# Savitribai Phule Pune University

## Centre for Information and Network Security

*Course: Introduction to Cyber Security / Information Security*

## Module 1: Pre-requisites in Information and Network Security

## Chapter 4: Cryptography / Encryption

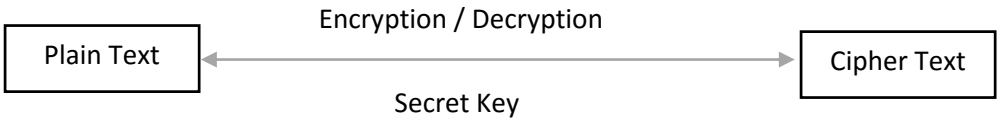
# Introduction to Cryptography

**Cryptography** comes from Greek *kryptos* means "hidden, secret"; and *gráphō*, "I write" respectively. It is the practice and study of hiding information. It is the science used to try to keep information secret and safe.

**Confidentiality** is one of the three core principles of information security. The aim of confidentiality is to ensure that information is hidden from people who are unauthorized to access it. The confidentiality principle mandates that information should solely be viewed by people with appropriate and correct privileges. It is achieved either by authorization / authentication i.e. providing right access and validating it at the time of accessing information or by cryptography, which involves **encryption** and **decryption** methods.

## Encryption

The process of converting a plain text message into a *cipher text* message i.e. non-readable format with the help of a *secret key* is called encryption and converting *cipher text* to plain text is called decryption.




### Types of Encryption

**Symmetric Encryption:** In this type of Encryption, both sender and receiver will use same key to Encrypt and Decrypt information. In the absence, of the secret key a third person will not be able to read the information.

E.g. Suman wants to send confidential information to Kirti. Both Suman and Kirti will have access to same Secret Key.

**Suman –Encrypt - *Secret Key* (Plaintext) = Ciphertext**

**Kirti – Decrypt - *Secret Key* (Ciphertext) = Plaintext**

**Assymetric Encryption:** In this type of Encryption, a pair of keys known as Public Key and Private Key is used. As name indicates, Public Key is shared and known to everyone where as Private Key is with the person himself.

Sender while Encrypting will use Receiver's Public Key and encrypt the message whereas Receiver will use his/her Private Key to decrypt the message and read it.

**Suman – Encrypt – [*Public Key* - Kirti] (Plaintext) = CipherText**

**Kirti – Decrypt - [*Private Key* – Kirti] (CipherText) = Plaintext**

It is apparent that secret key is very important in both the cases. So how do Suman and Kirti share Secret Key with each other?

**How to share Secret Key?**

For symmetric encryption, the private key needs to be shared between both the communicating parties and there are multiple mechanisms like *Diffie Hellman* and *RSA* to achieve that. These mechanisms use asymmetric key i.e. Public Key Infrastructure to share the *Secret Key*.

**Digital Certificate**

Now, you would think how to discover Public Key of others? The answer is *Digital Certificate*. A *Digital Certificate* contains information about its owner like name, Public Key, Validity of certificate etc. All the browsers recognize Digital Certificates and will download them automatically. They will extract the Public Key to decrypt the message before they show the content to the receiver. Hence, Digital Certificates is commonly used mechanism to share Public Key with each other.

Now, next problem is how to determine that the public key and the certificate belong to the user they claim to belong to. Public Key Infrastructure (PKI) is the answer to this problem.

## Public Key Infrastructure

A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.;

