

Capítulo 12

Tabela 12.1 Comparação de parâmetros do SHA

	SHA-1	SHA-256	SHA-384	SHA-512
Tamanho do resumo de mensagem	160	256	384	512
Tamanho da mensagem	$<2^{64}$	$<2^{64}$	$<2^{128}$	$<2^{128}$
Tamanho do bloco	512	512	1024	1024
Tamanho da palavra (word)	32	32	64	64
Número de etapas	80	64	80	80
Segurança	80	128	192	256

Notas: 1. Todos os tamanhos são medidos em bits.

2. A segurança refere-se ao fato de que um ataque do aniversário a um resumo da mensagem de comprimento n produz uma colisão com um fator de trabalho de aproximadamente $2^{n/2}$.

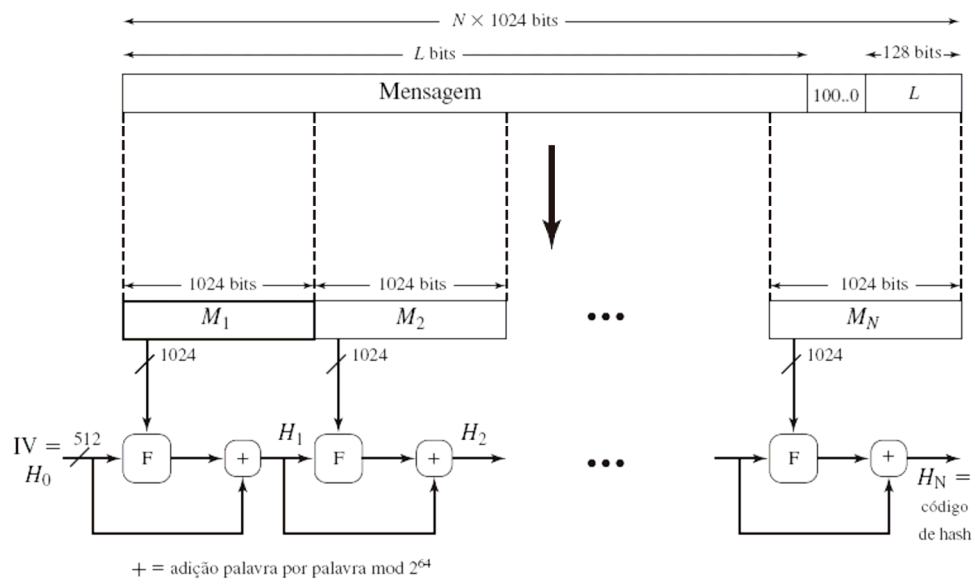


Figura 12.1 Geração de resumo da mensagem usando SHA-512.

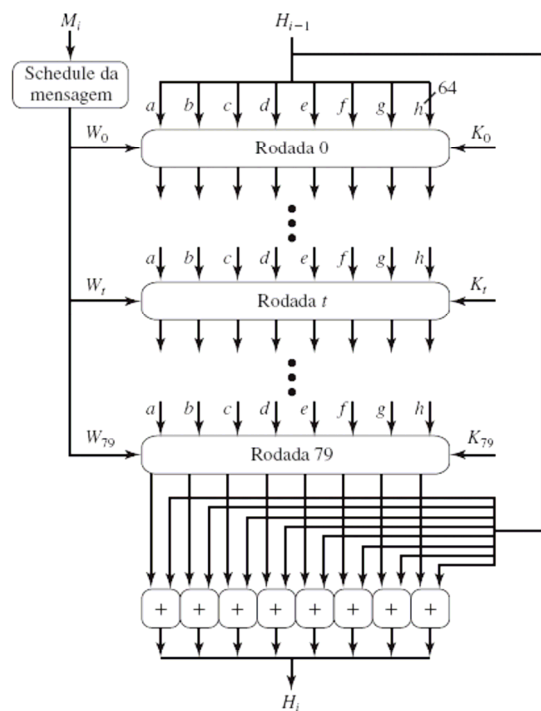


Figura 12.2 Processamento SHA-512 de um único bloco de 1.024 bits.

