Capítulo 9

Algoritmos Hash

Plano de Curso

- MD5 - Message Digest (RFC 1321) por Ron Rivest
- SHA - Security Hash Algorithm
- RIPEMD-160
- HMAC

Algoritmo MD5

1 - Adicionar bits (total ≡ 448 mod 512)

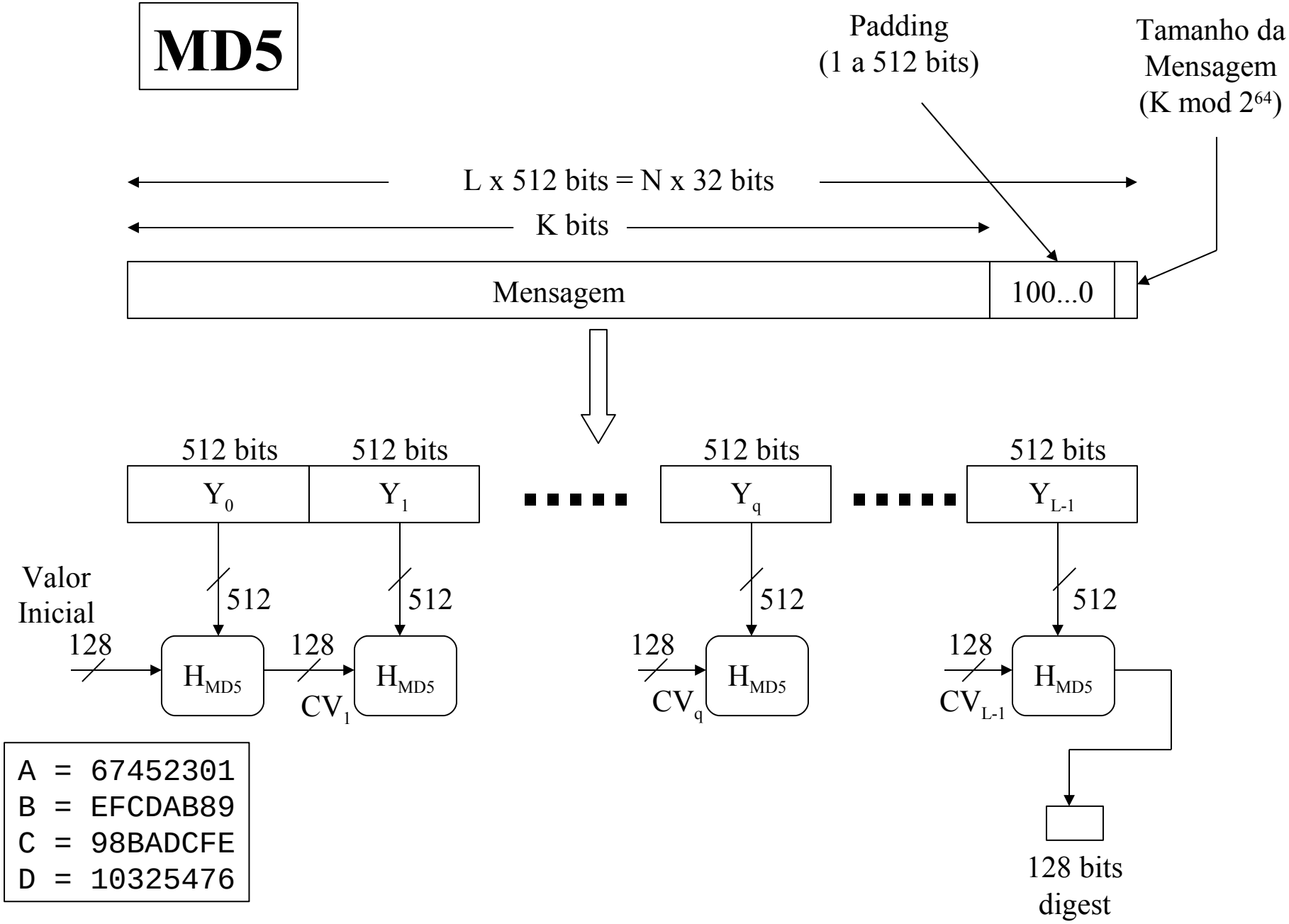
2 - Adicionar o Comprimento

3 - Inicializar Buffer MD

```
A = 67452301          B = EFCDAB89
C = 98BADCFE          D = 10325476
```

4 - Processar Mensagens em Blocos de 512 bits

MD5


Padding
(1 a 512 bits)
Tamanho da
Mensagem
(K mod 2^64)
L x 512 bits = N x 32 bits
K bits
Mensagem
100...0
512 bits
512 bits
512 bits
512 bits
Y0
Y1
Yq
YL-1
Valor
Inicial
128
512
512
512
512
128
128
128
HMD5
HMD5
HMD5
HMD5
CV1
CVq
CVL-1
A = 67452301
B = EFCDAB89
C = 98BADCFE
D = 10325476
128 bits
digest

