SNS COLLEGE OF TECHNOLOGY

Coimbatore-35

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade

Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

19ECT301- COMMUNICATION NETWORKS

III YEAR/ V SEMESTER

UNIT 4 –NETWORK & DATA SECURITY

TOPIC 3 – CRYPTOGRAPHY TECHNIQUES

- Cryptography is the study of securing communications from outside observers. **Encryption Algorithm** take the original message, or **Plain Text**, and converts it into **ciphertext,** which is not understandable. The key allows the user to **Decrypt** the message, thus ensuring on they can read the message.

- The strength of the randomness of an **Encryption** is also studied, which makes it harder for anyone to guess the key or input of the algorithm. Cryptography is how we can achieve more secure and robust connections to elevate our privacy.

- Advancements in cryptography makes it harder to break encryptions so that encrypted files, folders, or network connections are only accessible to authorized users.

Cryptography focuses on four different objectives:

Confidentiality: Confidentiality ensures that only the intended recipient can decrypt the message and read its contents.

Non-repudiation: Non-repudiation means the sender of the message cannot backtrack in the future and deny their reasons for sending or creating the message.

Integrity: Integrity focuses on the ability to be certain that the information contained within the message cannot be modified while in storage or transit.

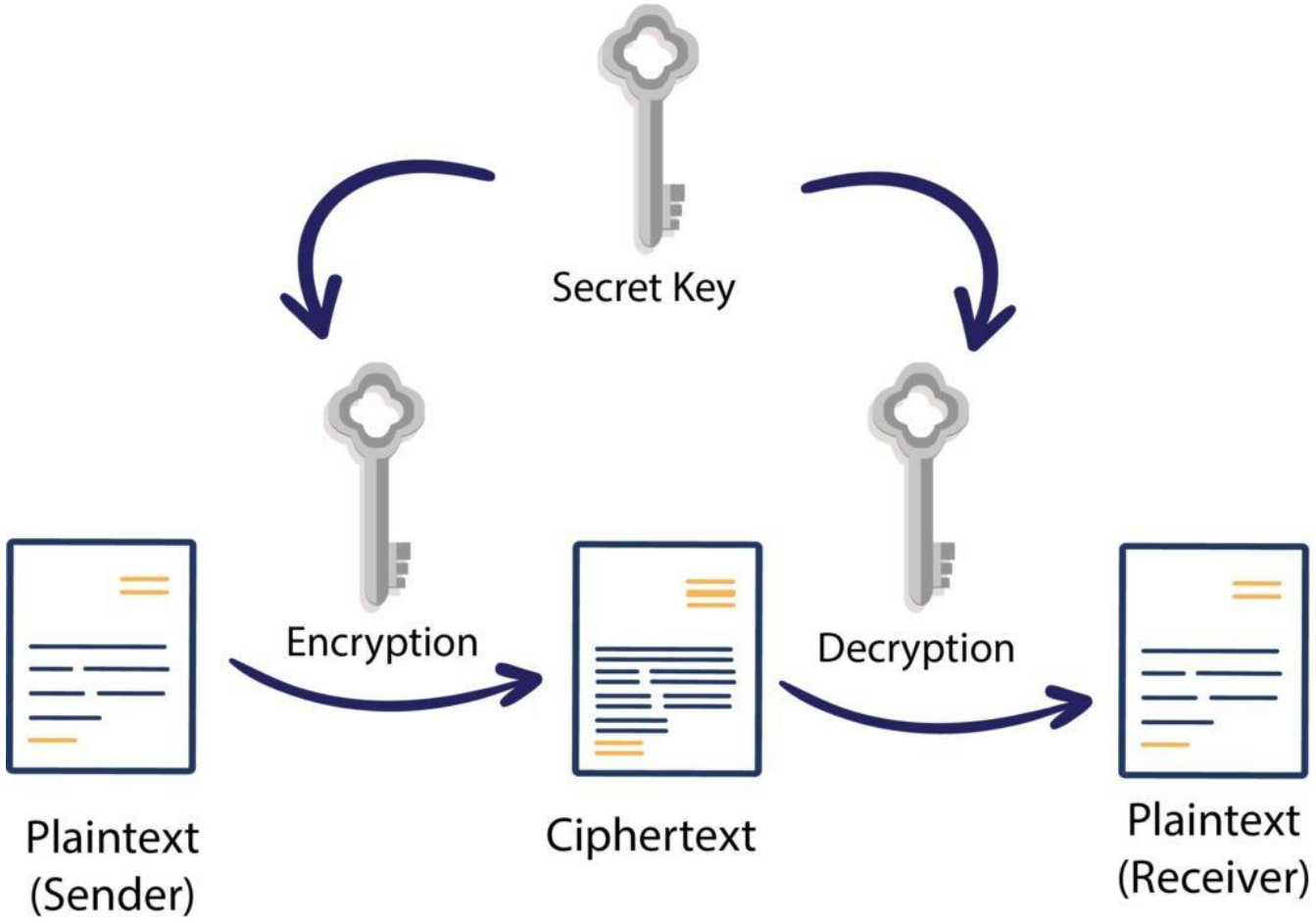
Authenticity: Authenticity ensures the sender and recipient can verify each other’s identities and the destination of the message.

