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 : Authentication requirement

- Data is prone to various attacks.
- One of these attacks includes message authentication.
- This threat arises when the user does not have any information about the originator of the message.
- Message authentication can be achieved using cryptographic methods which further make use of keys.

Authentication Requirements:

•**Revelation:** It means releasing the content of the message to someone who does not have an appropriate cryptographic key.

•**Analysis of Traffic:** Determination of the pattern of traffic through the duration of connection and frequency of connections between different parties.

•**Deception:** Adding out of context messages from a fraudulent source into a communication network. This will lead to mistrust between the parties communicating and may also cause loss of critical data.

•**Modification in the Content:** Changing the content of a message. This includes inserting new information or deleting/changing the existing one.

•**Modification in the sequence:** Changing the order of messages between parties. This includes insertion, deletion, and reordering of messages.

•**Modification in the Timings:** This includes replay and delay of messages sent between different parties. This way session tracking is also disrupted.

•**Source Refusal:** When the source denies being the originator of a message.

•**Destination refusal:** When the receiver of the message denies the reception.

Message Authentication:

•To deal with the analysis of traffic and deception issues, message authentication is helpful. Here, the receiver can be sure of the real sender and his identity. To do this, these methods can be incorporated:

- Parties should share secret codes that can be used at the time of identity authentication.
- Digital signatures are helpful in the authentication.
- A third party can be relied upon for verifying the authenticity of parties.

Digital Signatures:

•Digital signatures provide help against a majority of these issues.
•With the help of digital signatures, content, sequence, and timing of the messages can be easily monitored.
•Moreover, it also prevents denial of message transmission by the source.

Combination of protocols with Digital Signatures:

•This is needed to deal with the denial of messages received. Here, the use of digital signature is not sufficient and it additionally needs protocols to support its monitoring.