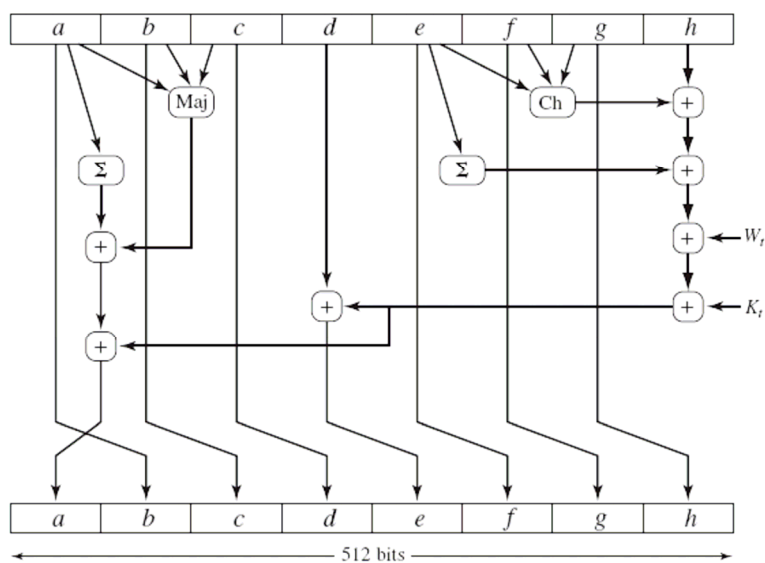


Figura 12.3 Operação elementar do SHA-512 (única rodada).

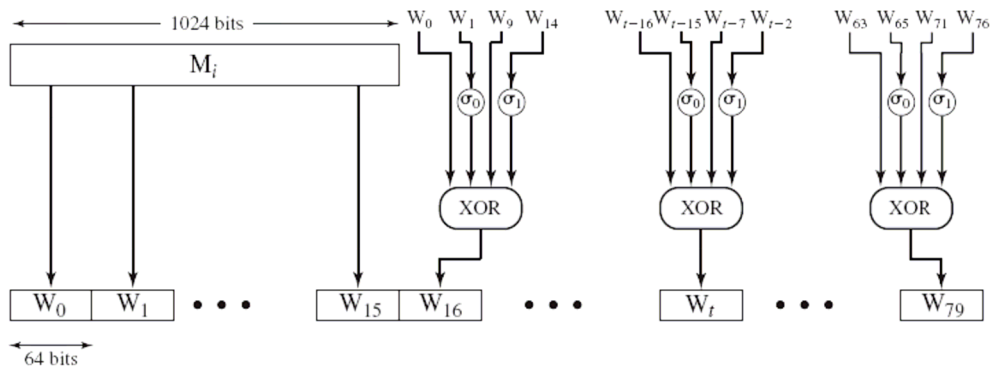
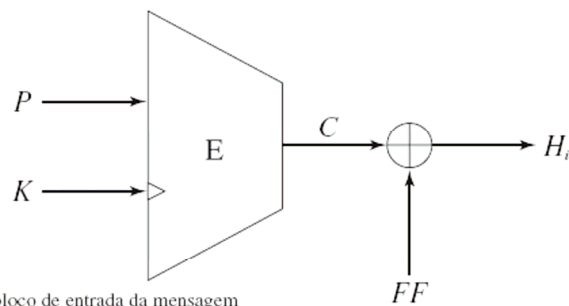


Figura 12.4 Criação da sequência de entrada de 80 palavras para processamento de único bloco do SHA-512.



m_i = i -ésimo bloco de entrada da mensagem
 H_i = i -ésimo valor de hash intermediário
 P = texto claro; K = chave de criptografia; C = texto cifrado
 FF = valor passado adiante
 P , K e FF podem ser escolhidos a partir do conjunto $(0, m_i, H_{i-1}, m_i \oplus H_{i-1})$

Observação: O triângulo indica a entrada da chave de criptografia.

Figura 12.5 Modelo da única iteração da função de hash (código de hash igual ao tamanho do bloco).

