Unit – 04: Asymmetric-Key Cryptography

- RSA,
- Elliptic curve cryptography ECC,
- Digital certificates and PKI.

Questions to be discussed:

1. What is asymmetric cryptography? Discuss RSA in brief.
2. Discuss Elliptic curve cryptography in details.
3. What do you mean by Digital certificates and PKI.

CTH EDUCATION

What is cryptography?

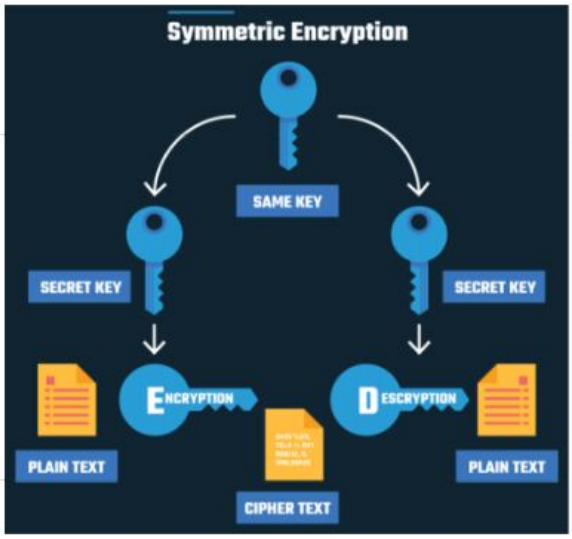
- Cryptography is technique of securing information.
- It is a technique of communications through use of codes.
- So the only intended person can understand the message and process it.

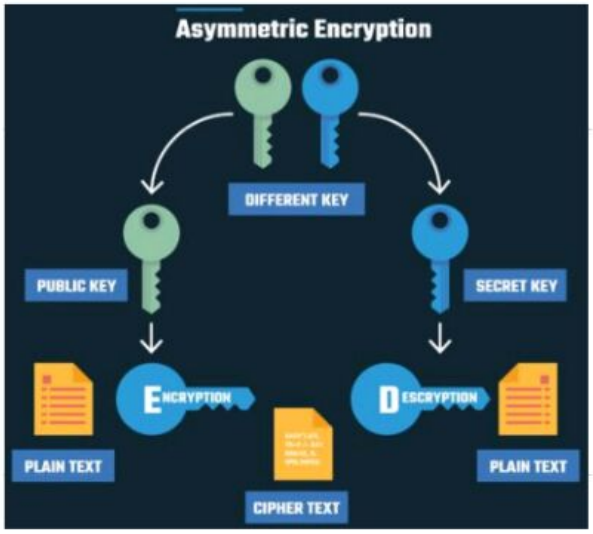
Examples:

- ➢ End-to-end encryption in WhatsApp.
- ➢ Digital signatures are the next real-time application of cryptography.

Symmetric and asymmetric key:

- Symmetric encryption involves using a single key to encrypt and decrypt data, while asymmetric encryption uses two keys - one public and one private - to encrypt and decrypt data.
- Each type of encryption has its own strengths and weaknesses, and the choice between the two depends on the specific needs of the user.





What is asymmetric cryptography?

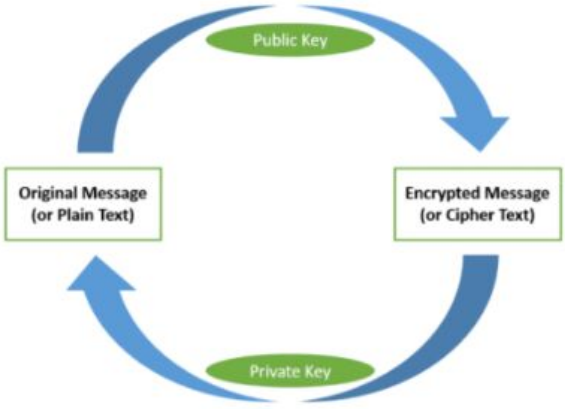
- Asymmetric cryptography is also known as public-key cryptography.
- It is a process that uses a pair of related keys - one public key and one private key - to encrypt and decrypt a message to protect it from unauthorized access.
- A public key can be used by any person to encrypt a message so that it can only be decrypted by the intended recipient with their private key.
- A private key is also known as a secret key - is shared only with key's initiator.
- Asymmetric cryptography is used to authenticate data using digital signatures.
- A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.
- It is the digital equivalent of a handwritten signature or stamped seal.

Types of Cryptography Algorithm:

- Cryptographic algorithms are primarily of two types, and you can use them for critical tasks, such as authentication, data encryption, and digital signatures.
  1. RSA(Rivest, Shamir, and Adleman)
  2. DES(Data Encryption Standard)

What is the RSA algorithm?

- The RSA algorithm is an asymmetric cryptography algorithm.
- It is the most secure encryption method based on the block cipher principle.
- Rivest, Shamir, and Adleman invented it in 1978, hence the name RSA algorithm.
- It converts plain text to ciphertext at the receiver end and vice versa.
- If we use User A's public key for encryption, we must use the same user's private key for decryption.
- You may wonder what I mean by saying the RSA algorithm is asymmetric.
- It means it works on two different keys: The Public Key and the Private Key.
- The Public Key is distributed to everyone while the Private Key is kept private.
- The RSA algorithm is based on how difficult it is to factorize a large integer.