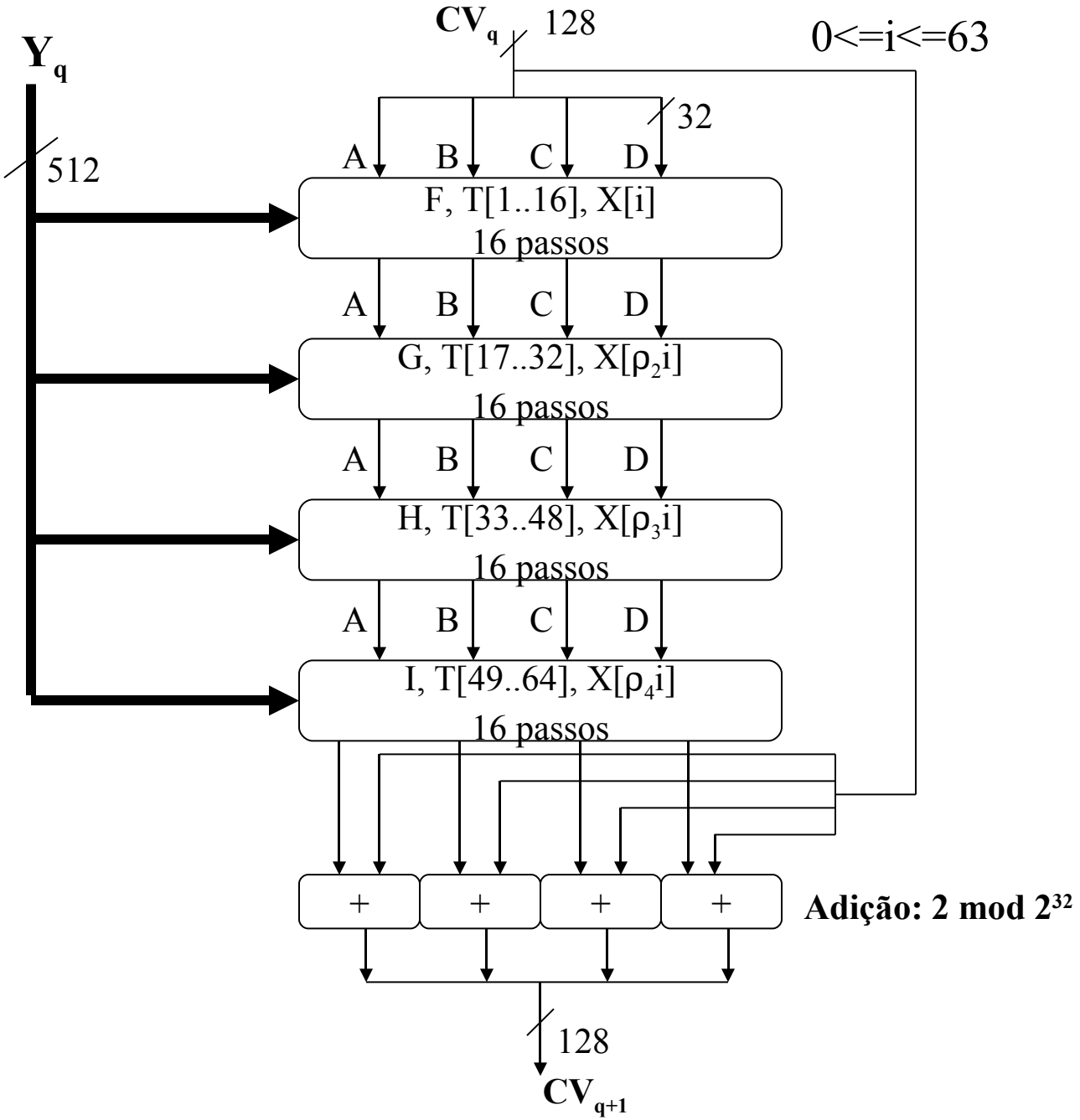
H_{MD5}

$1 <= j <= 64$

$T[j] = 2^{32} \times abs[\sin(j)]$

Tabela Verdade das Funções Lógicas

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	1
1	1	1	1	1	1	0



Função de Compressão

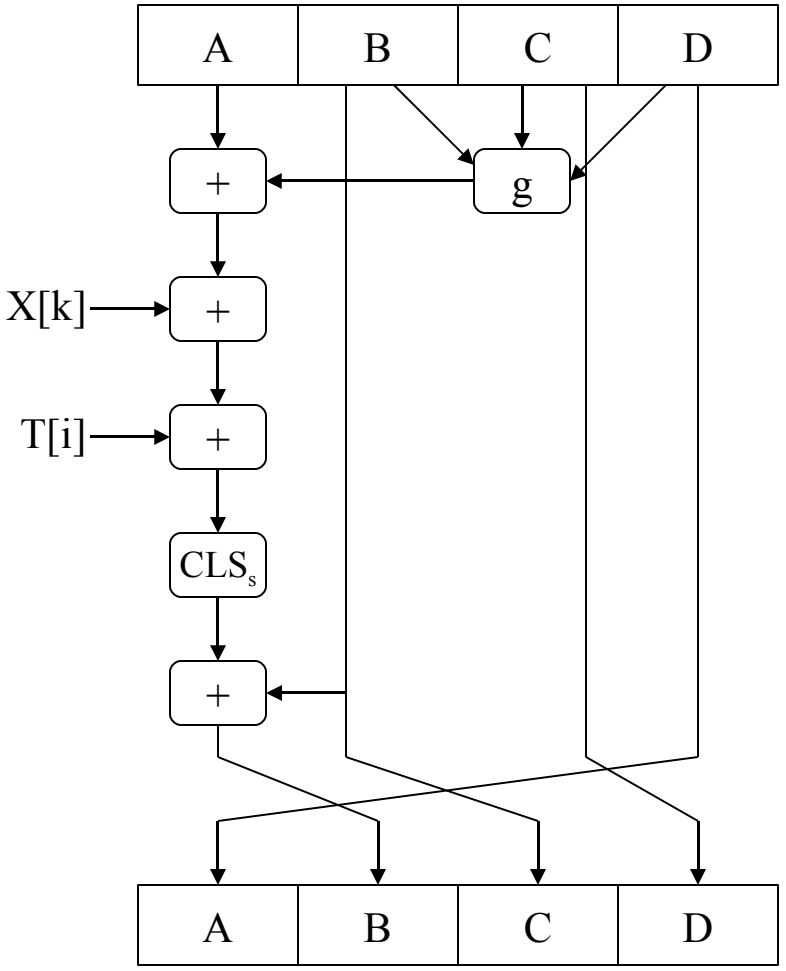
Fase	g	G(b,c,d)
1	F(b,c,d)	$(b \wedge c) \vee (\overline{b} \wedge d)$
2	G(b,c,d)	$(b \wedge d) \vee (c \wedge \overline{d})$
3	H(b,c,d)	$b \oplus c \oplus d$
4	I(b,c,d)	$c \oplus (b \vee \overline{d})$

