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

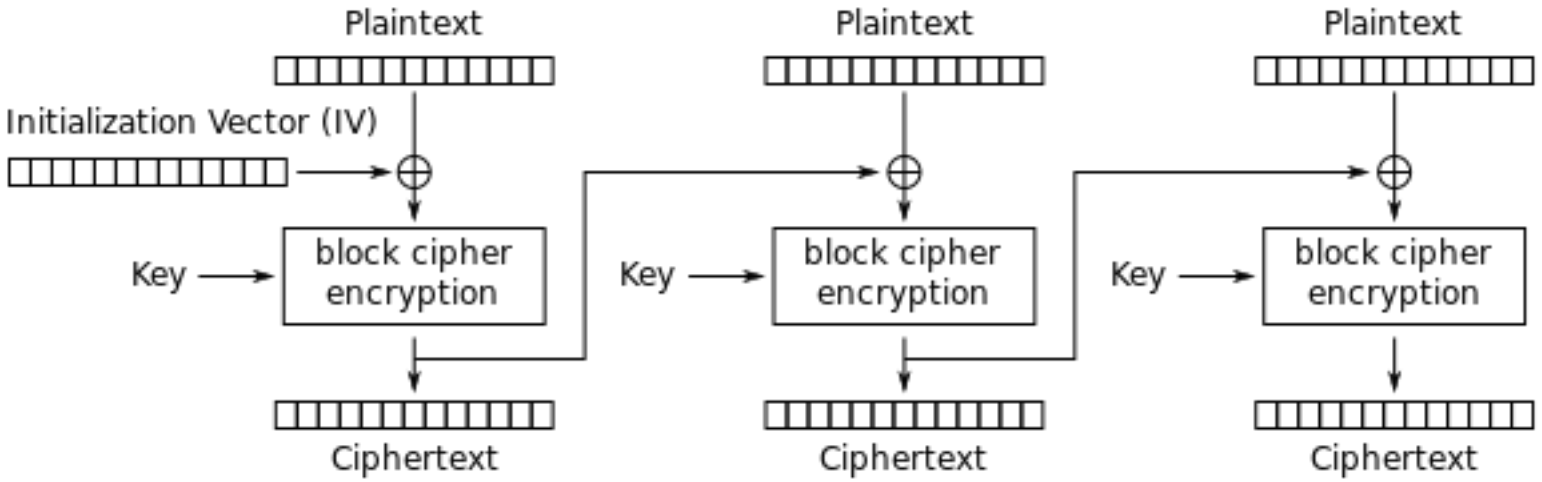
Simple Hash Functions

Bit by Bit XOR

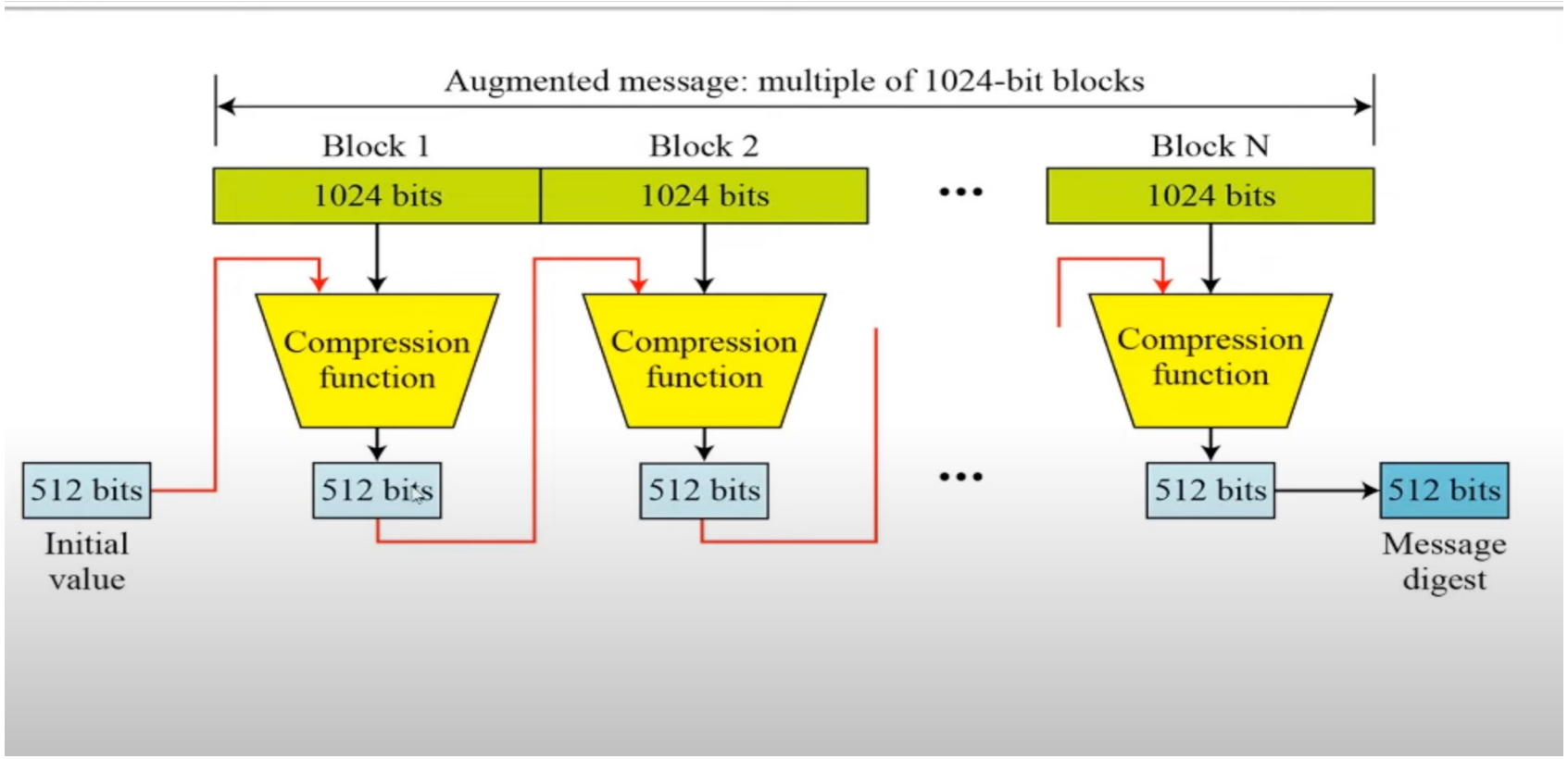
- The input (message, file, etc.) is viewed as a sequence of n-bit blocks. The input is processed one block at a time in an iterative fashion to produce an n-bit hash function.
