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 : **Message Authentication Functions**

Message Authentication Functions:

All message authentication and digital signature mechanisms are based on two functionality levels:

•**Lower level:** At this level, there is a need for a function that produces an authenticator, which is the value that will further help in the authentication of a message.

•**Higher-level:** The lower level function is used here in order to help receivers verify the authenticity of messages.

These message authentication functions are divided into three classes:

•**Message encryption:** While sending data over the internet, there is always a risk of a Man in the middle(MITM) attack.

•A possible solution for this is to use message encryption. In message encryption, the data is first converted to a ciphertext and then sent any further.

•Message encryption can be done in two ways:

These message authentication functions are divided into three classes:

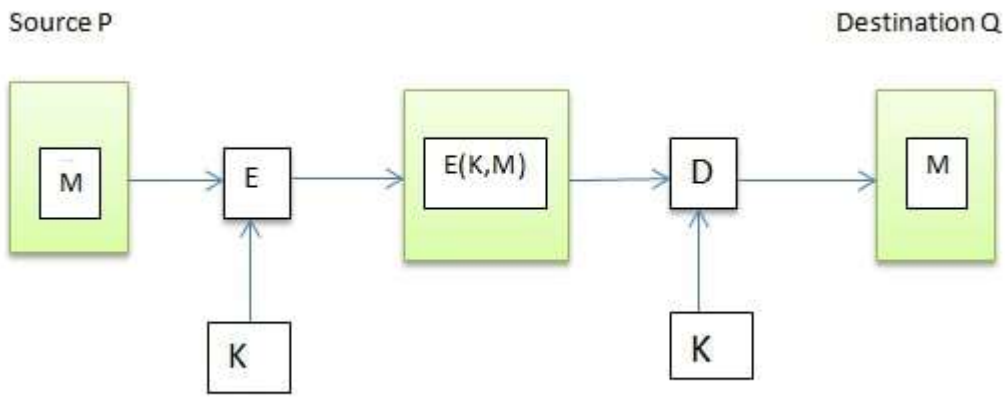
•Message encryption:

•While sending data over the internet, there is always a risk of a Man in the middle(MITM) attack.

• A possible solution for this is to use message encryption.

•In message encryption, the data is first converted to a ciphertext and then sent any further. Message encryption can be done in two ways:

Symmetric Encryption:



•**Symmetric Encryption:**

•Say we have to send the message M from a source P to destination Q. This message M can be encrypted using a secret key K that both P and Q share. Without this key K, no other person can get the plain text from the ciphertext. This maintains confidentiality. Further, Q can be sure that P has sent the message. This is because other than Q, P is the only party who possesses the key K and thus the ciphertext can be decrypted only by Q and no one else. This maintains authenticity. At a very basic level, symmetric encryption looks like this:

•**Public key Encryption:**

Public key encryption is not as advanced as symmetric encryption as it provides confidentiality but not authentication.

To provide both authentication and confidentiality, the private key is used.

•**Message authentication code (MAC):**

A message authentication code is a security code that the user of a computer has to type in order to access any account or portal.

•These codes are recognized by the system so that it can grant access to the right user. These codes help in maintaining information integrity.

• It also confirms the authenticity of the message.

Hash function:

•A hash function is nothing but a mathematical function that can convert a numeric value into another numeric value that is compressed.

•The input to this hash function can be of any length but the output is always of fixed length.

•The values that a hash function returns are called the message digest or hash values.