



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-

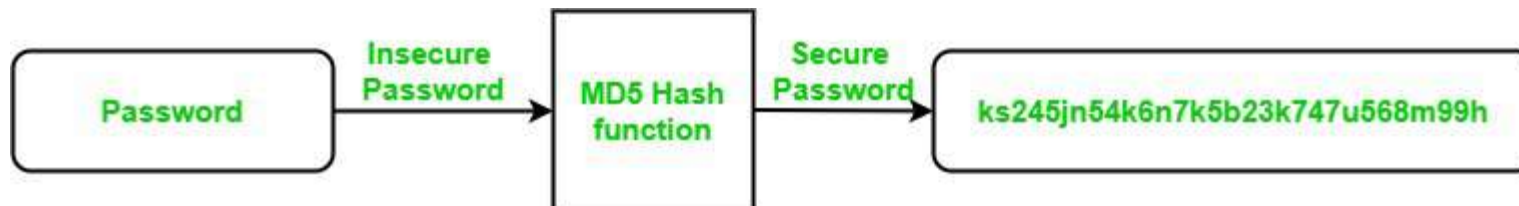
Topic : MD5 Message digest algorithm



- **MD5** is a cryptographic hash function algorithm that takes the message as input of any length and changes it into a fixed-length message of 16 bytes.
- MD5 algorithm stands for the **message-digest algorithm**. MD5 was developed as an improvement of MD4, with advanced security purposes.
- The output of MD5 (Digest size) is always **128 bits**. **MD5** was developed in 1991 by **Ronald Rivest**.

Use Of MD5 Algorithm:

- It is used for file authentication.
- In a web application, it is used for security purposes. e.g. Secure password of users etc.
- Using this algorithm, We can store our password in 128 bits format





Application Of MD5 Algorithm:

- We use message digest to verify the integrity of files/ authenticates files.
- MD5 was used for data security and encryption.
- It is used to Digest the message of any size and also used for Password verification.
- For Game Boards and Graphics.

Advantages of MD5 Algorithm:

- MD5 is faster and simple to understand.
- MD5 algorithm generates a strong password in 16 bytes format. All developers like web developers etc use the MD5 algorithm to secure the password of users.
- To integrate the MD5 algorithm, relatively low memory is necessary.
- It is very easy and faster to generate a digest message of the original message.

Disadvantages of MD5 Algorithm:

- MD5 generates the same hash function for different inputs.
- MD5 provides poor security over [SHA1](#).
- MD5 has been considered an insecure algorithm. So now we are using SHA256 instead of MD5
- MD5 is neither a symmetric nor asymmetric algorithm.