dARSHIT RATHOD

160470107048

VVPEC CE SEM-7

LAB MANUAL

INFORMATION & NETWORK SECURITY

Table of Contents

[INTRODUCTION TO INS: 1](#_Toc12385509)

# INTRODUCTION TO INS:

* **What is Cryptography??**

**Cryptography** is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analysing protocols which prevents malicious third parties from retrieving information being shared between two entities.

Secure Communication refers to the scenario where the message or data shared between two parties can’t be accessed by an adversary. In Cryptography, an Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security.

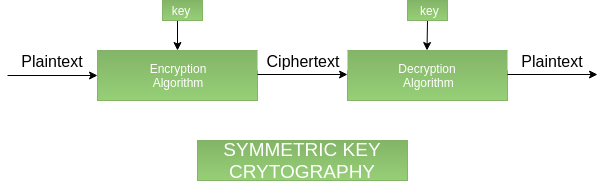
Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

1. **Confidentiality** refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.
2. **Data integrity** refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.
3. **Authentication** is the process of making sure that the piece of data being claimed by the user belongs to it.
4. **Non-repudiation** refers to ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

* **What is Symmetric and 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.



**Advantage:**

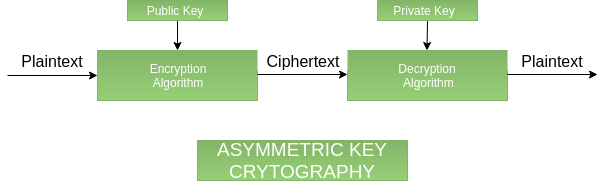
* Extremely Secure
* A system only which possesses the secret key can decrypt a message.

**Disadvantage:**

* Exchange of the key: It must be ensured that the key to encryption, will be exchanged via a secure channel (e.g. in person). However, in practice this can be really difficult
* The number of the keys that are required: For each pair of participants that wish to exchange encrypted messages, a new key is required.

**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 use 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.



**Advantage:**

* **Convenience:** It solves the problem of distributing the key for encryption. Everyone publishes their public keys and private keys are kept secret.
* Provides for message authentication
* **Detection of tampering:** The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit.

**Disadvantages**

* **Slow:** Public key encryption is slow compared to symmetric encryption.
* **Widespread security compromise is possible:** If an attacker determines a person's private key, his or her entire messages can be read.
* **Loss of private key may be irreparable:** The loss of a private key means that all received messages cannot be decrypted.

# References

<http://techrejects.blogspot.com>

<https://www.geeksforgeeks.org>

<https://itstillworks.com>