CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous class

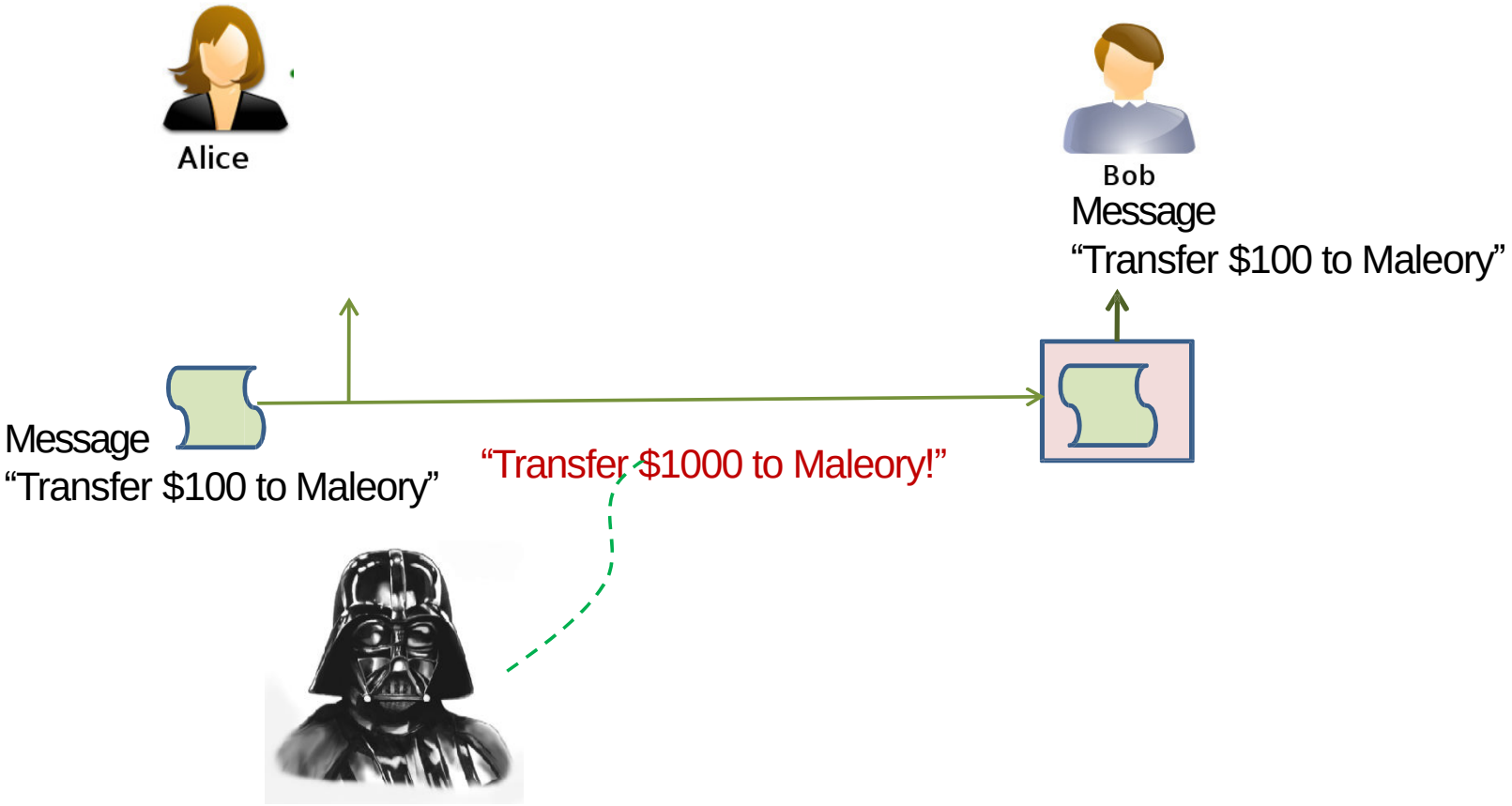
- Crypto Basics
- Cryptographic algorithms
  - important element in security services
- review various types of elements
  - symmetric encryption

