figure-2 Cryptography Types

A]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.[4]

Same key is used by sender & receiver.

symmetric key cryptography makes use of two types of ciphers: **block ciphers** and **stream ciphers**. A block cipher takes a predetermined number of bits, known as a block, in the plaintext message and encrypts that block. Blocks are commonly composed of 64 bits but can be larger or smaller depending on the particular algorithm being used and the various modes in which the algorithm might be capable of operating. A stream cipher encrypts each bit in the plaintext message, 1 bit at a time. It is also possible for a block cipher to act as a stream cipher by setting a block size of 1 bit.[5]

Advantages:-

-simple

-Faster

Disadvantages:-

-Key must exchange in secure way

-easy for hacker to get a key as it is passed in unsecure way.

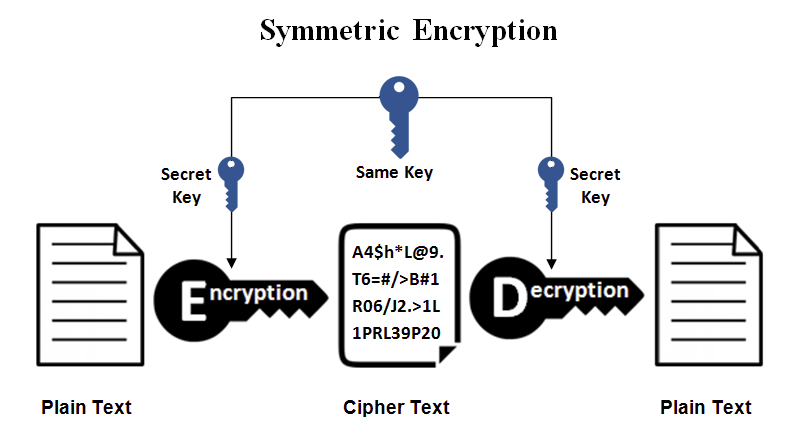


Figure-3 Symmetric cryptography

B]Asymmetric 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.[6]

2 different keys are used for sender & receiver.

Advantages:-

-no need to send key with message to receiver.

-if encryption key is stolen than also attacker can’t decrypt message as decryption key is only available with receiver.

-More secured authentication

Disadvantages:-

-Relatively complex

-Utilzes more resources

-Take more time

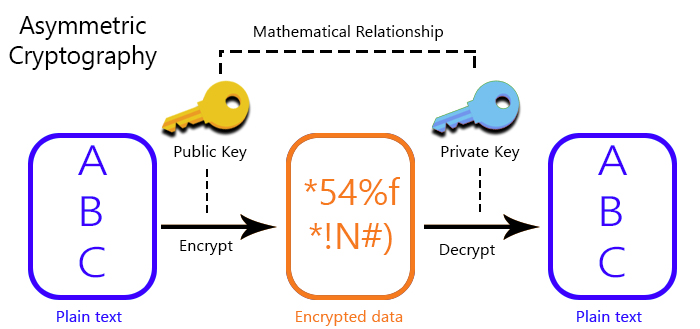
****

Figure-4 ASymmetric cryptography

**References**

1)ijsrset.com/paper/3512.pdf

2)www.google.com/overview of cryptography

3)https://searchsecurity.techtarget.com/definition/cryptography

4)https://www.geeksforgeeks.org/cryptography-introduction-to-crypto-terminologies/

5)https://www.sciencedirect.com/topics/computer-science/symmetric-key-cryptography

6)https://www.sciencedirect.com/topics/computer-science/asymmetric-key-cryptography