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

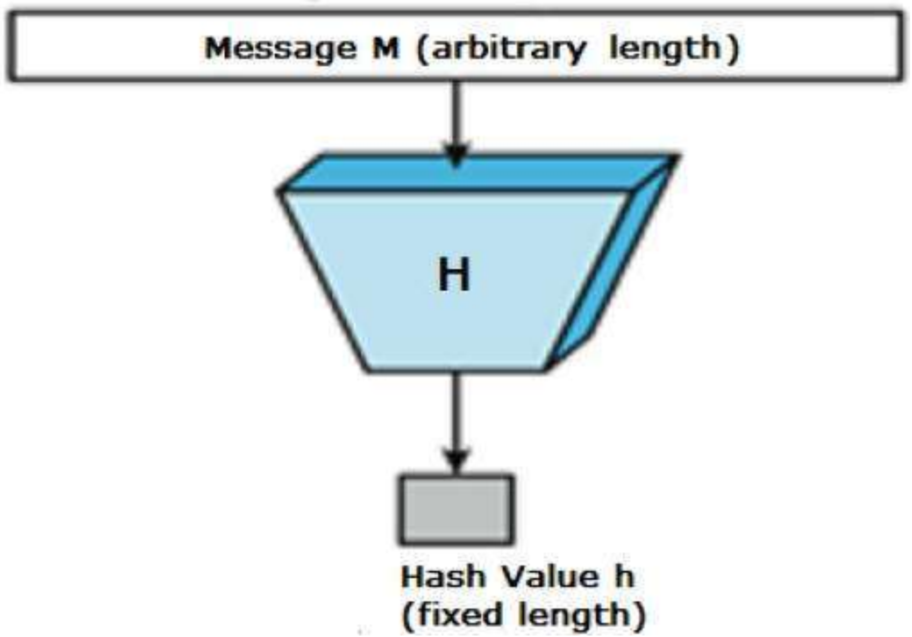
DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

