

Lecture 16

Yuan Xue

Oct 24 2006



Outline

- ◆ Review of Hash function
- ◆ Hash algorithm design
 - MD5
- ◆ HMAC
- ◆ Digital Signature

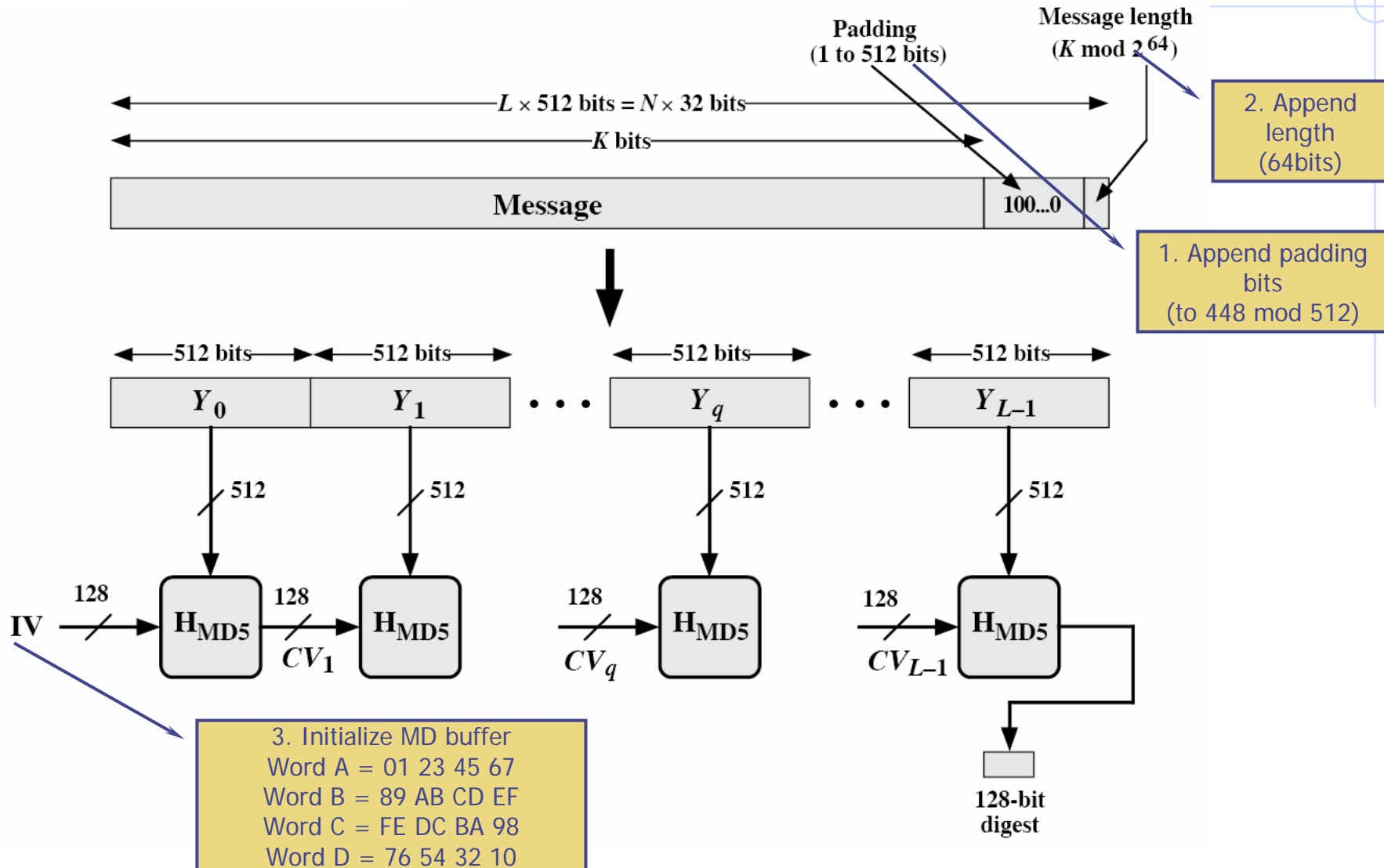


Review of Hash function

- ◆ Hash function H
 - $h = H(M)$
 - ◆ M is a message of variable length
 - ◆ h is a fixed-length hash value
- ◆ H satisfies the following properties:
 - One-way property
 - Weak collision resistance
 - Strong collision resistance
- ◆ Widely used hash functions
 - MD5
 - SHA family (e.g. SHA-1, SHA-2)
- ◆ Usage
 - Standalone
 - With encryption algorithms
 - ◆ Message Authentication
 - ◆ Digital Signature

