SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

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 COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity Including BCT)

COURSE NAME : Fundamentals Of Cryptography

II YEAR / III SEMESTER

Unit III-

Topic : key management

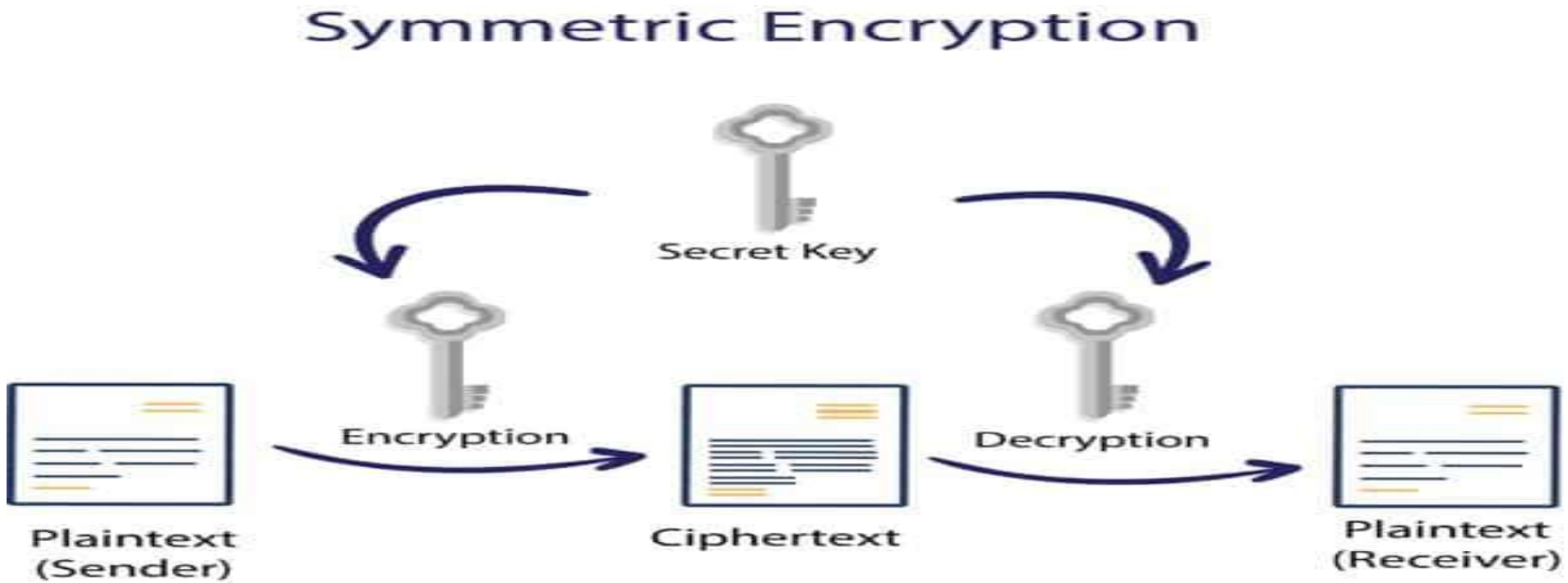
- Cryptographic keys are a vital part of any security system. They do everything from data **encryption** and **decryption** to user authentication.
- Key Management is the process of putting certain standards in place to ensure the security of cryptographic keys in an organization.
- Key Management deal with the creation, exchange, storage, deletion, and refreshing of keys. They also deal with the members access of the keys.
- The compromise of any cryptographic key could lead to the collapse of an organization's entire security infrastructure, allowing the attacker to decrypt sensitive data, authenticate themselves as privileged users, or give themselves access to other sources of classified information.

Why is Key Management Important

- Key management forms the basis of all data security.
- Data is encrypted and decrypted via the use of encryption keys, which means the loss or compromise of any encryption key would invalidate the data security measures put into place.
- Keys also ensure the safe transmission of data across an Internet connection. With authentication methods, like **code signing,** attackers could pretend to be a trusted service like Microsoft, while giving victim's computers malware, if they steal a poorly protected key

Types of Keys

- There are two types of cryptographic keys, **symmetric** and **asymmetric** keys.
- Symmetric keys deal with **data-at-rest**, which is data stored in a static location, such as a database.
- Symmetric key encryption uses the same key for both encryption and decryption.
- Using data in a database as an example, while the data is stored in the database, it is encrypted with the symmetric key.
- Once an authorized user attempts to access the data, the information is decrypted with the same symmetric key and made accessible to the user.



- The other type of cryptographic key is an asymmetric key.
- Encryption using asymmetric keys is a little more complicated than symmetric key encryption.
- Instead of using the same key for both encryption and decryption, two separate keys called a public and private key, are used for the encryption and decryption of data.
- These keys are created as a pair, so that they relate to each other.
- The public key of a pair of asymmetric keys is mainly used to encrypt data.
- This key can be shared with anyone since it encrypts, not decrypts, data.
- The private key is used for the decryption of data encrypted by its public key counterpart, so it must stay secure.
- Asymmetric keys focus on encrypting **data-in-motion**
- When transporting sensitive data, most encryption processes use both symmetric and asymmetric keys to encrypt data.

•The data is first encrypted-at-rest by a symmetric encryption key.

•The symmetric key is now encrypted by the public key of the person who the data is being sent to. That encrypted symmetric key and the **ciphertext** are sent to the recipient of the data.
•Once the ciphertext and key reach the recipient, the symmetric key is decrypted by that user's private key, and the ciphertext is decrypted.

How Key Management Works

•Key management follows a lifecycle of operations which are needed to ensure the key is created, stored, used, and rotated securely. Most cryptographic keys follow a lifecycle which involves key

1. Generation-**The generation of a key is the first step in ensuring that key is secure**
2. Distribution-**ensuring the safe distribution of the keys**
3. Use
4. Storage
5. Rotation
6. Backup/Recovery
7. Revocation
8. Destruction