History of Cryptography

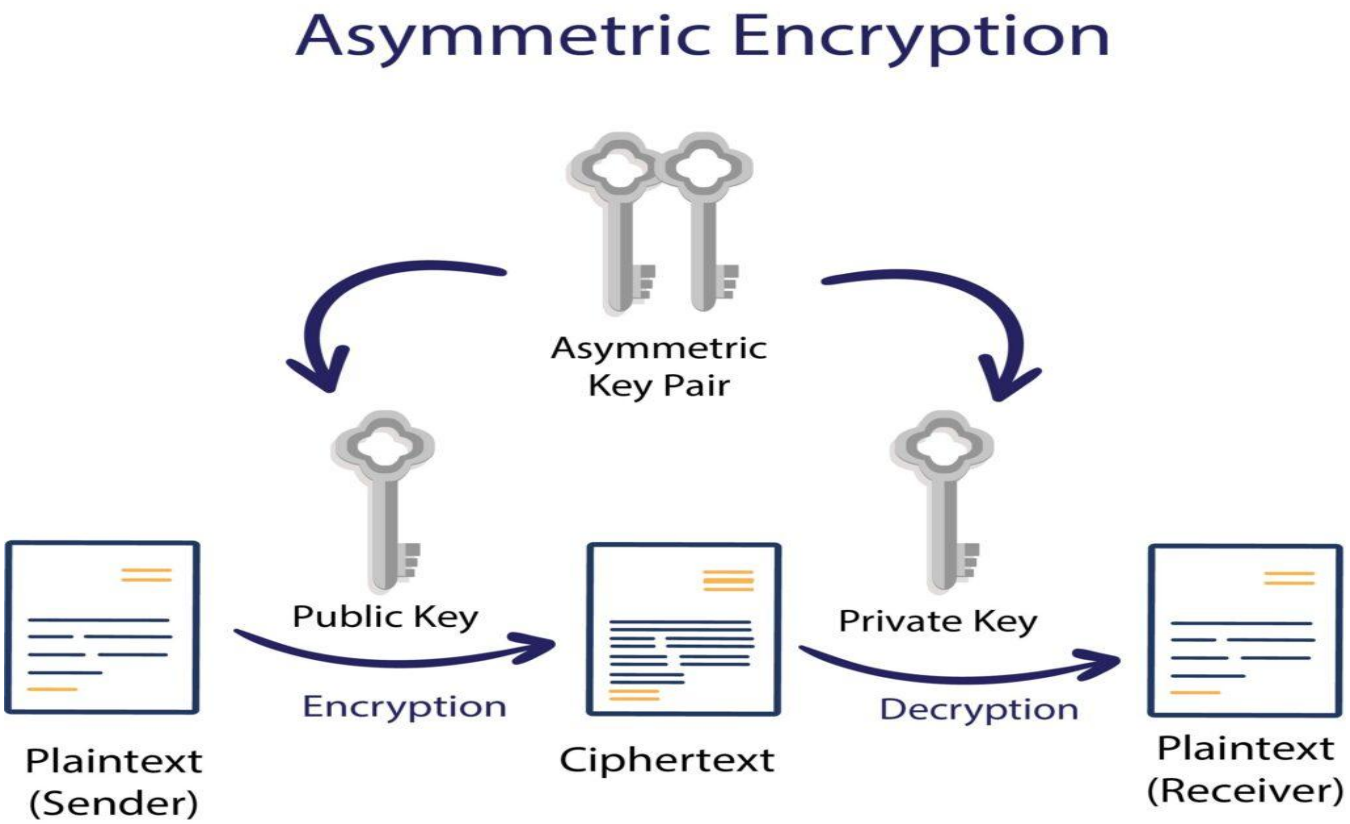
Cryptography began with ciphers, the first of which was the Caesar Cipher. Ciphers were a lot easier to unravel compared to modern cryptographic algorithms, but they both used **keys and plaintext.** Though simple, ciphers from the past were the earliest forms of encryption. Today's algorithms and cryptosystems are much more advanced.

They use multiple rounds of ciphers and encrypting the ciphertext of messages to ensure the most secure transit and storage of data. There are also methods of cryptography used now that are irreversible, maintaining the security of the message forever.

Symmetric Encryption



Public Key Cryptography, or asymmetric cryptography, uses two keys to encrypt data. One is used for encryption, while the other key can decrypts the message. Unlike symmetric cryptography, if one key is used to encrypt, that same key cannot decrypt the message, rather the other key shall be used.



One key is kept private, and is called the “private key”, while the other is shared publicly and can be used by anyone, hence it is known as the “public key”. The mathematical relation of the keys is such that the private key cannot be derived from the public key, but the public key can be derived from the private. The private key should not be distributed and should remain with the owner only.