Onde:

AND - $\wedge$
OR - $\vee$
NOT - $\overline{\ }$
XOR - $\oplus$

$\rho_2(i) = (1+5i) \bmod 16$
$\rho_3(i) = (5+3i) \bmod 16$
$\rho_4(i) = 7i \bmod 16$

S - RFC 1321



MD4

Ron Rivest, 1990
RFC 1320, 1992

- 3 rodadas
- Constantes aditivas iguais (0, t1, t2)
- 3 funções lógicas primitivas

Criptoanálise do MD5

- Criptanálise Diferencial de uma rodada, por Berson em 1992
- Ataque de Dobbertin em 1996. Conseguiu uma entrada diferente para a mesma saída de 128 bits (Um único bloco)

Algoritmo de Hash Seguro - SHA

Bloco de 160 bits

NIST
SHA = FIPS PUB 180, 1993
SHA-1 = FIPS PUB 180-1, 1995

1 - Adicionar bits (total ≡ 448 mod 512)

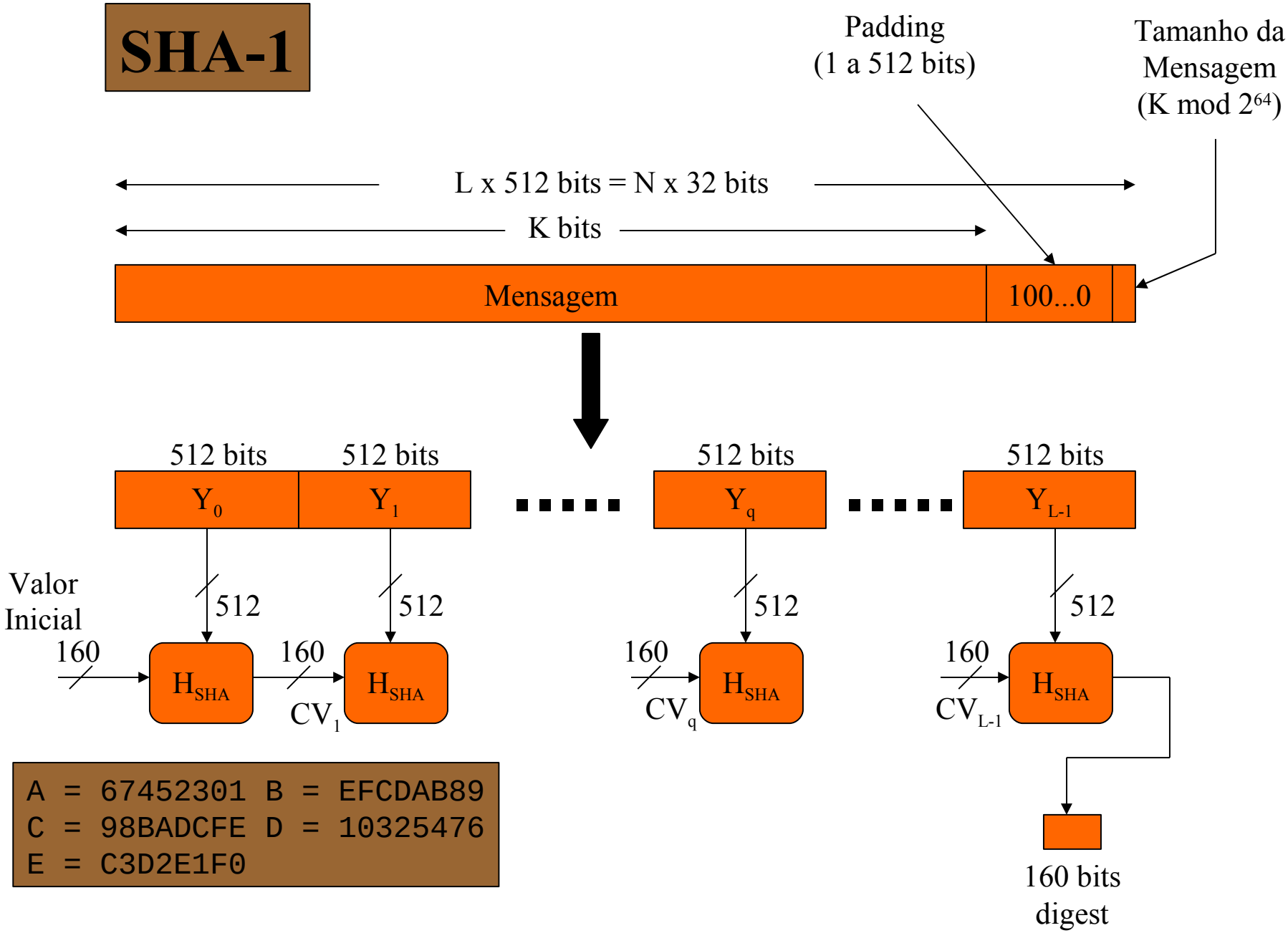
2 - Adicionar o Comprimento

3 - Inicializar Buffer MD

```
A = 67452301        B = EFCDAB89
C = 98BADCFE        D = 10325476
E = C3D2E1F0
```