Present class

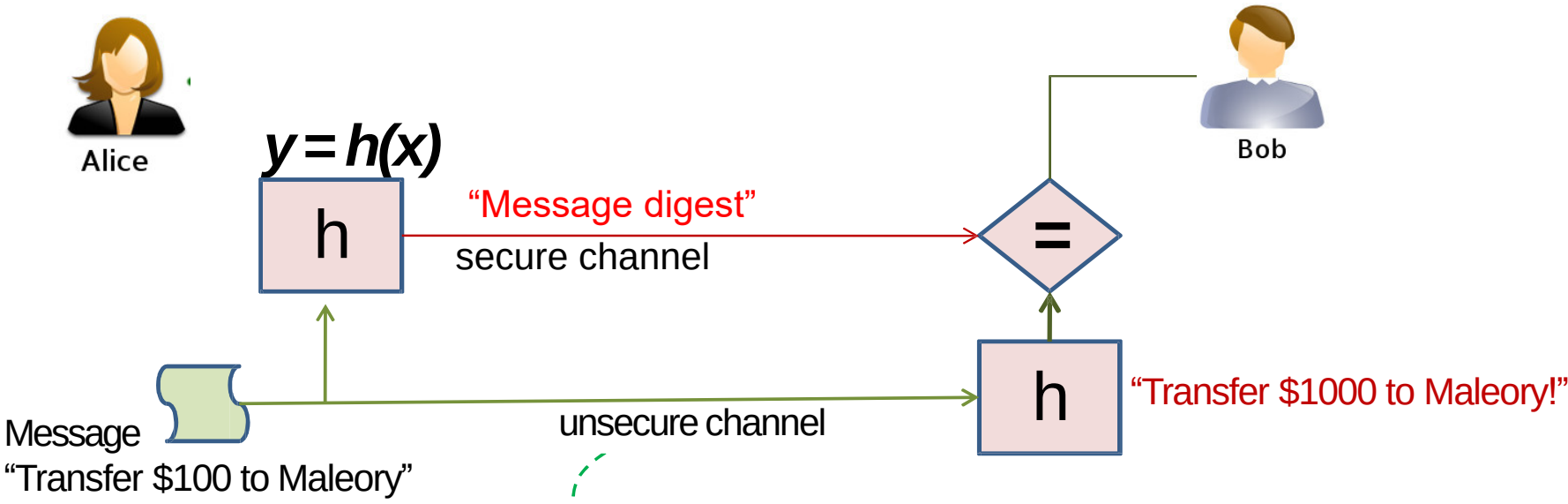
- Crypto Basics

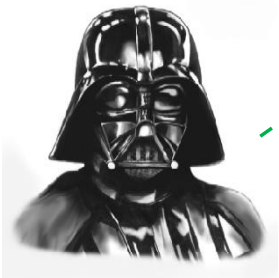
- review various types of elements
  - Cryptographic Hash function
    - MAC
  - Public key encryption

Hash (Manipulation Detection code)



Hash (Manipulation Detection code)