19ITB302-Cryptography and Network Security

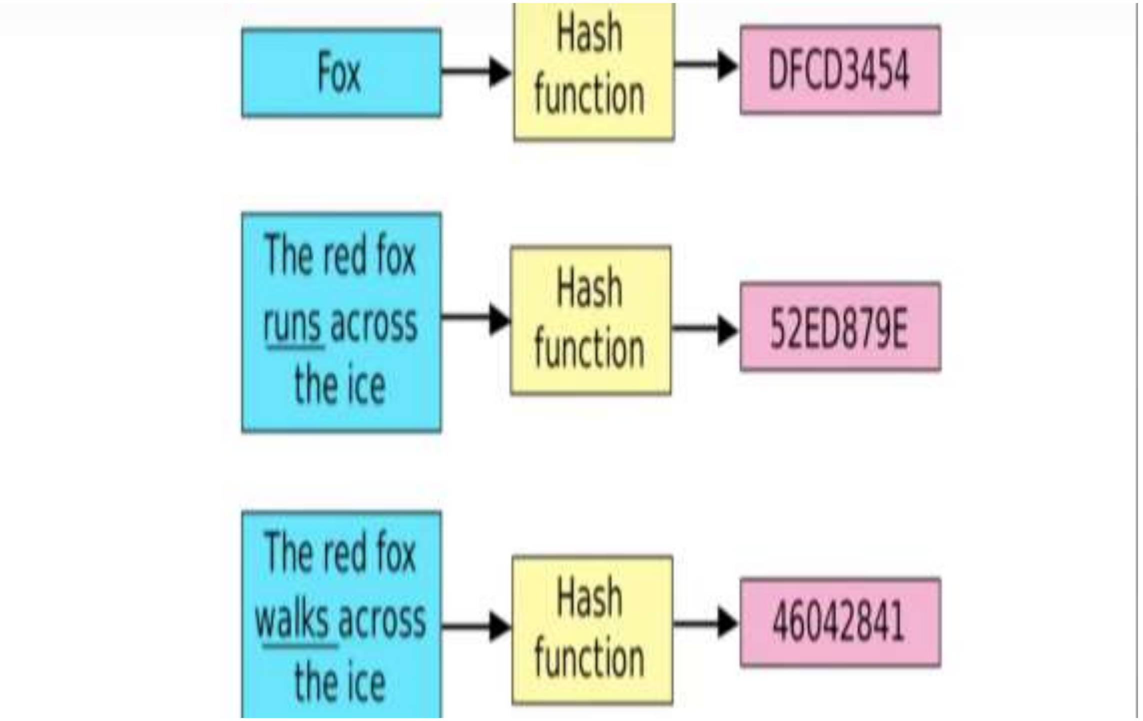
UNIT-3 HASH FUNCTION AND DIGITAL SIGNATURE

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

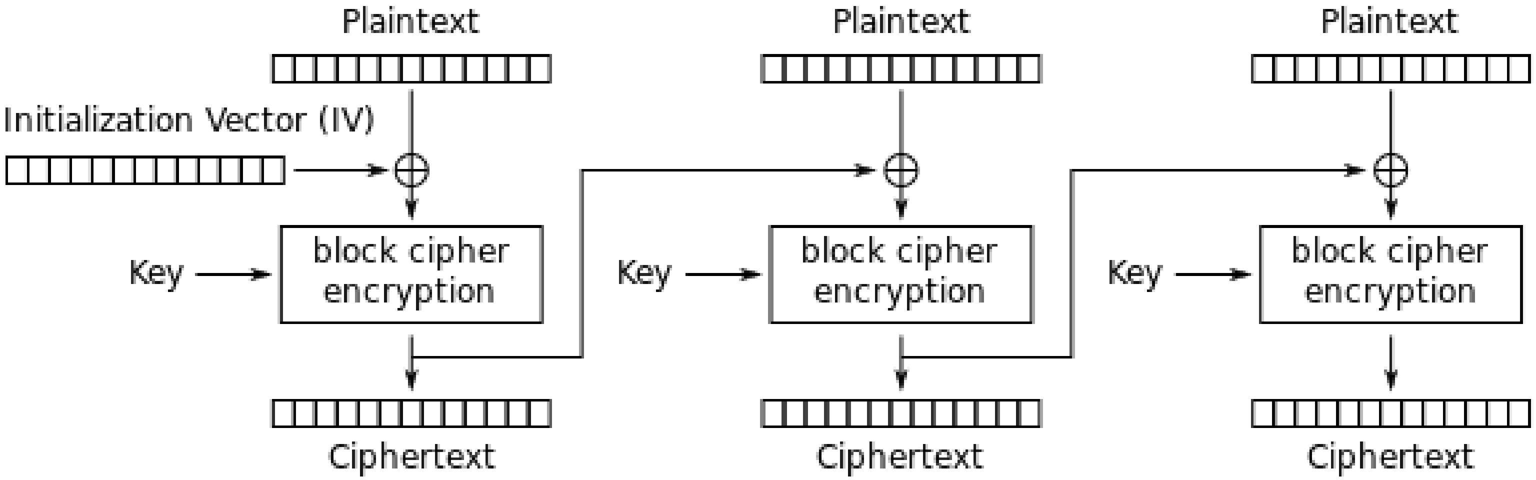
Simple Hash Functions

Bit by Bit XOR

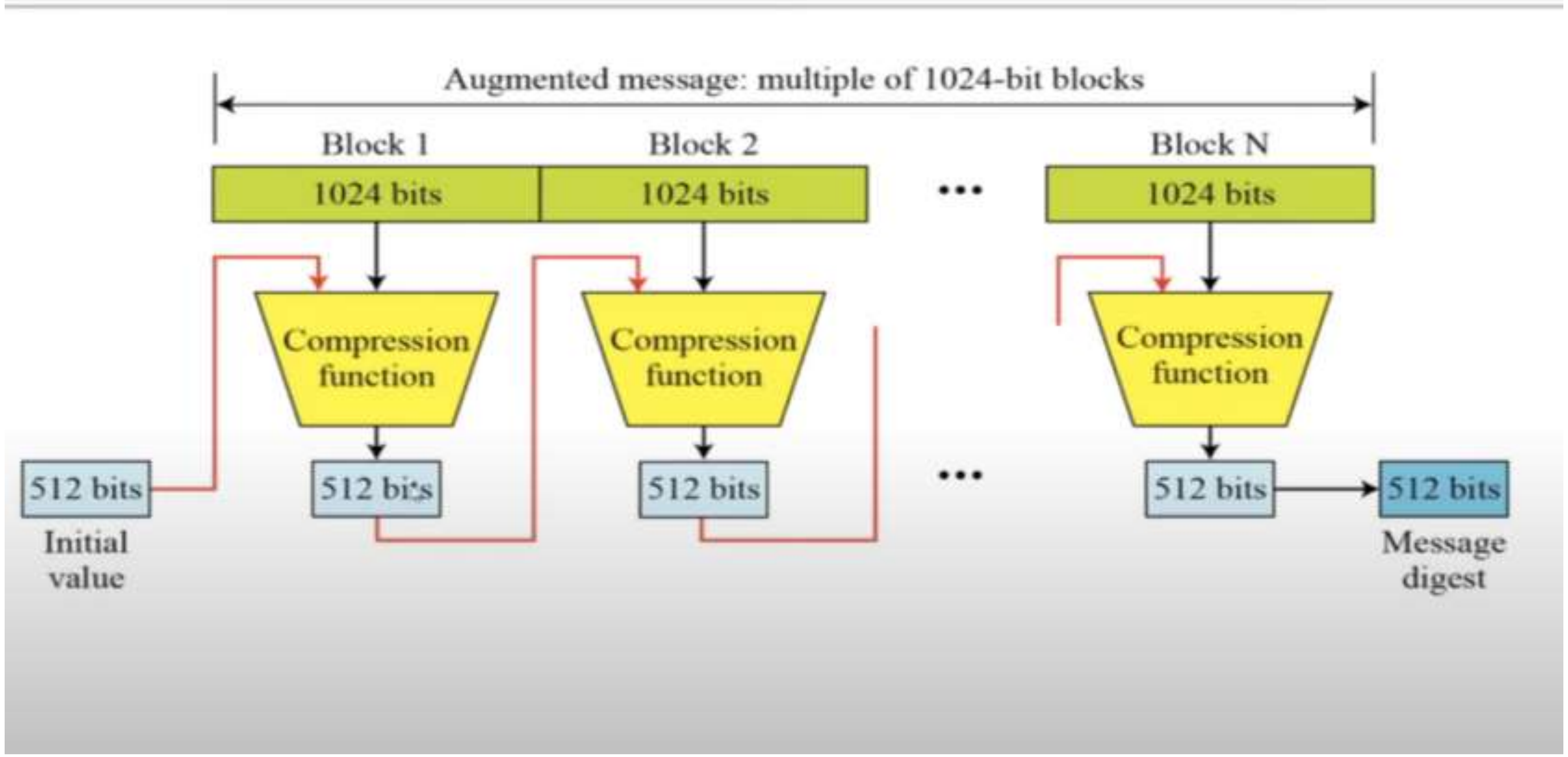
- The input (message, file, etc.) is viewed as a sequence of n-bit blocks. The input is processed one block at a time in an iterative fashion to produce an n-bit hash function.
- One of the simplest hash functions is the bit-by-bit exclusive-OR (XOR) of every block. This can be expressed as
- Ci = bi1 $\oplus$bi2 $\oplus$ ….$\oplus$bim