- One of the simplest hash functions is the bit-by-bit exclusive-OR (XOR) of every block. This can be expressed as
- $Ci = bi1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

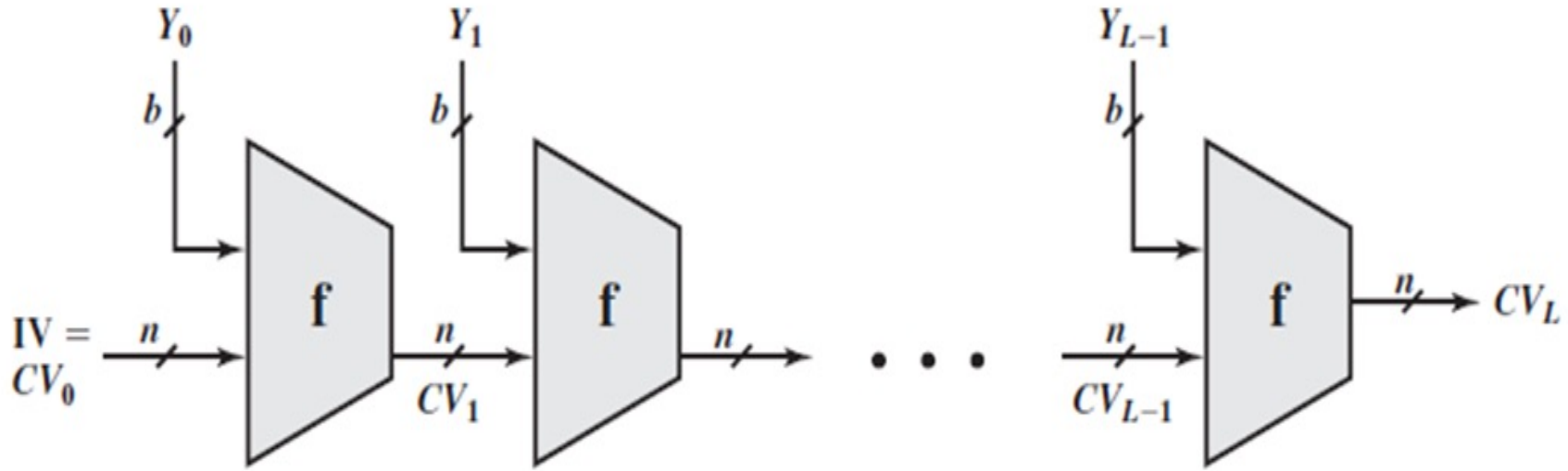
Hash Function based on CBC

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
512 bits
512 bits
512 bits
512 bits
Initial value
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