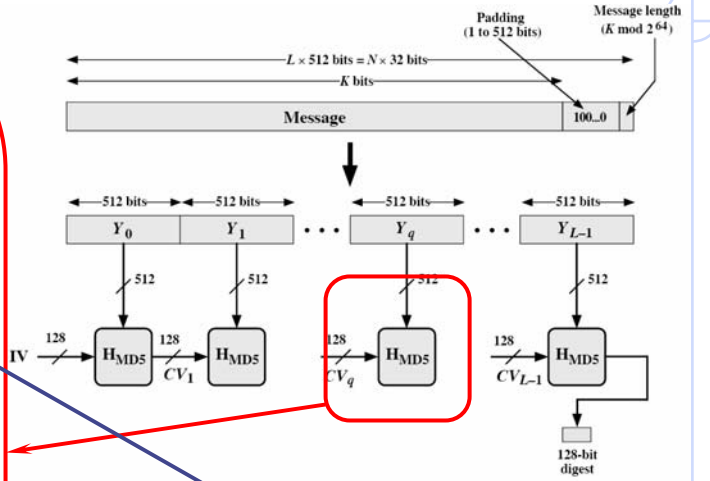
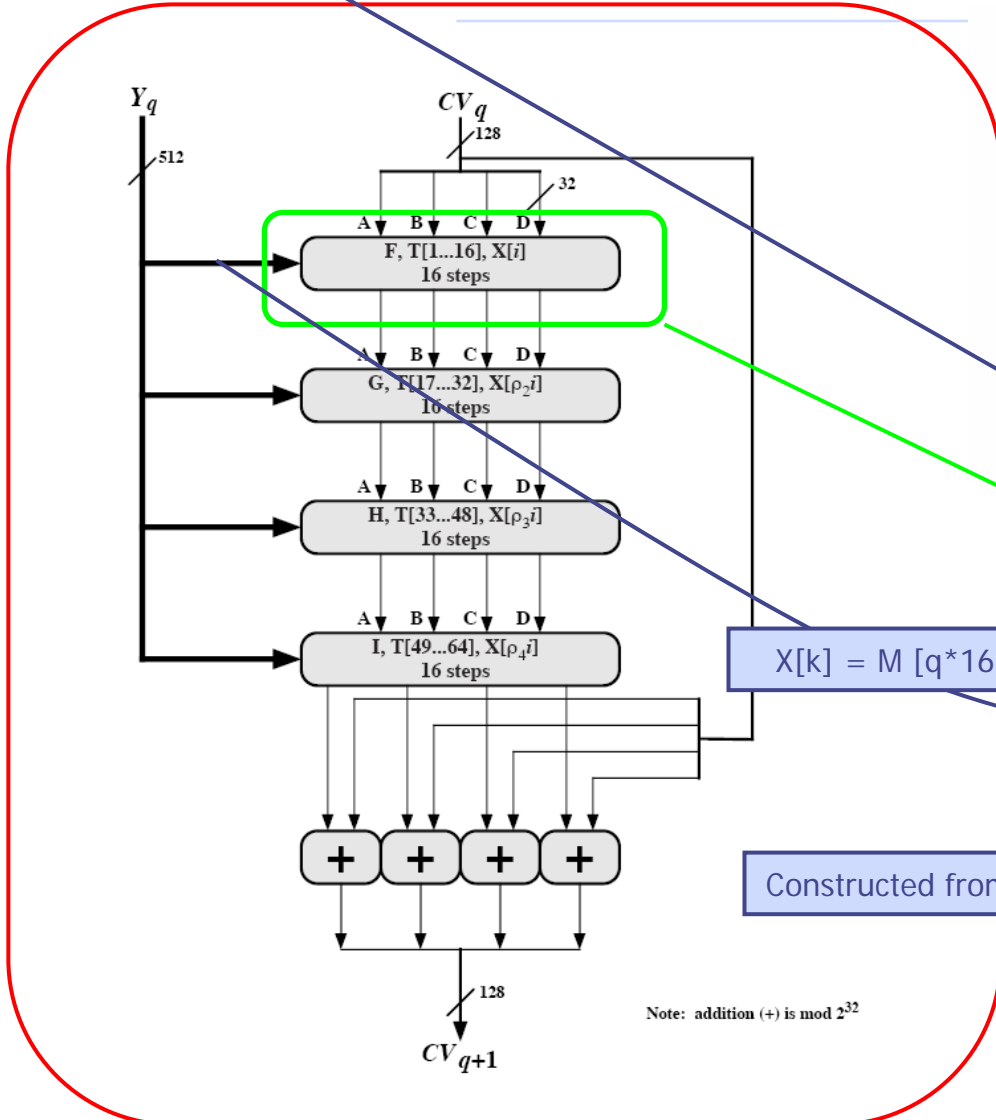