4 - Processar Mensagens em Blocos de 512 bits

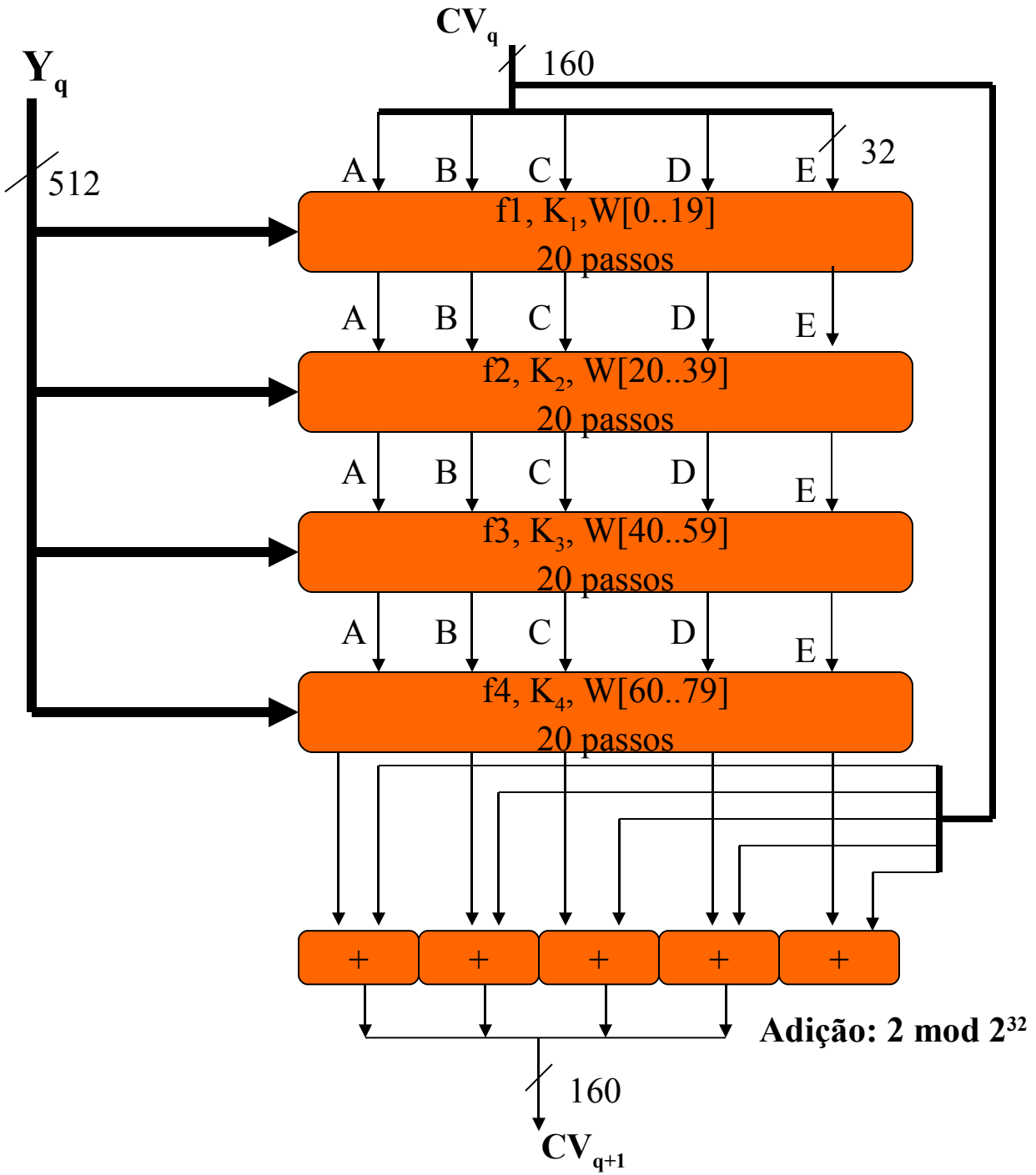
SHA-1


Padding
(1 a 512 bits)
Tamanho da
Mensagem
(K mod 2^64)
L x 512 bits = N x 32 bits
K bits
Mensagem
100...0
512 bits
512 bits
512 bits
512 bits
Y0
Y1
Yq
YL-1
Valor
Inicial
160
512
512
512
512
160
160
160
HSHA
HSHA
HSHA
HSHA
CV1
CVq
CVL-1
A = 67452301 B = EFCDAB89
C = 98BADCFE D = 10325476
E = C3D2E1F0
160 bits
digest

SHA-1

$K_1 = 5A827999$
$K_2 = 6ED9EBA1$
$K_3 = 8F1BBCDC$
$K_4 = CA62C1D6$

$K_1 = 2^{30} \times \sqrt{2}$
$K_2 = 2^{30} \times \sqrt{3}$
$K_3 = 2^{30} \times \sqrt{5}$
$K_4 = 2^{30} \times \sqrt{10}$