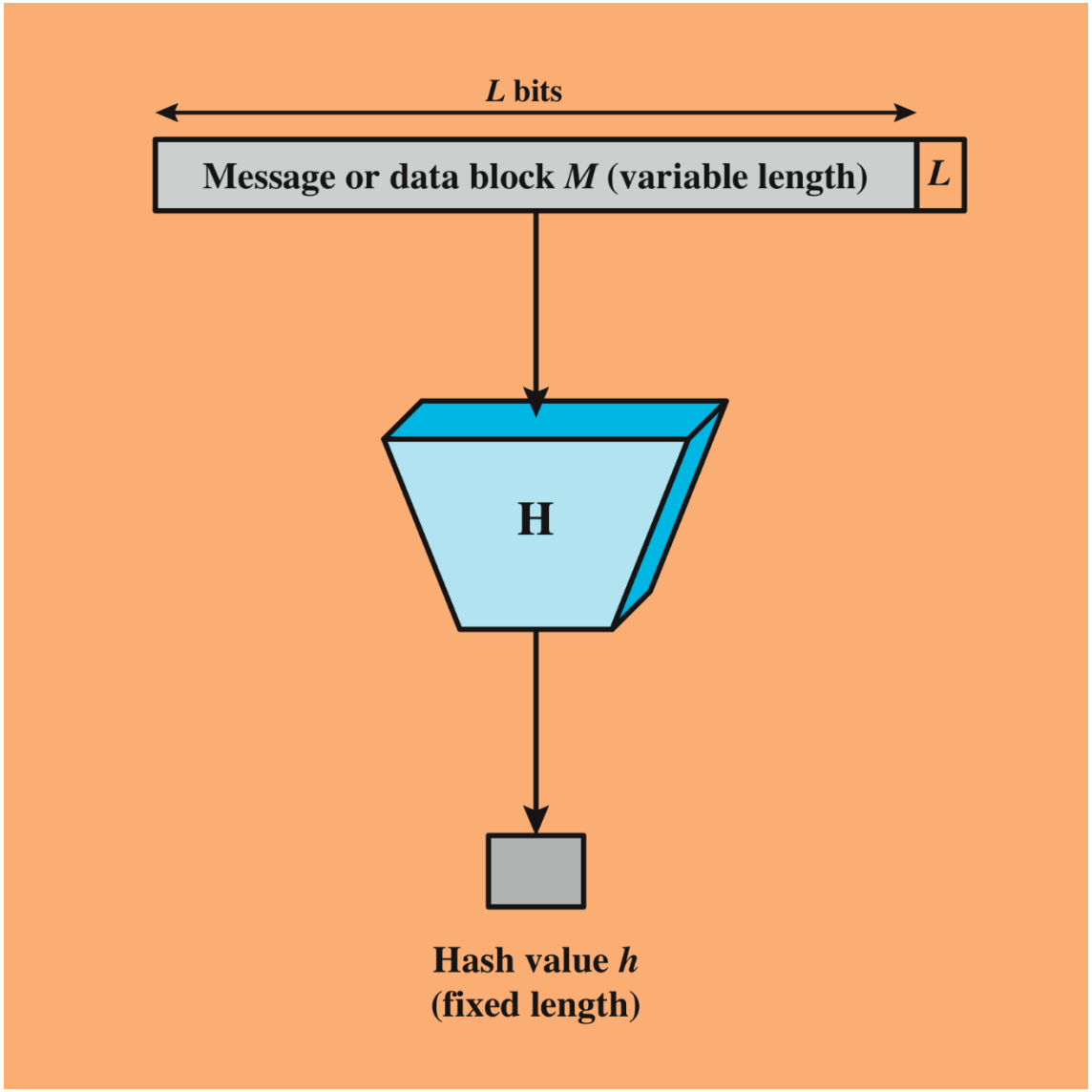
To suceed
Maleory needs to modify x to x', such that
h(x) = h(x')

