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 I

Topic :Conventional Encryption Model

Conventional Encryption Model

Conventional encryption is a cryptographic system that uses the same key used by the sender to encrypt the message and by the receiver to decrypt the message.

1.Plain text

It is the original data that is given to the algorithm as an input.

2.Encryption algorithm

This encryption algorithm performs various transformations on plain text to convert it into ciphertext.

3.Secret key

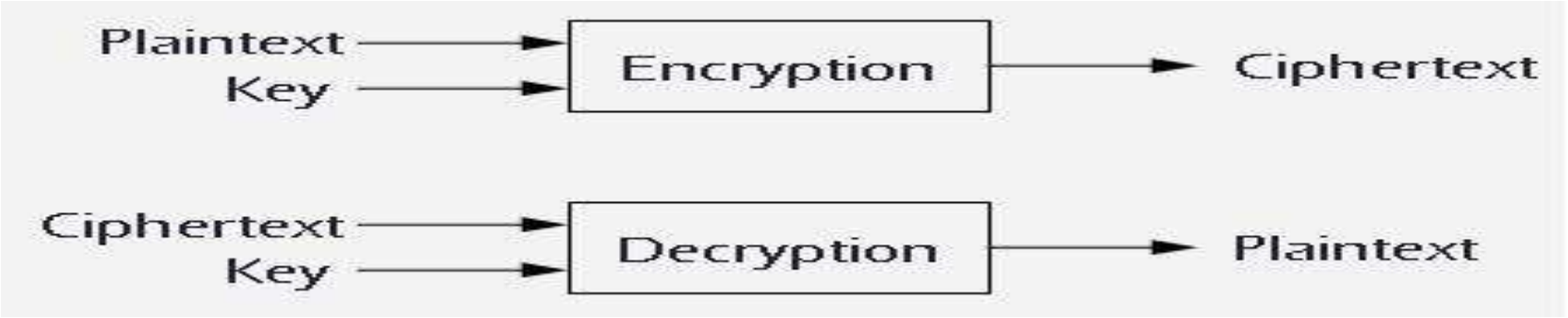
The secret key is also an input to the algorithm. The encryption algorithm will produce different outputs based on the keys used at that time.

4.Ciphertext

It contains encrypted information because it contains a form of original plaintext that is unreadable by a human or computer without proper cipher to decrypt it. It is output from the algorithm.

5.Decryption Algorithm

This is used to run encryption algorithms in reverse. Ciphertext and Secret key is input here and it produces plain text as output.



Advantages of Conventional Encryption :

1.Simple –
This type of encryption is easy to carry out.

2.Uses fewer computer resources –
Conventional encryption does not require a lot of computer resources when compared to public-key encryption.

3.Fast –
Conventional encryption is much faster than asymmetric key encryption.

Disadvantages of Conventional Encryption Model:

1.Origin and authenticity of the message cannot be guaranteed, since both sender and receiver use the same key, messages cannot be verified to have come from a particular user.
2.It isn’t much secured when compared to public-key encryption.
3.If the receiver lost the key, he/she cant decrypt the message and thus making the whole process useless.
4.This scheme does not scale well to a large number of users because both the sender and the receiver have to agree on a secret key before transmission.