Hash Algorithm Design – MD5



b	c	d	F	G	H	I
0	0	0	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0

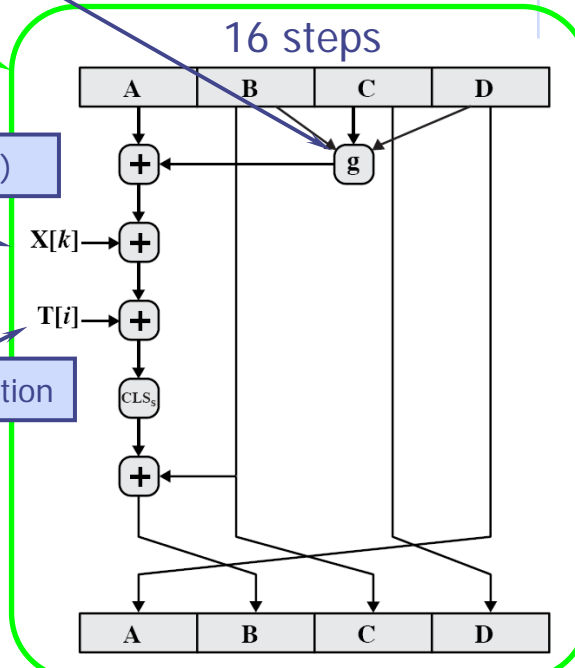
Hash Algorithm Design – MD5



$X[k] = M[q \cdot 16 + k] \text{ (32 bit)}$

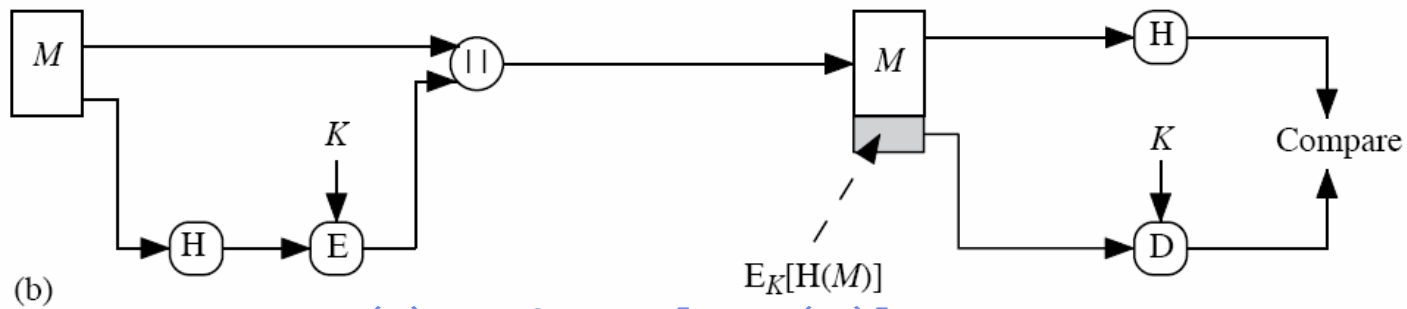
Constructed from sine function

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

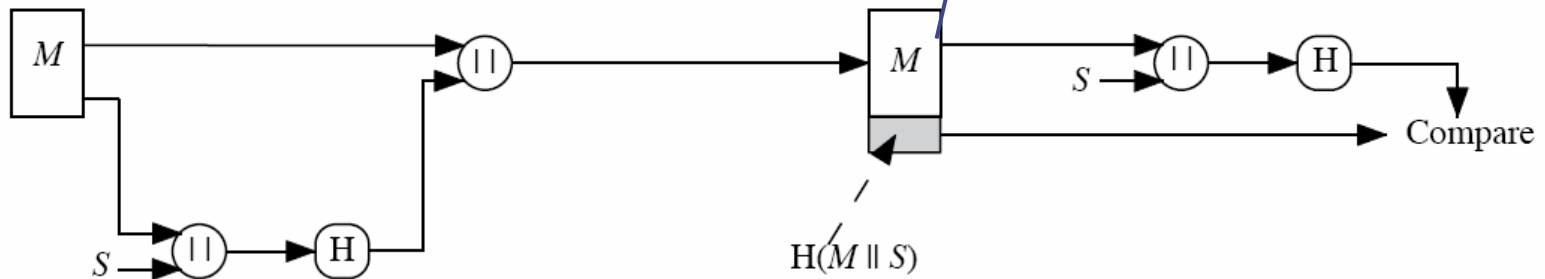


HMAC

- ◆ Hash function works with a symmetric key to provide message authentication
- ◆ Two methods