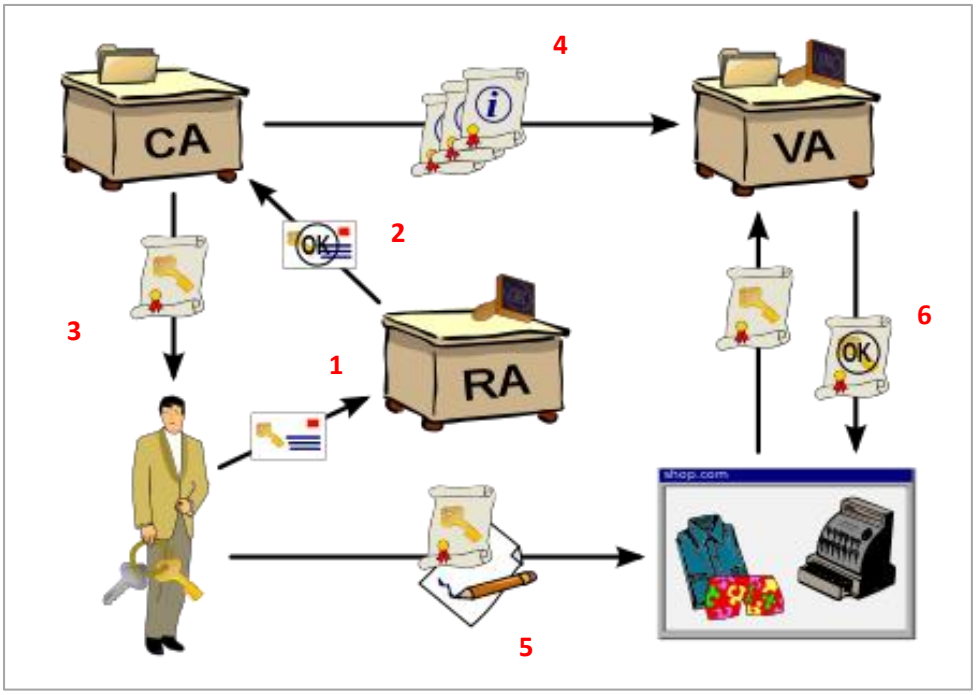
There are 3 key roles in PKI as below:

Certificate Authority (CA): A Certificate Authority issues digital certificates to person or organization which requests for it. In many cases, it will also play role of Verification Authority (VA) and verify the digital certificates.

E.g. Here are some of *Comodo*, *Symantec*, *GoDaddy*, *GlobalSign*, *DigiCert*

Registration Authority (RA): Registration Authority is responsible for accepting requests for digital certificates and authenticating the person or organization making the request. This authority will verify identity of person / organization and ensure that person / organization is what it is claiming.

Validation Authority (VA): A Validation Authority (VA) is an organization which verifies the digital certificates. It is often a 3rd party organization i.e. a separate organization than CA or RA.




Source: *https://en.wikipedia.org/wiki/Public_key_infrastructure*

1. User sends required information to Registration Authority.
2. Registration Authority verifies provided information & if found OK then registers user and shares OK report with Certificate Authority
3. Certificate Authority shares Public & Private Key with the user
4. Certificate Authority shared Public & Private Key with Validation Authority as well
5. While shopping, user will initiate transaction encrypted with his Private Key
6. Shopping website will share the Key information shared by user with Validation Authority. VA will validate it & if found to be correct then validate and authorize transaction.

## Applications of Cryptography

Cryptography is used in many of the common activities in our daily lives. Below are some of the activities where cryptography is used:

1. Authentication Services: Authentication is a process of confirming that the user is what he/she is claiming to be.

   E.g. User Name/ Passwords: Storing and transmitting passwords used for authentication of users.

2. **E-mail:** Email is one of the most common mode of communication in today's world. It is used to share confidential / important information between two individuals / organizations. Security issues with email programs surfaced early in their lifecycle. The vendors of email programs realized that they would have to figure out a way for everyone to be able to send *secure* email.

That is, e-mail in some sort of coded or encrypted form. It only made sense that this new feature be standardized, so they created *S/MIME* — Secure Multipurpose Internet Mail Extensions.

3. **E-Commerce** – E-commerce portals handle user information, bank /card information, passwords etc. hence it is necessary that this information is securely transmitted from user to the portal, from portal to 3rd party systems & back.

   Typically, these portal use Transport Layer Security (TLS)/ Secure Sockets Layer (SSL) protocols. The TLS/SSL protocols help prevent communications eavesdropping, tampering, and forgery. Web servers and browsers use the TLS handshake to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before transmitting data. The TLS handshake uses public key cryptography, such as RSA or DSS, to authenticate computers and to negotiate a shared secret. Of course, Digital Certificates are also used.

   TLS uses symmetric cryptography, such as DES or RC4, to encrypt the data, such as credit card numbers, prior to transmission over the network. Any message transmissions include a message authentication code (MAC) created with a hash function such as SHA or MD5 to prevent any communications tampering and forgery.