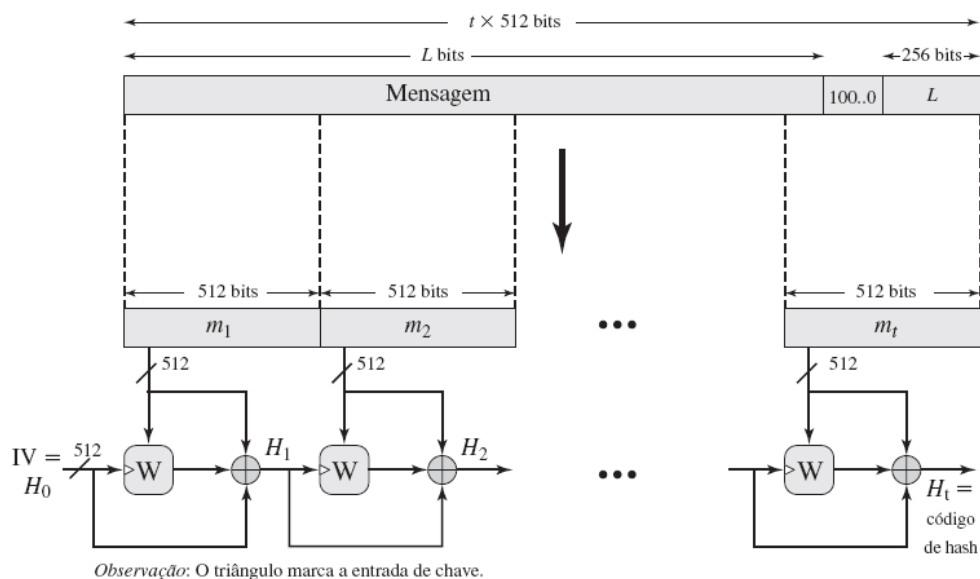


Figura 12.6 Geração de resumo da mensagem usando Whirlpool.

Tabela 12.2 Comparação da cifra de bloco do Whirlpool W e AES.

	W	AES
Tamanho do bloco (bits)	512	128
Tamanho da chave (bits)	512	128, 192 ou 256
Orientação da matriz	Entrada é mapeada por linha	Entrada é mapeada por coluna
Número de rodadas	10	10, 12 ou 14
Expansão de chave	Função de rodada W	Algoritmo de expansão dedicado
Polinômio $GF(2^8)$	$x^8 + x^4 + x^3 + x^2 + 1$ (011D)	$x^8 + x^4 + x^3 + x + 1$ (011B)
Origem da caixa-S	Estrutura recursiva	Inverso multiplicativo em $G(2^8)$ mais transformação afim
Origem das constantes da rodada	Entradas sucessivas de caixa-S	Elementos 2^i de $GF(2^8)$
Camada de difusão	Multiplicação à direita por matriz MDS circulante 8×8 (1, 1, 4, 1, 8, 5, 2, 9) – linhas mistas	Multiplicação à esquerda por matriz MDS circulante 4×4 (2, 3, 1, 1) – colunas mistas
Permutação	Deslocar colunas	Deslocar linhas

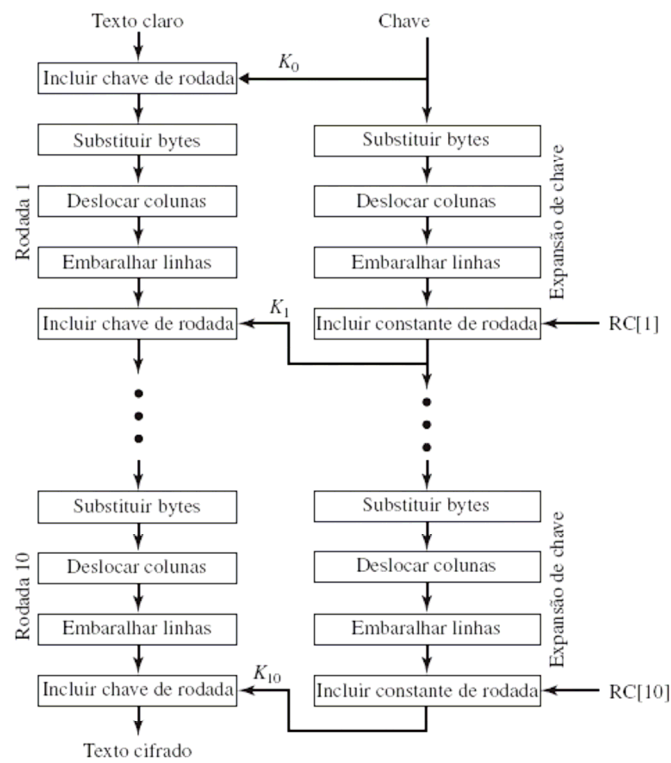


Figura 12.7 Cifra W do Whirlpool.

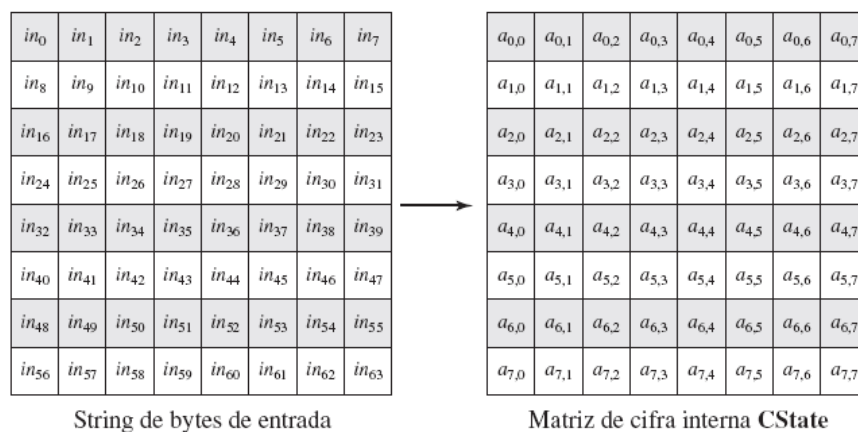


Figura 12.8 Estrutura de matriz do Whirlpool.