Goal of Hash functions is to resist such collisions

Attacks against MDC

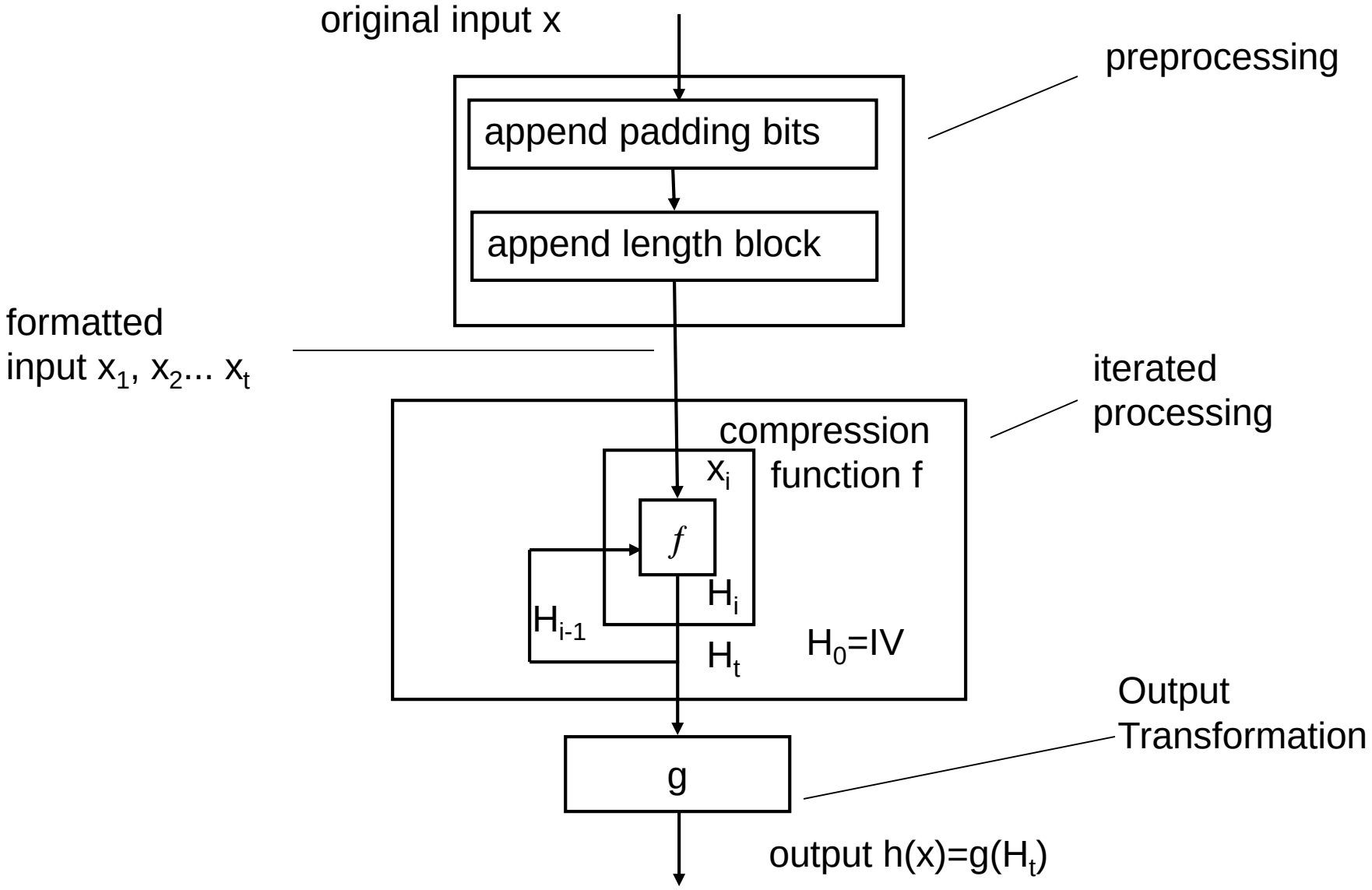
OWHF: given y find x s.t. h(x)=y; or given (x,h(x)) find x' ≠x s.t. h(x')=h(x)

CRHF: find any two inputs x' ≠x s.t. h(x')=h(x) (birthday attack)

