SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
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

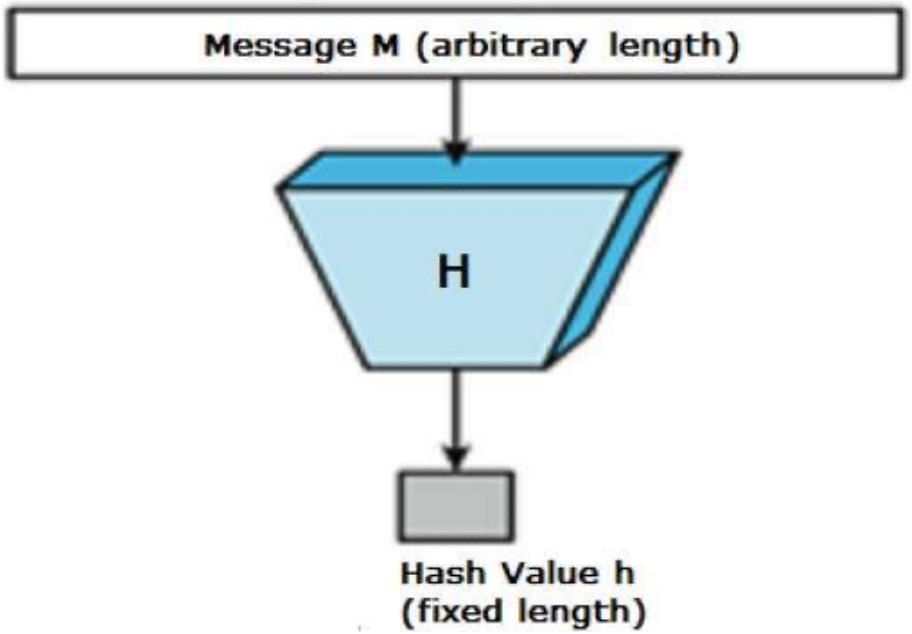
DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

19ITB302-Cryptography and Network Security

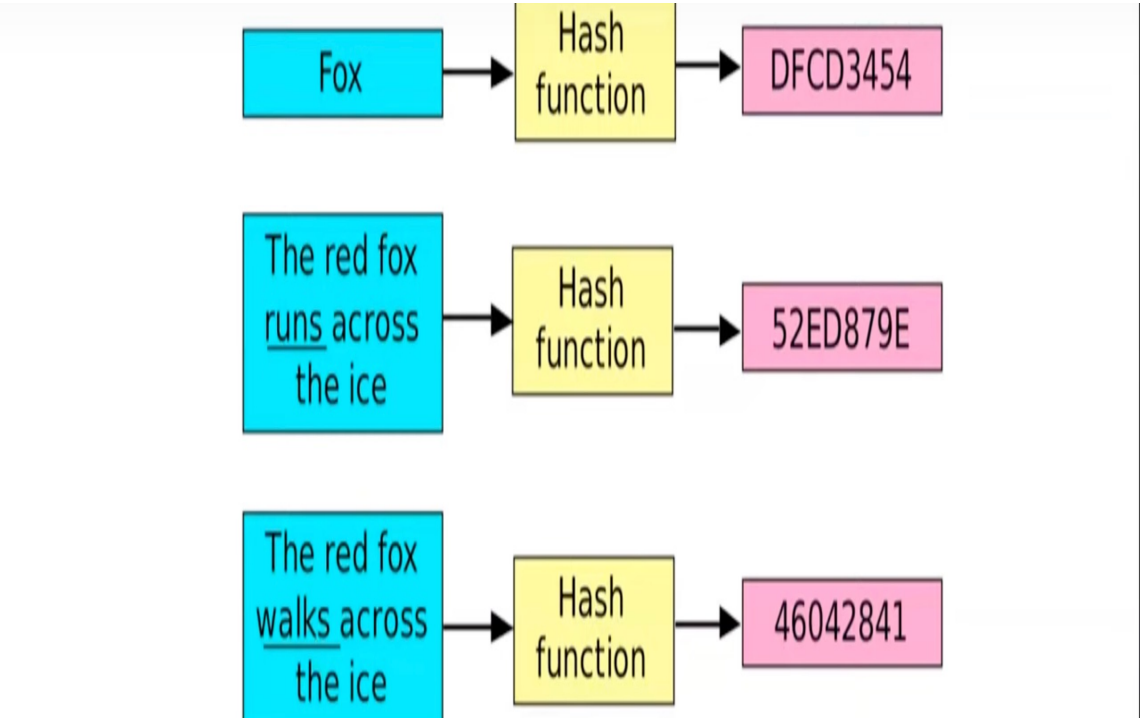
UNIT-3 HASH FUNCTION AND DIGITAL SIGNATURE

Cryptographic Hash Functions

- A **hash function** H accepts a variable-length block of data **M** as input and produces a fixed-size hash value **h = H(M)**
- Values returned by a hash function are called **message digest** or simply **hash values**.
- A change to any bit or bits in M results, with high probability, in a change to the hash code.
- The kind of hash function needed for security applications is referred to as a **cryptographic hash function.**



- A cryptographic hash function is an algorithm for which it is computationally infeasible to invert
- Because of these characteristics, hash functions are often used to determine whether or not data has changed.
- A small change in the input data will have the whole hash function output to be changed.



Properties of Hash function

- **Compression**:Output of the hash function is much smaller than the size of the input
- **Pre image resistance**: Its difficult to find the input from given hash function output, h=H(m) if h is given, it is infeasible to find m
- **Collision Resistance**: It is difficult to find m1 and m2 such that hash value H(m1)=H(m2)

Characteristics of Hash function

- It is quick to calculate hash value(h) for any given message
- Hash Function can be applied to variable length of data block
- A small Change in a message should change the hash value
- Hash function has one way property
- Hash function uses all the input data