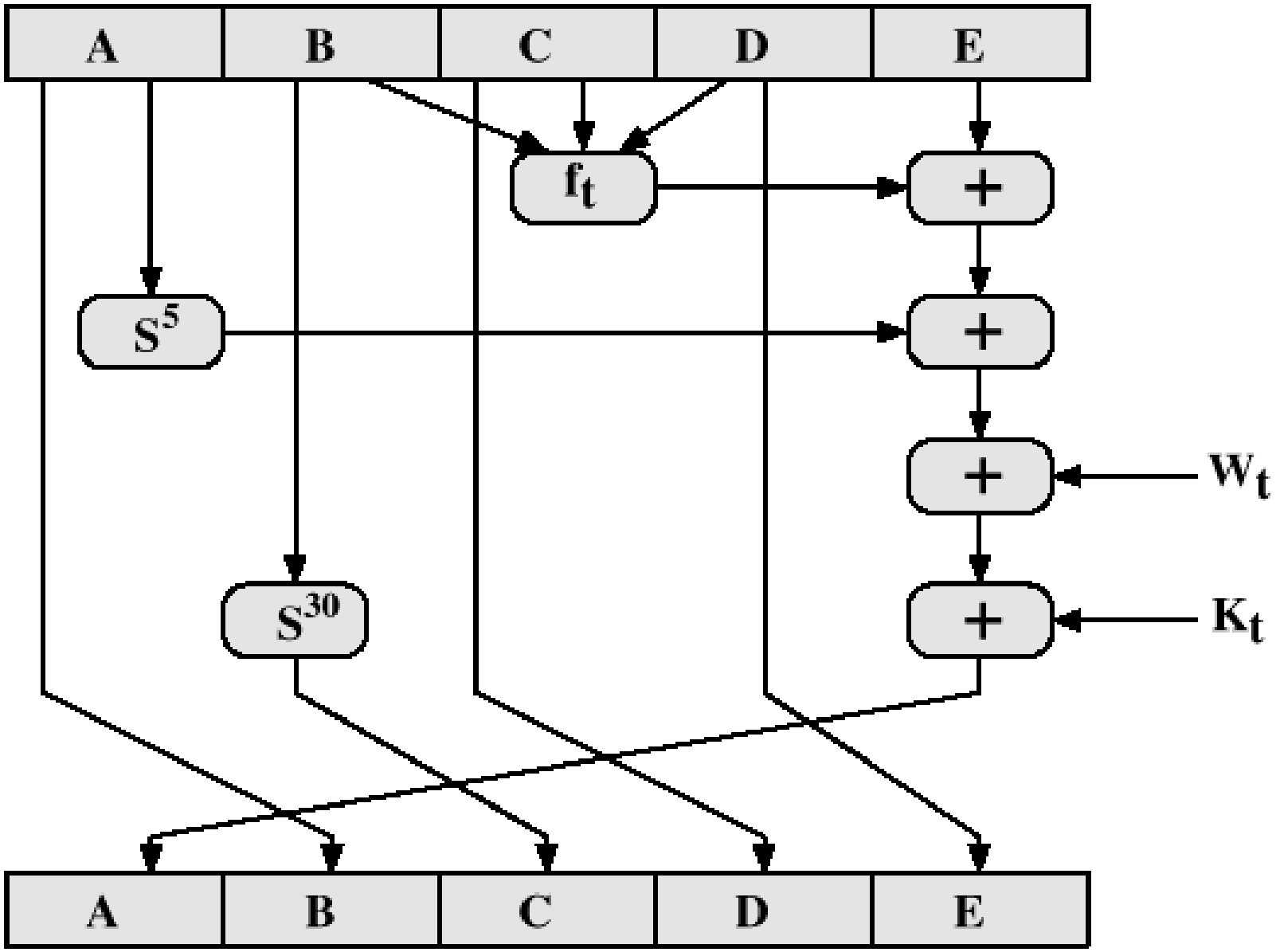


SHA-1

Tabela Verdade das Funções Lógicas

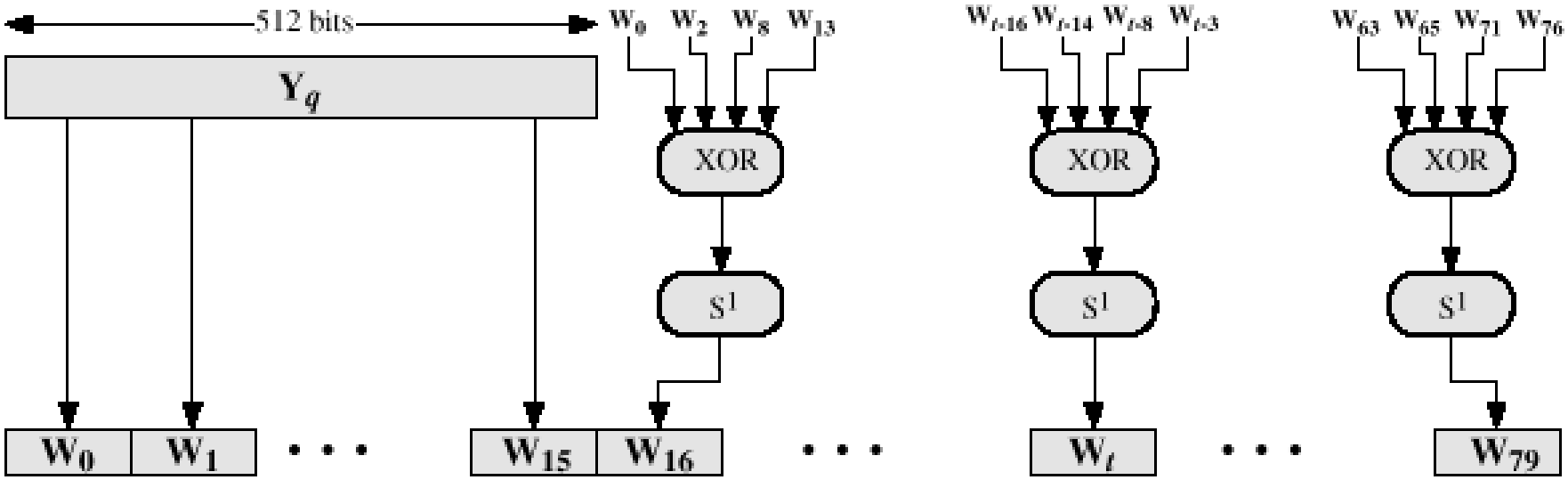
b	c	d	$f_{0..19}$	$f_{20..39}$	$f_{40..59}$	$f_{60..79}$
0	0	0	0	0	0	0
0	0	1	1	1	0	1
0	1	0	0	1	0	1
0	1	1	1	0	1	0
1	0	0	0	1	0	1
1	0	1	0	0	1	0
1	1	0	1	0	1	0
1	1	1	1	1	1	1