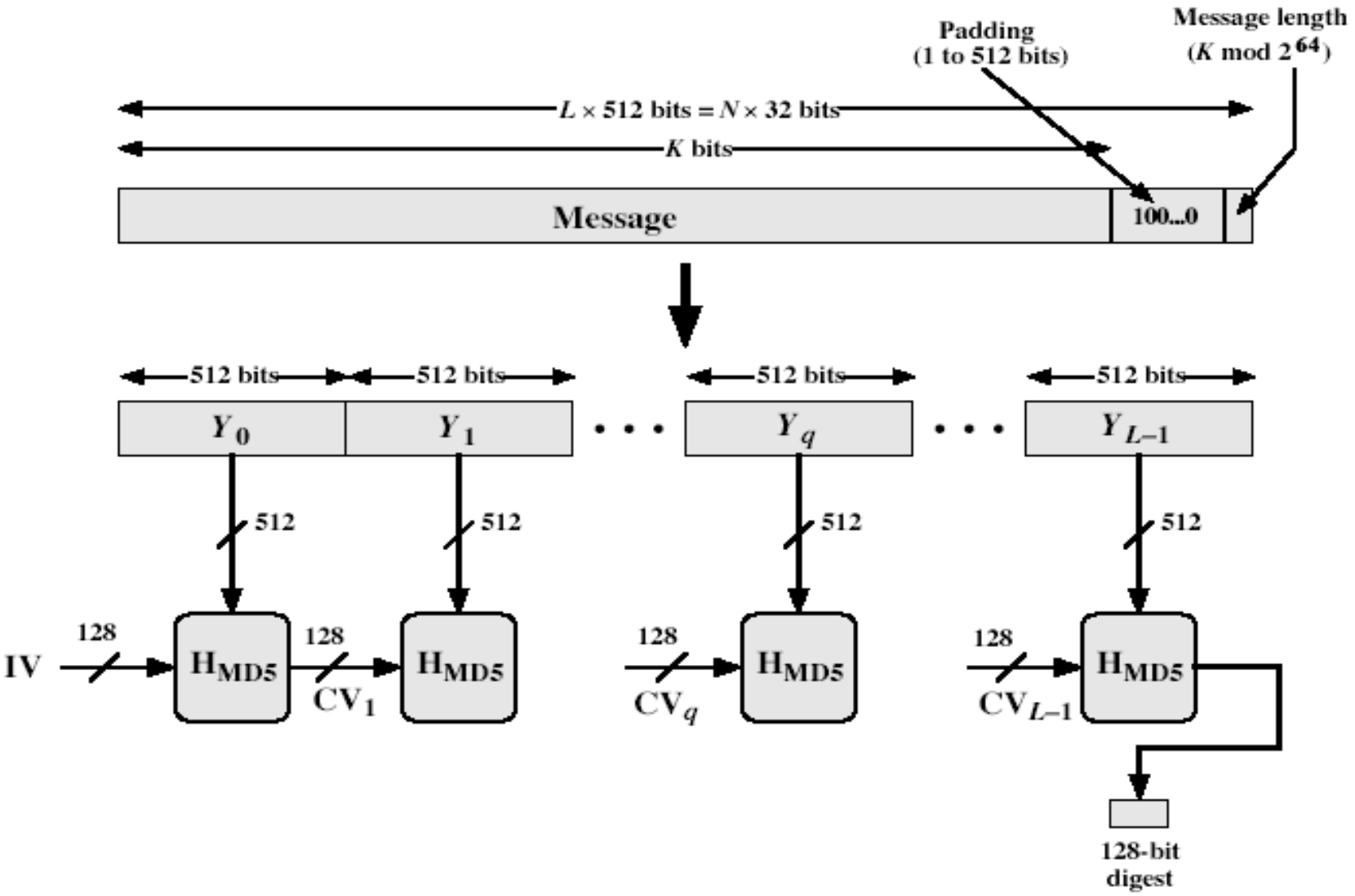


Secure Hash Functions

Iterated Hash Function



MD5 Overview

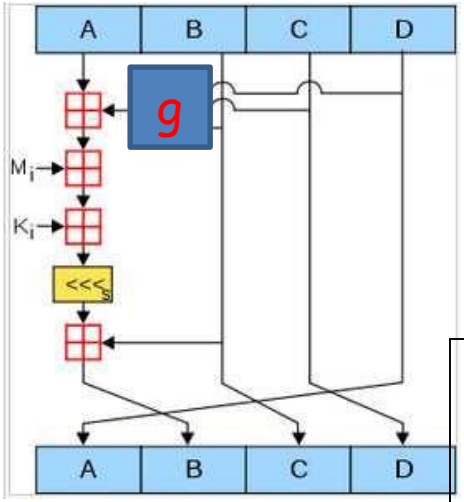


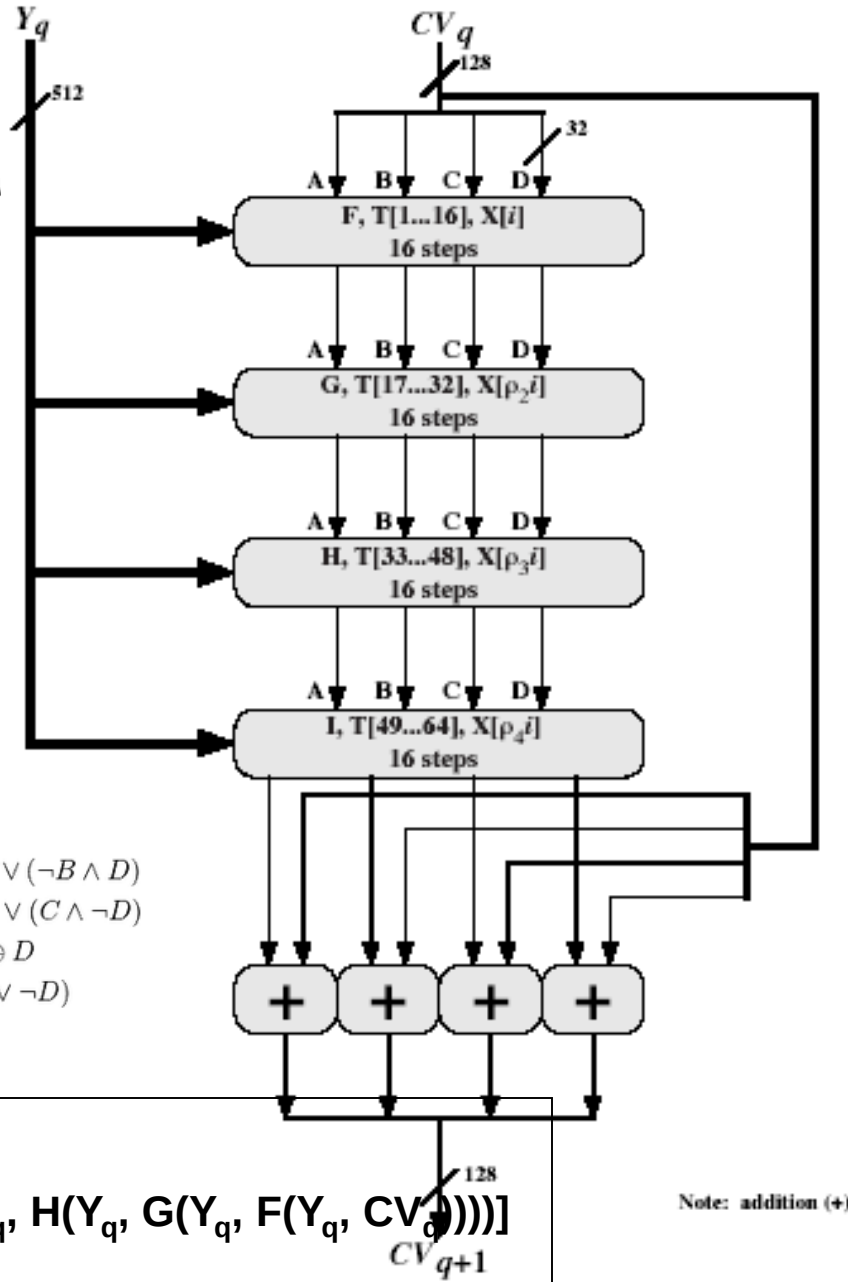
each round has 16 steps of the form:
B = B+((A+g(B,C,D)+X[k]+T[i])<<<s)
T[i] is a constant value (ith 32-bit word in matrix T) derived from sin

X[k] is M[q x 16 + k], the kth 32-bit word in the qth 512-bit block of the message

<<<s is circular left shift of the 32-bit argument by s bits

IV: h1 = 0x67452301, h2 = 0xefcdab89, h3 = 0x98badcfe, h4 = 0x10325476





$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D)$$

CV_0 = IV

CV_{q+1} = SUM_{32}[CV_q, I (Y_q, H(Y_q, G(Y_q, F(Y_q, CV_q))))]

MD = CV_{L-1}

Note: addition (+) is mod 2^{32}

Figure MD5 Processing of a Single 512-bit Block

Thanks