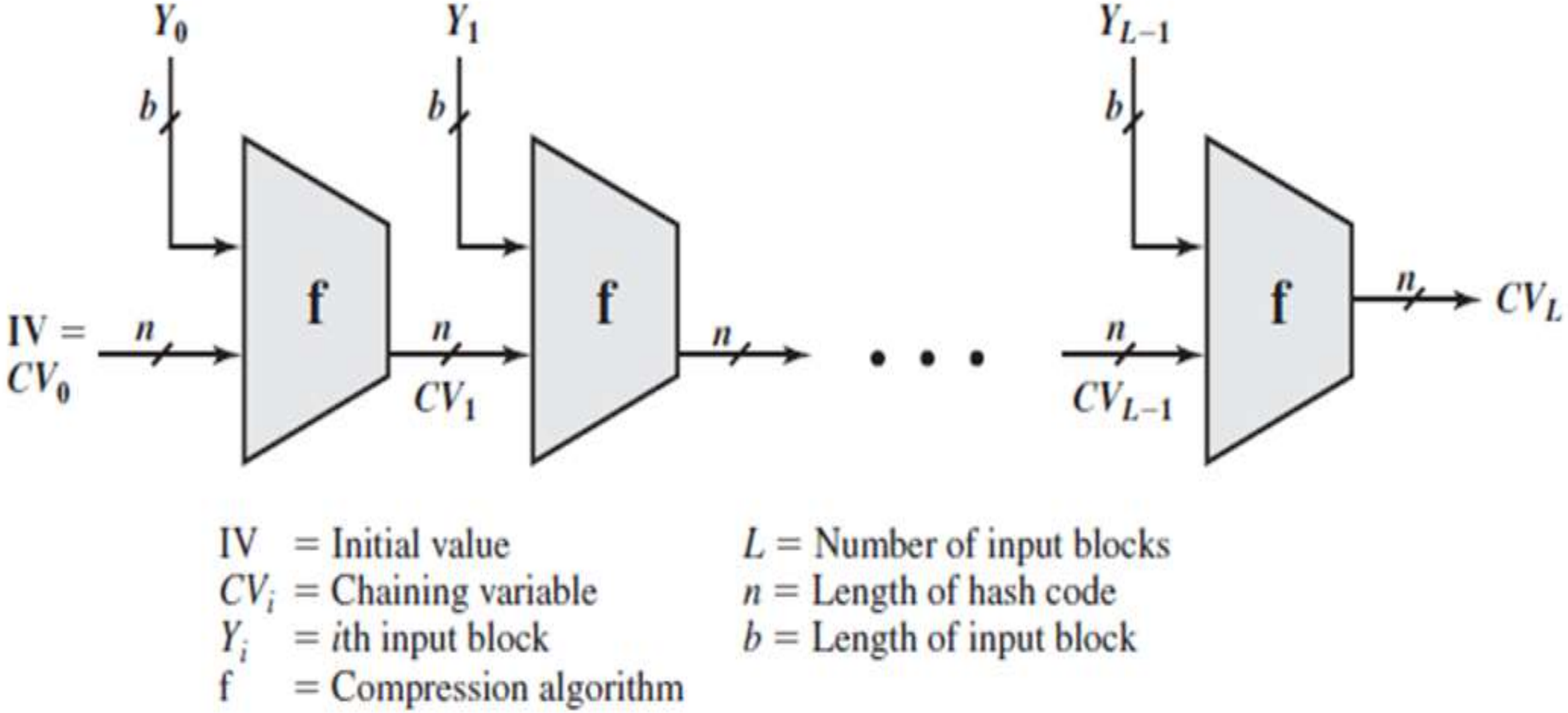
Hash Function based on CBC

Cipher Block Chain



Cipher Block Chaining (CBC) mode encryption


Augmented message: multiple of 1024-bit blocks
Block 1
Block 2
Block N
1024 bits
1024 bits
1024 bits
• • •
Compression function
Compression function
Compression function
512 bits
Initial value
512 bits
512 bits
• • •
512 bits
512 bits
Message digest



IV = Initial value
CV_i = Chaining variable
Y_i = ith input block
f = Compression algorithm