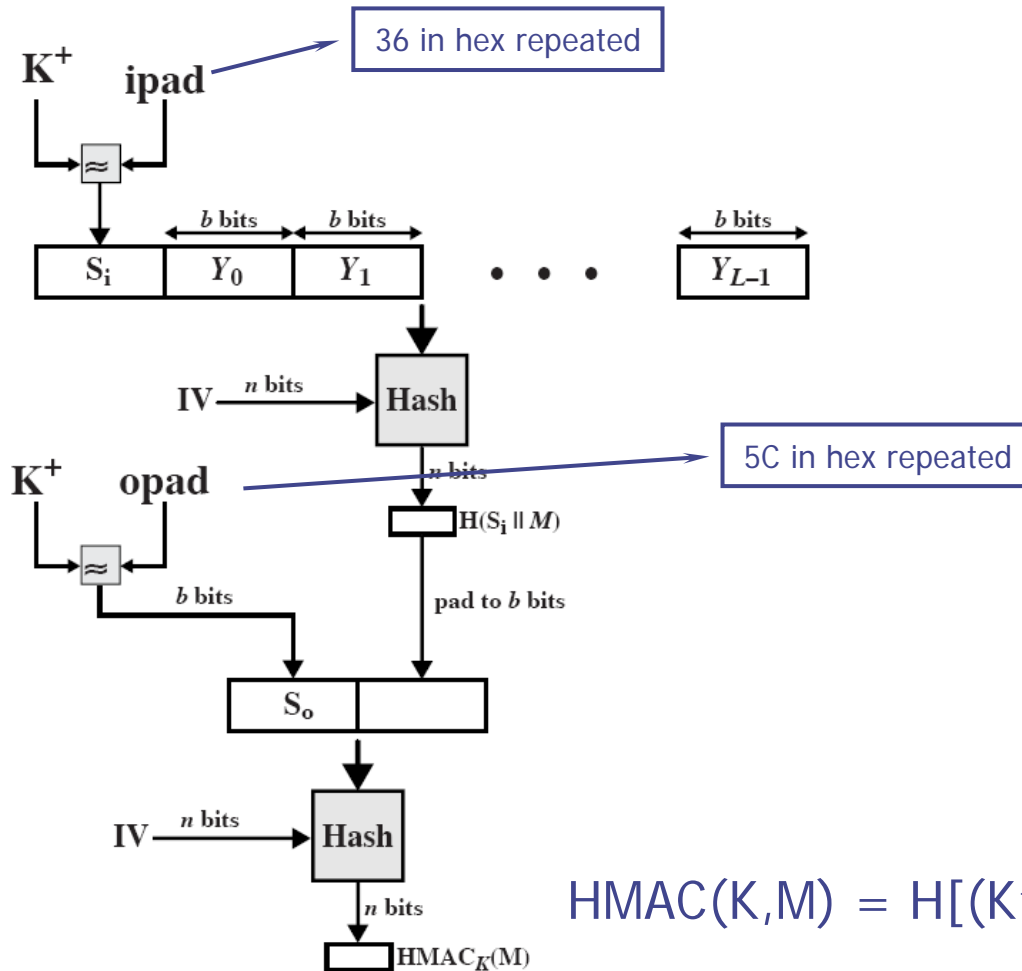


$$(1) \text{ MAC} = E [K, H(M)]$$



$$(2) \text{ MAC} = H [M || S] \rightarrow \text{Idea for HMAC}$$

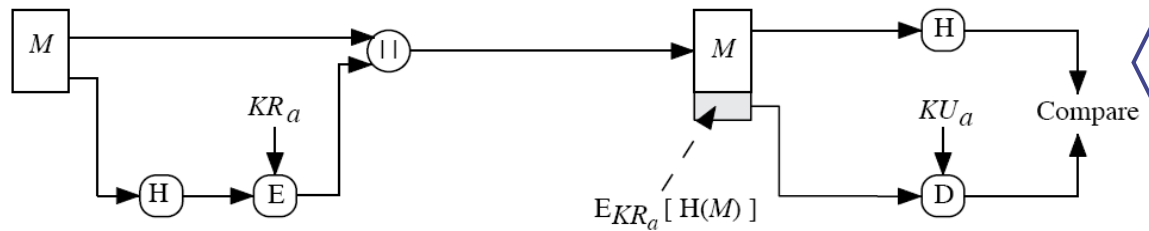
HMAC Structure



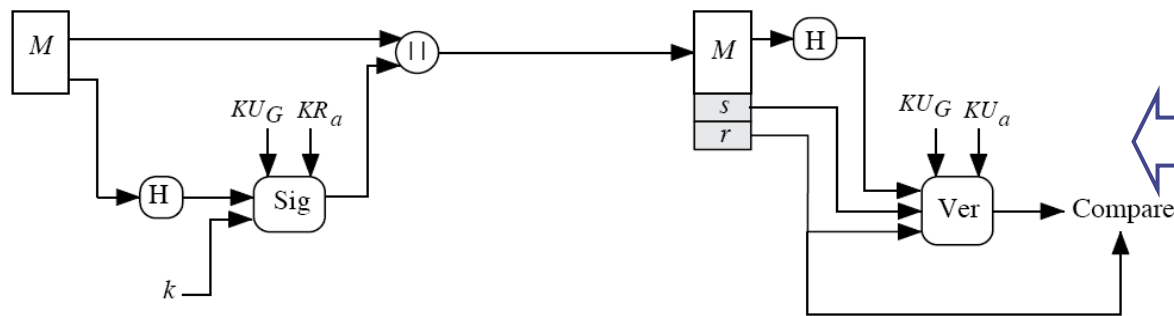
$$HMAC(K, M) = H[(K^+ \oplus opad) || H[(K^+ \oplus ipad) || M]]$$

Digital Signature

Two approaches



(a) RSA Approach



(b) DSS Approach

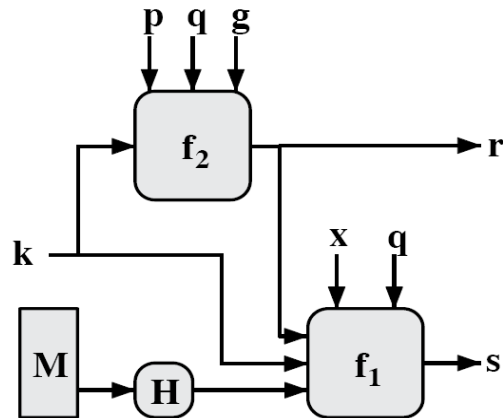
- Encryption of hash value via private key provides digital signature
- Any asymmetric encryption algorithm could be used
 - ◆ E.g. RSA

- Many asymmetric encryption algorithms have export restriction
- DSA (digital signature algorithm)-based approach

