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

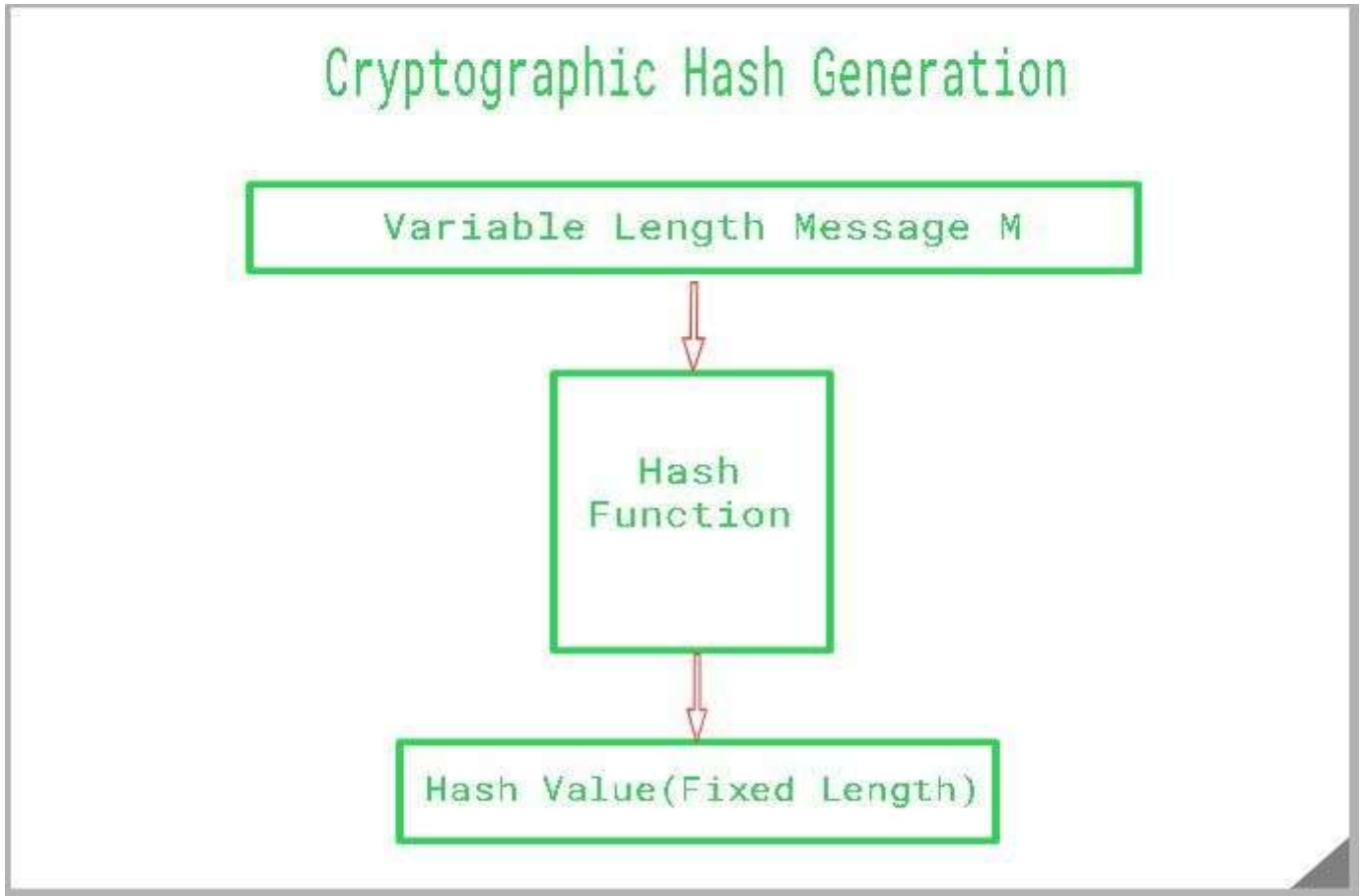
II YEAR / III SEMESTER

Unit III-

Topic : Hash Functions

Cryptographic Hash is a Hash function that takes random size input and yields a fixed-size output.

- It is easy to calculate but challenging to retrieve the original data.
- It is strong and difficult to duplicate the same hash with unique inputs and is a one-way function so revert is not possible.
- Hashing is also known by different names such as Digest, Message Digest, Checksum, etc.



Properties Of Cryptography Hash Function

The ideal cryptographic hash function has the following main properties:
1.Deterministic: This means that the same message always results in the same hash.
2.Quick: It is quick to compute the hash value for any given message.
3.Avalanche Effect: This means that every minor change in the message results in a major change in the hash value.
4.One-Way Function: You cannot reverse the cryptographic hash function to get to the data.
5.Collision Resistance: It is infeasible to find two different messages that produce the same hash value.
6.Pre-Image Resistance: The hash value shouldn't be predictable from the given string and vice versa.
7.Second Pre-Image Resistance: Given an input, it should be difficult to find another input that has the same hash value.

Hash Uses

- Digital signatures.
- Digital fingerprints.
- Logging sensitive data.
- Saving passwords.
- Blockchain.

How to create a Cryptographic Hash

•Create a random salt value using SecureRandom class, SecureRandom class generates strong random values. The engineNextBytes(byte[] bytes) method is used to generate a user-specified number of random bytes.

•Convert two sets of bytes into one using ByteArrayOutputStream class and create it to ByteArray.

•Create an instance of a message-digest passing SHA2_ALGORITHM which returns a hash of the given input value.

•UUID is used to genmessage-digested to a string and passed as input.

•The returned object can be converted to a hex binary format using DatatypeConverter.