Tabela 12.3 Whirlpool Caixa-5.

(a) Caixa-S

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	18	23	C6	E8	87	B8	01	4F	36	A6	D2	F5	79	6F	91	52
1	60	BC	9B	8E	A3	0C	7B	35	1D	E0	D7	C2	2E	4B	FE	57
2	15	77	37	E5	9F	F0	4A	CA	58	C9	29	0A	B1	A0	6B	85
3	BD	5D	10	F4	CB	3E	05	67	E4	27	41	8B	A7	7D	95	C8
4	FB	EE	7C	66	DD	17	47	9E	CA	2D	BF	07	AD	5A	83	33
5	63	02	AA	71	C8	19	49	C9	F2	E3	5B	88	9A	26	32	B0
6	E9	0F	D5	80	BE	CD	34	48	FF	7A	90	5F	20	68	1A	AE
7	B4	54	93	22	64	F1	73	12	40	08	C3	EC	DB	A1	8D	3D
8	97	00	CF	2B	76	82	D6	1B	B5	AF	6A	50	45	F3	30	EF
9	3F	55	A2	EA	65	BA	2F	C0	DE	1C	FD	4D	92	75	06	8A
A	B2	E6	0E	1F	62	D4	A8	96	F9	C5	25	59	84	72	39	4C
B	5E	78	38	8C	C1	A5	E2	61	B3	21	9C	1E	43	C7	FC	04
C	51	99	6D	0D	FA	DF	7E	24	3B	AB	CE	11	8F	4E	B7	EB
D	3C	81	94	F7	B9	13	2C	D3	E7	6E	C4	03	56	44	7F	A9
E	2A	BB	C1	53	DC	0B	9D	6C	31	74	F6	46	AC	89	14	E1
F	16	3A	69	09	70	B6	C0	ED	CC	42	98	A4	28	5C	F8	86

(b) E mini-box

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$E(u)$	1	B	9	C	D	6	F	3	E	8	7	4	A	2	5	0

(c) E^{-1} mini-box

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$E^{-1}(u)$	F	0	D	7	B	E	5	A	9	2	C	1	3	4	8	6

(d) R mini-box

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$R(u)$	7	C	B	D	E	4	9	F	6	3	8	A	2	5	1	0

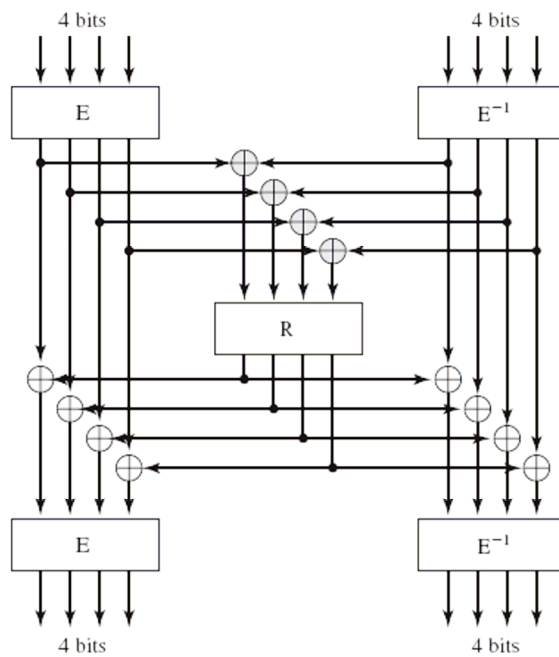


Figura 12.9 Implementação da caixa-S do Whirlpool.