Digital Signature Algorithm

◆ Digital Signature Algorithm

- An asymmetric key algorithm
- Can not be used for encryption
- Can ONLY be used for digital signature



$$s = f_1(H(M), k, x, r, q) = (k^{-1} (H(M) + xr)) \bmod q$$

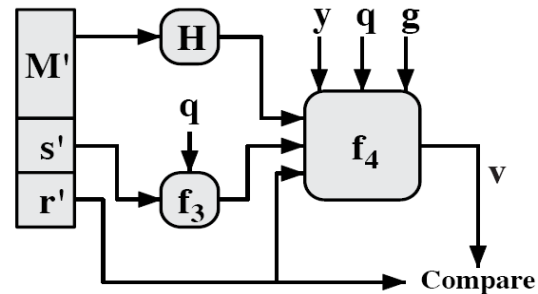
$$r = f_2(k, p, q, g) = (g^k \bmod p) \bmod q$$

(a) Signing

◆ Algorithm

- Based on discrete log operation
- Global variables
 - ◆ p, q, g
 - ◆ Private key x
 - ◆ Public key $y = g^x \bmod p$

◆ User per-msg secret num k



$$w = f_3(s', q) = (s')^{-1} \bmod q$$

$$v = f_4(y, q, g, H(M'), w, r')$$

$$= ((g^{H(M')w} \bmod q) y^{r'w} \bmod q) \bmod p \bmod q$$

(b) Verifying