1 Passo



Criação das 80 palavras W

$$W_t = S^1(W_{t-16} \oplus W_{t-14} \oplus W_{t-8} \oplus W_{t-3})$$



RIPEMD - 160

Projeto RIPE, 1996

Bloco de 160 bits

1 - Adicionar bits (total ≡ 448 mod 512)

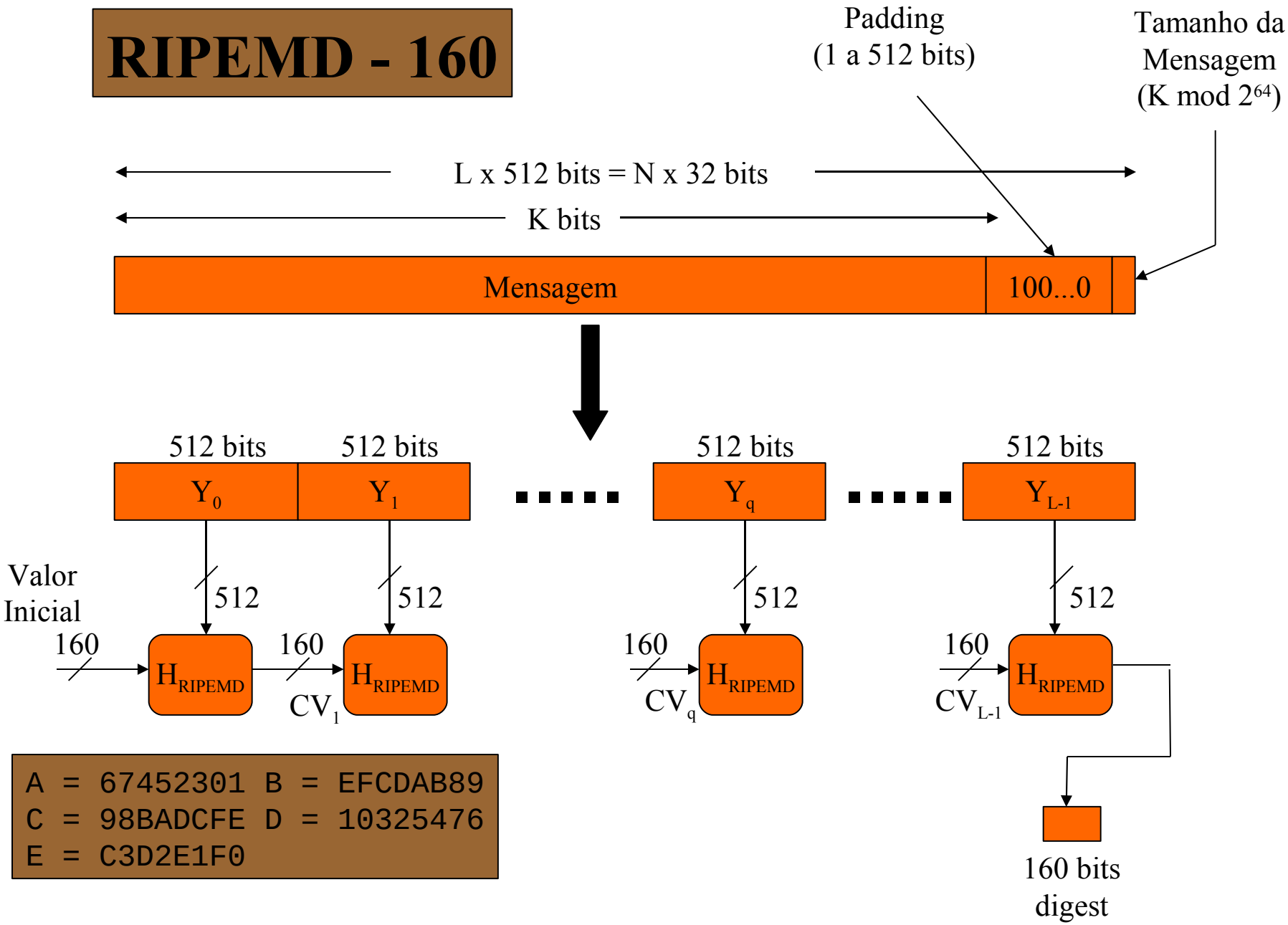
2 - Adicionar o Comprimento

3 - Inicializar Buffer MD

```
A = 67452301        B = EFCDAB89
C = 98BADCFE        D = 10325476
E = C3D2E1F0
```