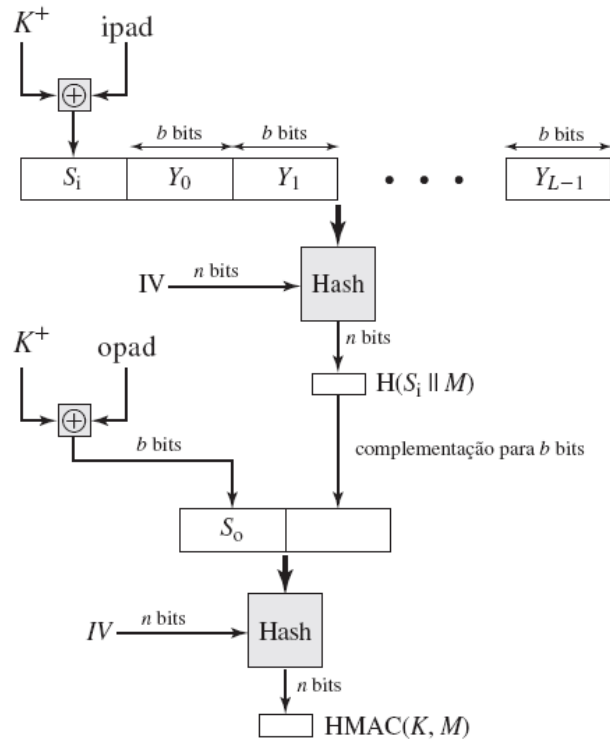


Figura 12.10 Estrutura do HMAC.

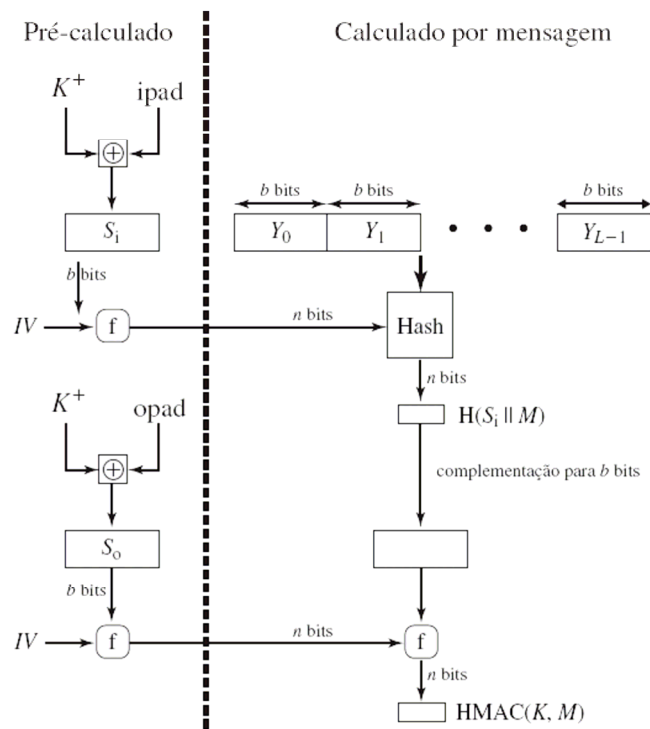


Figura 12.11 Implementação eficiente do HMAC.

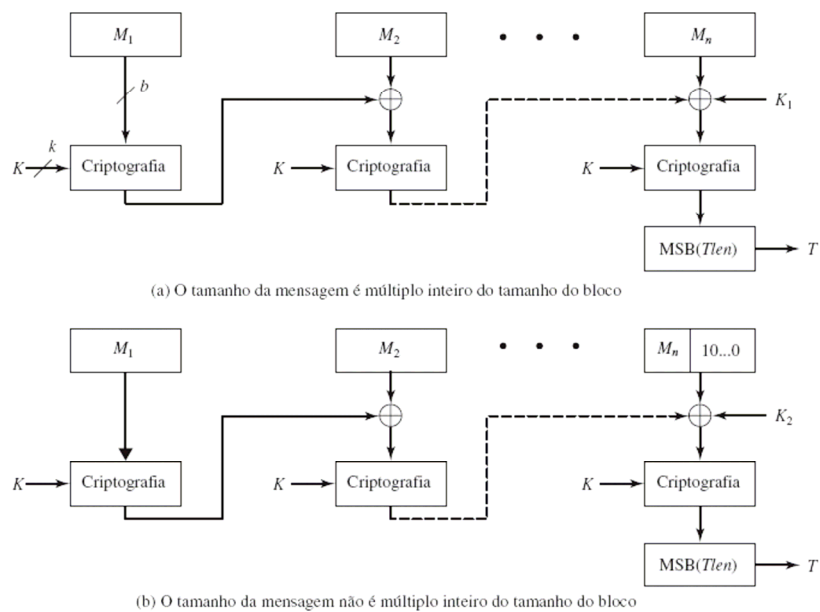


Figura 12.12 Cipher-based message authentication code (CMAC).