JAYOTI VIDYAPEETH WOMEN'S UNIVERSITY, JAIPUR
Government of Rajasthan established
Through ACT No. 17 of 2008 as per UGC ACT 1956
NAAC Accredited University

Faculty of Education and methodology

Department of Science and Technology

Faculty Name- Jv'n Narendra Kumar Chahar (Assistant Professor)

Program- B.Tech 8thSemester

Course Name – Cryptography and Network Security

Session no.: 07

Session Name- Conventional Encryption

Academic Day starts with –

- Greeting with saying **'Namaste'** by joining Hands together following by 2-3 Minutes Happy session, Celebrating birthday of any student of respective class and **National Anthem**.

Lecture starts with- quotations' answer writing

Review of previous Session **– Symmetric and public key algorithms**

Topic to be discussed today- Today We will discuss about **Conventional Encryption**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

Introduction & Brief Discussion about the Topic **– Conventional Encryption**

Conventional Encryption

- Referred conventional / private-key / single-key
- Sender and recipient share a common key

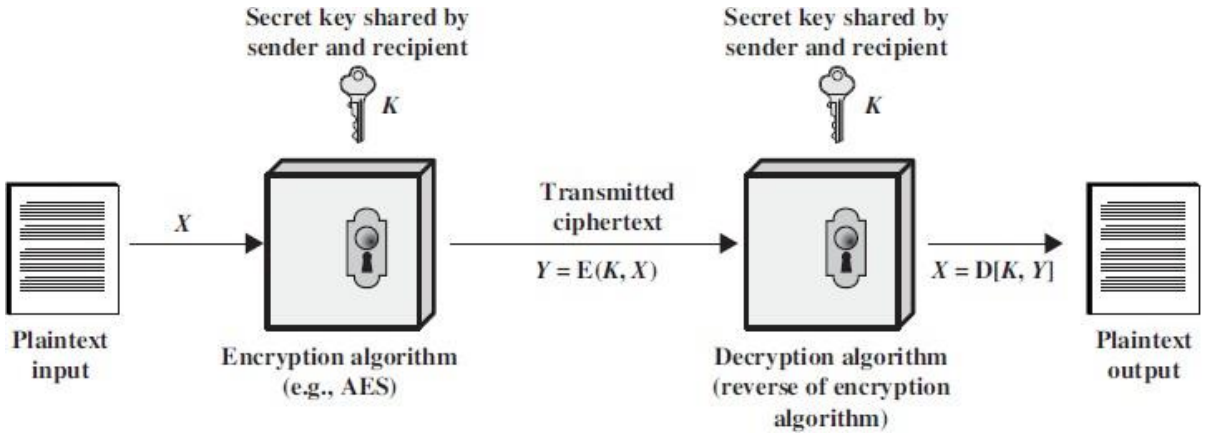
All classical encryption algorithms are private-key was only type prior to invention of public-key in 1970"

Some basic terminologies used:

- **plaintext** - the original message
- **cipher text** - the coded message
- **Cipher** - algorithm for transforming plaintext to cipher text
- **Key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to cipher text
- **decipher (decrypt)** - recovering cipher text from plaintext
- **Cryptography** - study of encryption principles/methods

Cryptanalysis (code breaking) - the study of principles/ methods of deciphering cipher text without knowing key

- **Cryptology** - the field of both cryptography and cryptanalysis



Here the original message, referred to as plaintext, is converted into apparently random nonsense, referred to as cipher text. The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext. Changing the key changes, the output of the algorithm. Once the cipher text is produced, it may be transmitted. Upon reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption. The security depends on several factors. First, the encryption algorithm must be powerful enough that it is impractical to decrypt a message on the basis of cipher text alone. Beyond that, the security depends on the secrecy of the key, not the secrecy of the algorithm.

Two requirements for secure use of symmetric encryption:

A strong encryption algorithm

A secret key known only to sender / receiver

$Y = E_{K(X)}$

$X = D_{K(Y)}$

assume encryption algorithm is known

implies a secure channel to distribute key

A source produces a message in plaintext, X = [X1, X2… XM] where M are the number of letters in the message. A key of the form K = [K1, K2… KJ] is generated. If the key is generated at the source, then it must be provided to the destination by means of some secure channel.

With the message X and the encryption key K as input, the encryption algorithm forms the cipher text Y = [Y1, Y2, YN]. This can be expressed as

$Y = E_{K(X)}$

The intended receiver, in possession of the key, is able to invert the transformation:

$X = D_{K(Y)}$

An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both. It is assumed that the opponent knows the encryption and decryption algorithms.

If the opponent is interested in only this particular message, then the focus of effort is to recover X by generating a plaintext estimate. Often if the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover K by generating an estimate.

Reference-

1. **Book:** William Stallings, "Cryptography & Network Security", Pearson Education, 4th Edition 2006.

QUESTIONS: -

Q1. List the basic terminology used in cryptography.

Q2. Explain symmetric key encryption with steps.

Q3. What are the requirements for secure use of symmetric encryption?

Next, we will discuss about Classical Encryption Techniques.

- Academic Day ends with-
  National song 'Vande Mataram'