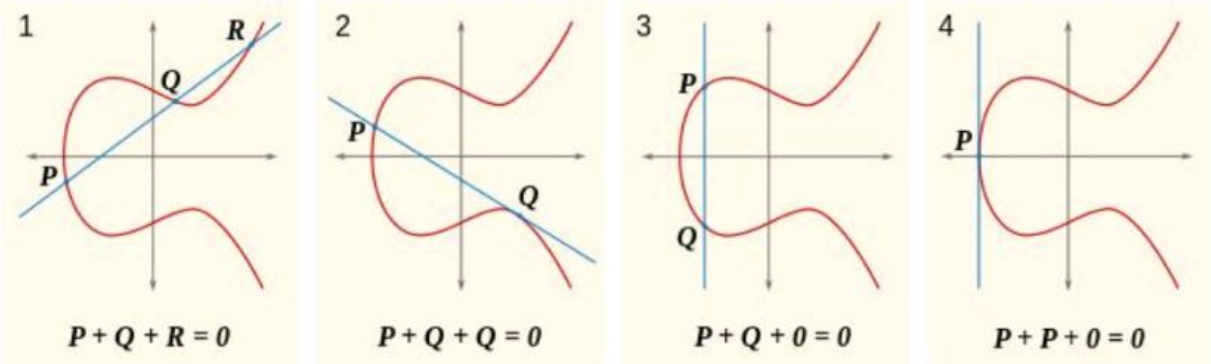


Difference Between AES and RSA Encryption:

AES	RSA
Symmetric key encryption	Asymmetric encryption
128, 192, or 256 bits	1024, 2048, or 4096 bits (common)
Fast and efficient for bulk data	Slower, not suited for large data
Securing file storage AES is preferable due to its faster encryption and decryption speeds	Secure communications ensuring a secure channel for data transmission between clients and servers.
Secure file storage and communication	Secure email and digital certificates

Elliptic Curve Cryptography(ECC):

- ECC stands for Elliptic Curve Cryptography.
- This method was introduced in 1985 by Neal Koblitz and Victor S. Miller.
- Its high-security makes it the ideal standard for protecting sensitive mobiles and apps.
- ECC uses a fairly difficult mathematical operation based on elliptic curves on a finite field.
- With ECC you have a curve, defined by a math function, a starting point (A), and an ending point (Z) in the curve.
- The key is that to get to Z, you have done a series of "hops", or multiplications that resulted in Z.
- This amount of hops is the private key.



Digital certificates and PKI:

- Digital certificates facilitate secure electronic communication and exchange data between people, systems, and online devices.
- They are issued by Certificate Authorities (CAs) and perform two primary functions:
  1. Verifying the identity of the sender/receiver of an electronic message
  2. Providing the means to encrypt/decrypt messages between sender and receiver.
- There are three basic types of digital signature certificates:
  1. Individual digital signature certificates (signing certificates).
  2. Server certificates.
  3. Encryption certificates.

Individual digital signature certificates (signing certificates):

- These certificates are used to identify a person and include personal information.
- They can be used to sign electronic documents and emails to implement access control mechanisms for sensitive or valuable information.

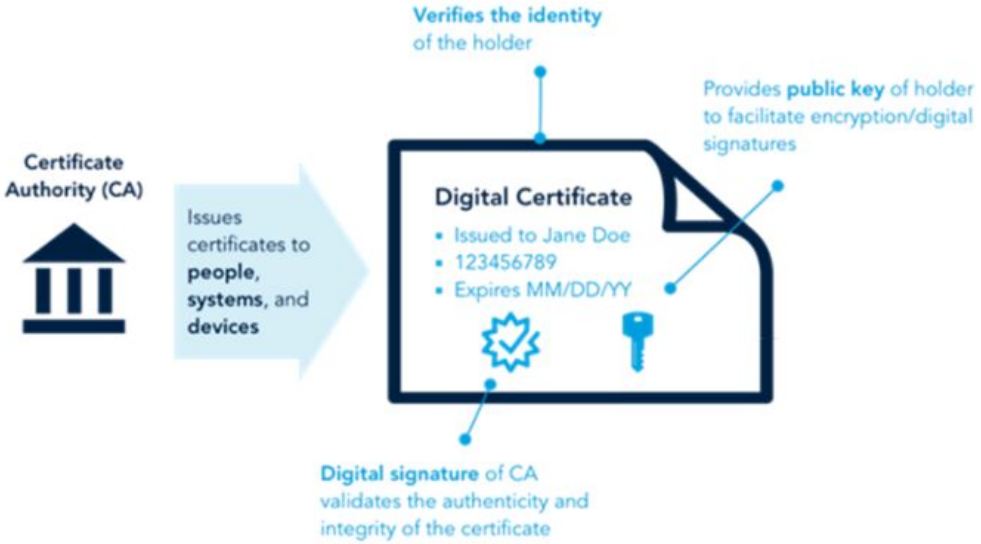
Server certificates:

- These certificates identify a server (computer) and contain the host name or IP address.
- They are used for one- or two-layer SSL to ensure secure communication of data over a network.

Encryption certificates:

- These certificates are used to encrypt a message using the public key of the recipient to ensure data confidentiality during transmission. Different signatures for encryption and digital signatures are available from different CAs. (adapted from *Government of India 2010*)

Figure 13. Digital certificates



PKI:

- PKI stands for public-key infrastructure.
- A system including policies, institutions, and technologies—that manages the distribution, authentication, and revocation of digital certificates is called public-key infrastructure (PKI).
- Because digital certificates are standard in data exchange and security protocols for digital ID systems a country's PKI is landscape is a common building block for many ID systems.
- For example, when a smartcard or SIM card that uses PKI for authentication and digital signatures is personalized, it is issued with a private key and digital certificate signed by a CA that attests to the authenticity of the credential and provides the public-key necessary for other devices (e.g., card readers, servers, etc.) to verify the authenticity and integrity of the card.