4 - Processar Mensagens em Blocos de 512 bits

RIPEMD - 160

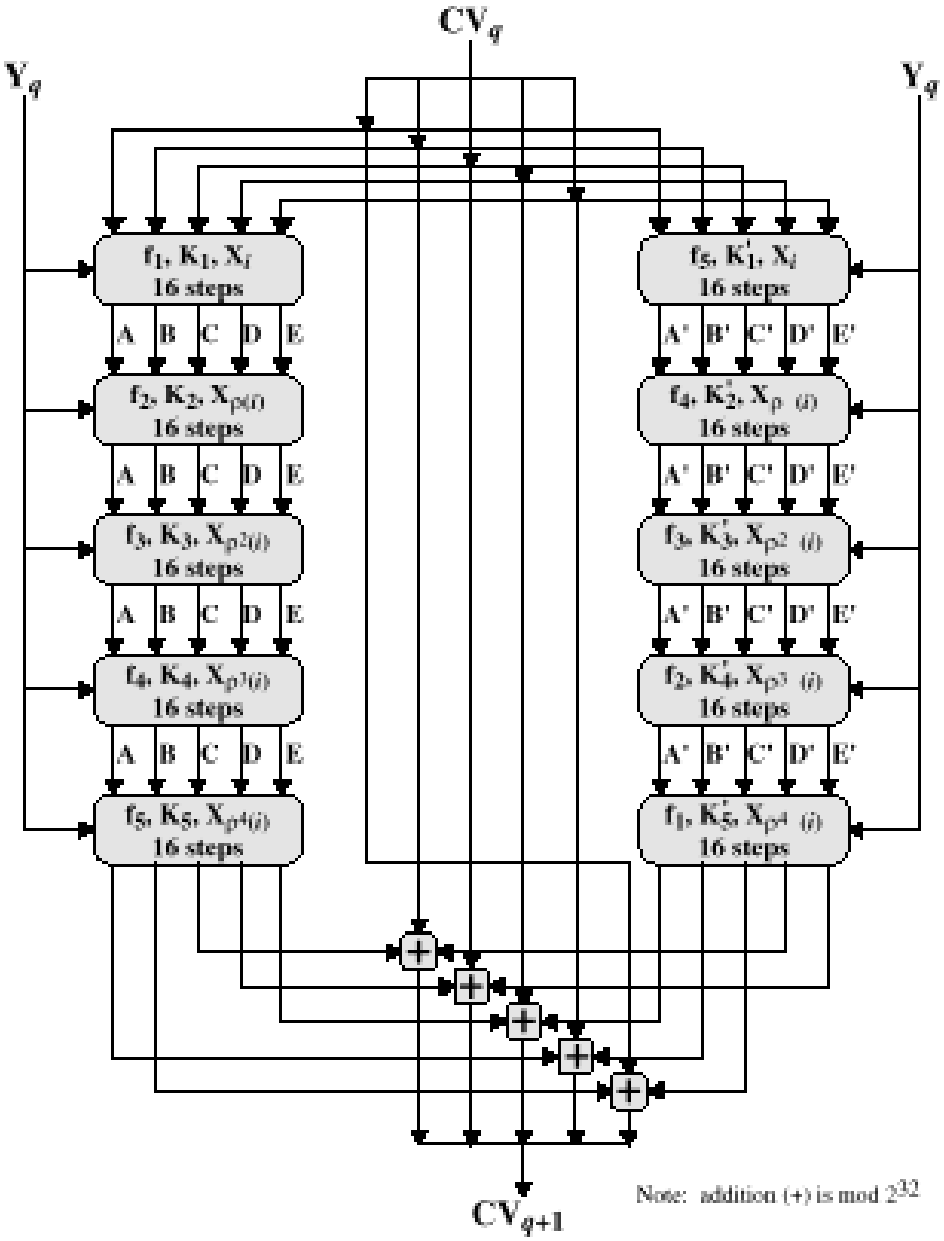



```
A = 67452301 B = EFCDAB89
C = 98BADCFE D = 10325476
E = C3D2E1F0
```