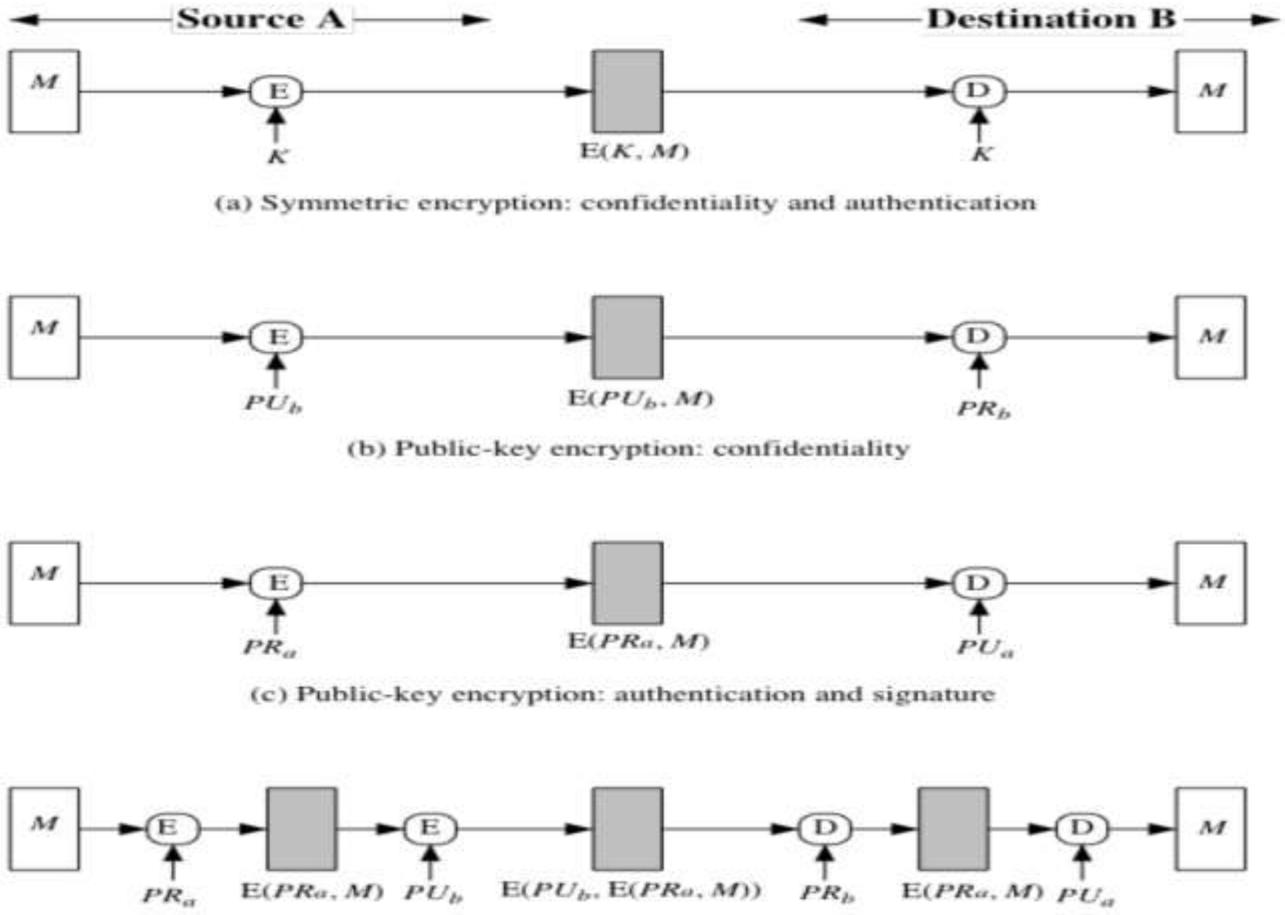
L = Number of input blocks
n = Length of hash code
b = Length of input block

Secure Hash Algorithm (SHA)

- SHA was developed by the National Institute of Standards and Technology (NIST) and published as a federal information processing standard (FIPS 180) in 1993.
- SHA-1 produces a hash value of 160 bits. In 2002, NIST produced a revised version of the standard, FIPS 180-2, that defined three new versions of SHA, with hash value lengths of 256, 384, and 512 bits, known as SHA-256, SHA-384, and SHA-512, respectively. Collectively, these hash algorithms are known as SHA-2

• The algorithm takes as input a message with a maximum length of less than 2128 bits and produces as output a 512-bit message digest. The input is processed in 1024-bit blocks

Message Encryption



(a) Symmetric encryption: confidentiality and authentication

(b) Public-key encryption: confidentiality

(c) Public-key encryption: authentication and signature

(d) Public-key encryption: confidentiality, authentication, and signature