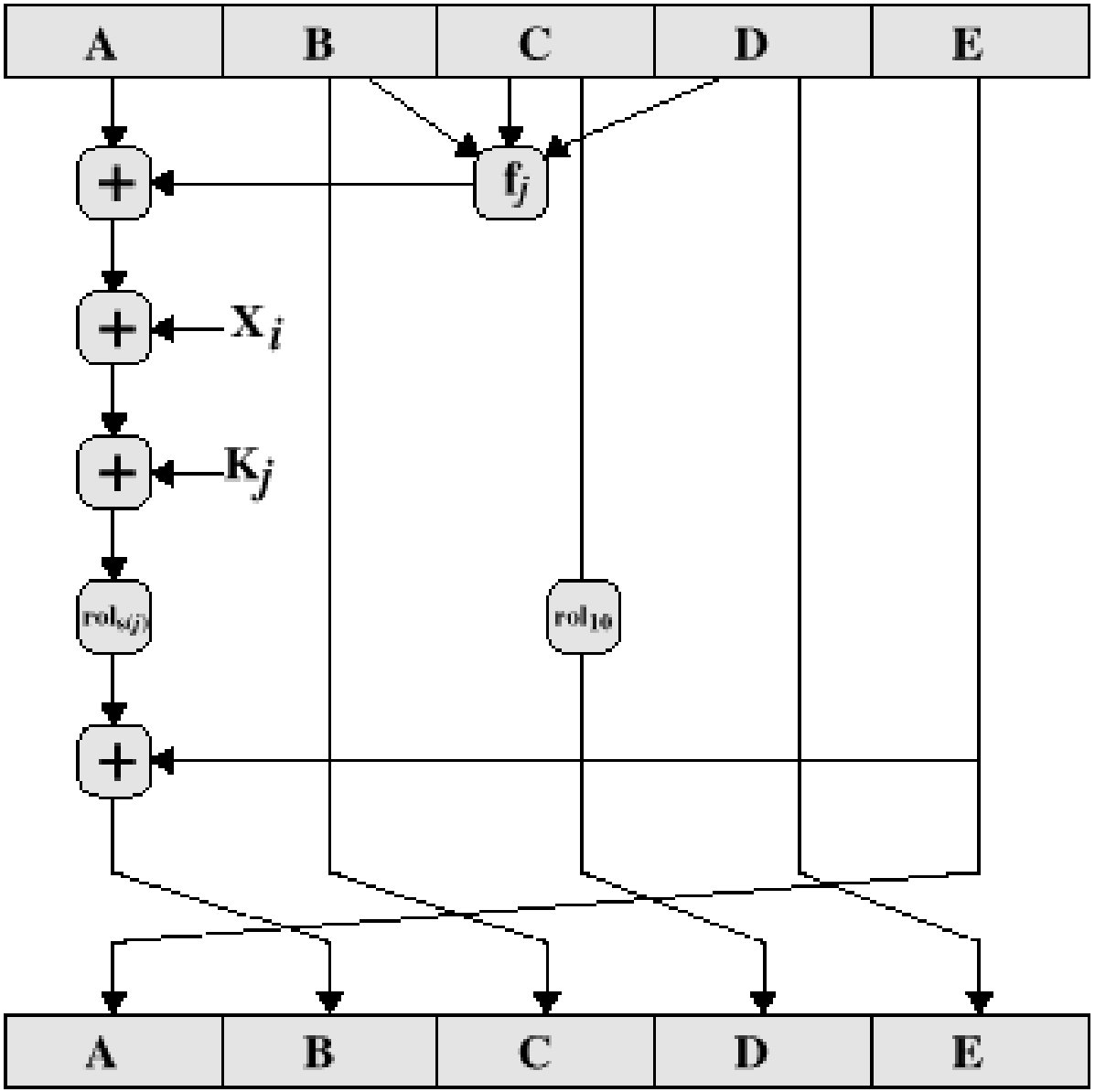
RIPEMD - 160

$K_1 = 0$
$K_2 = 2^{30} \times \sqrt{2}$
$K_3 = 2^{30} \times \sqrt{3}$
$K_4 = 2^{30} \times \sqrt{5}$
$K_5 = 2^{30} \times \sqrt{7}$

$K'_1 = 2^{30} \times \sqrt[3]{2}$
$K'_2 = 2^{30} \times \sqrt[3]{3}$
$K'_3 = 2^{30} \times \sqrt[3]{5}$
$K'_4 = 2^{30} \times \sqrt[3]{7}$
$K'_5 = 0$

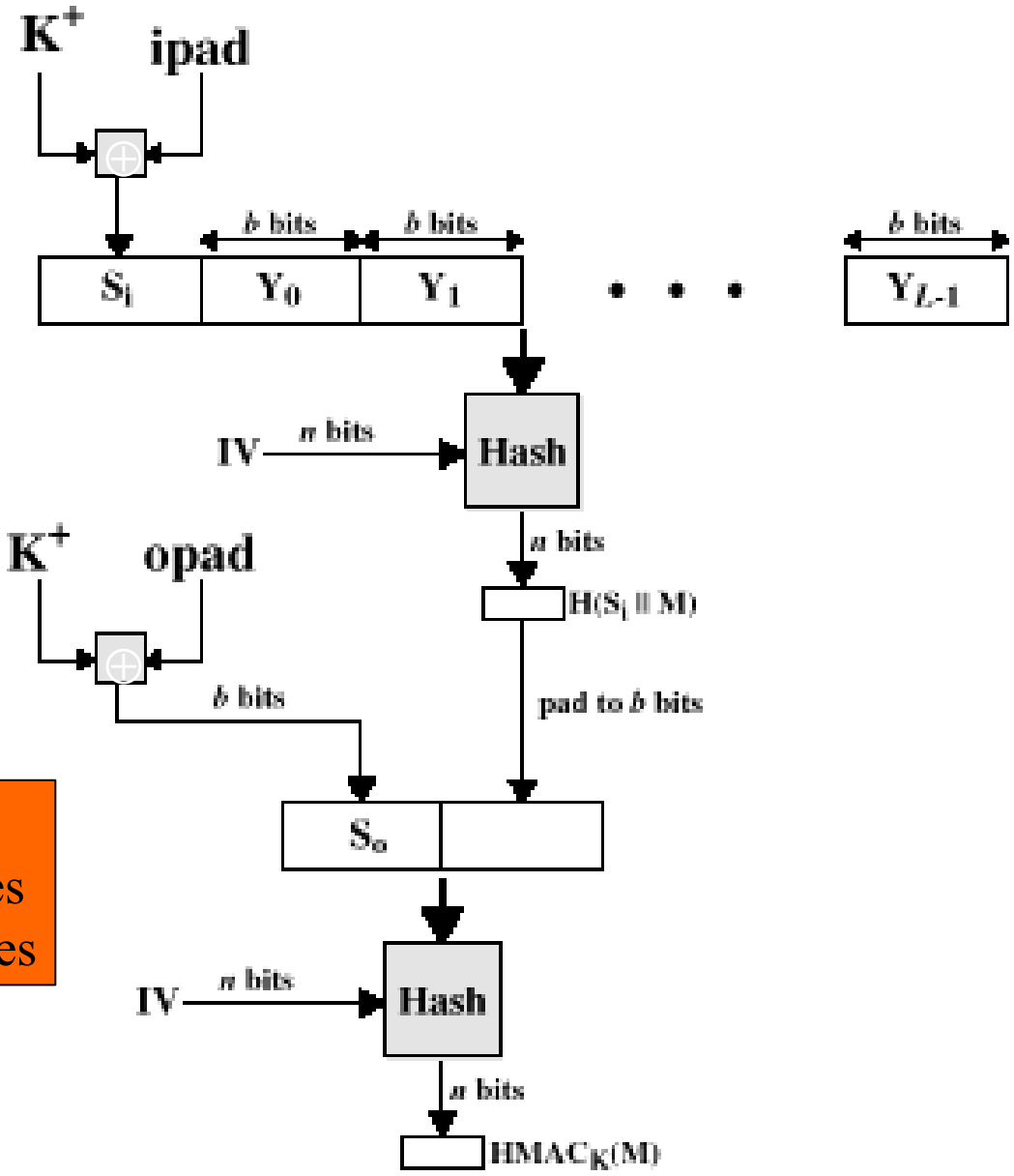


Um Passo



HMAC

FIPS PUB 113
RFC 2104
- MAC para IPsec
- SSL



K+ = K adicionado de zeros
ipad = 00110110 repetido b/8 vezes
opad = 01011100 repetido b/8 vezes

Implementação Eficiente