Capítulo 11

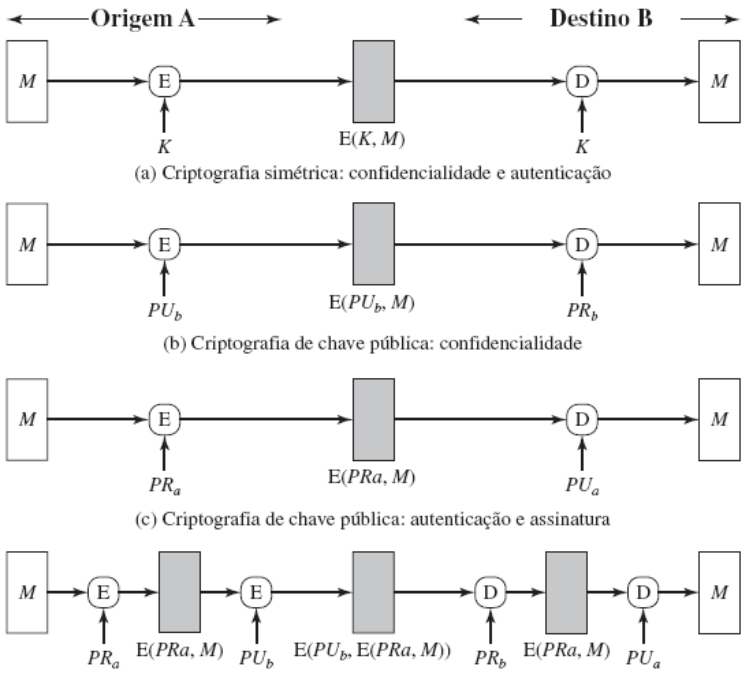


Figura 11.1 Usos básicos da criptografia de mensagens.

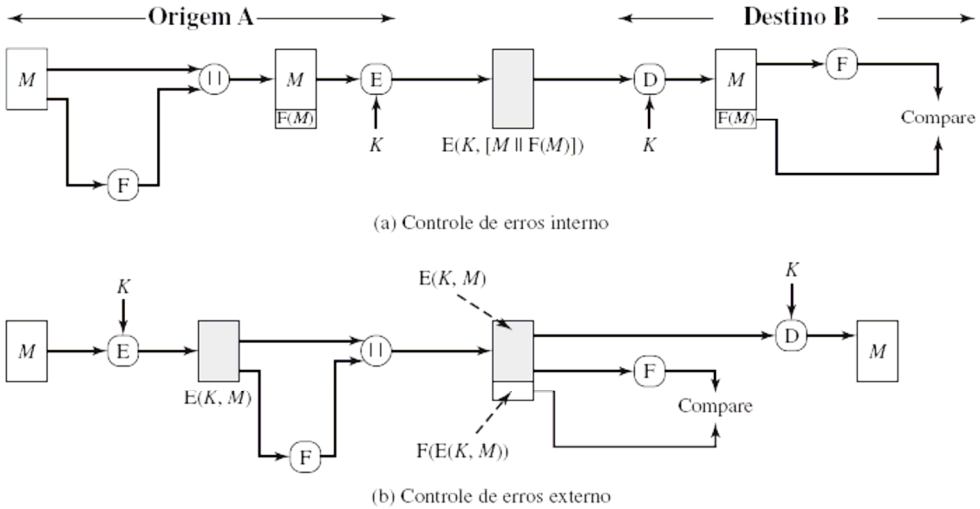


Figura 11.2 Controle de erros interno e externo.

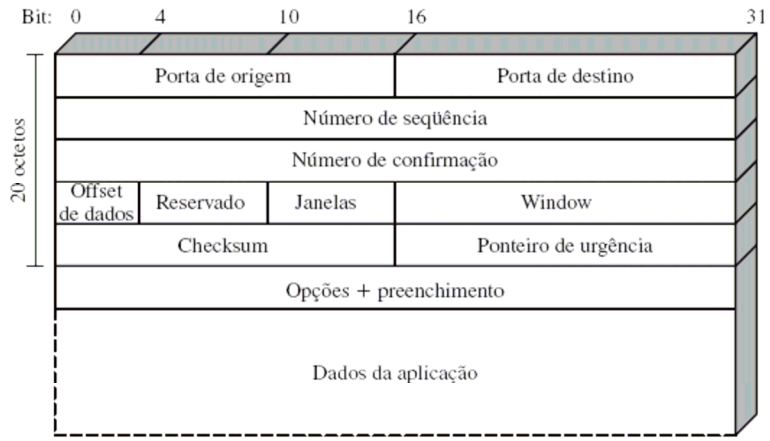


Figura 11.3 Segmento TCP.

Tabela 11.1 Conseqüências de confidencialidade e autenticação da criptografia da mensagem (ver Figura 11.1)

$A \rightarrow B: E(K, M)$
• Oferece confidencialidade — somente A e B compartilham K
• Oferece um grau de autenticação — Só poderia vir de A — Não foi alterada em trânsito — Requer alguma formatação/redundância
• Não oferece assinatura — Receptor poderia forjar mensagem — Emissor poderia negar mensagem

(a) Criptografia simétrica

$A \rightarrow B: E(PU_b, M)$
• Oferece confidencialidade — Somente B tem PR_b para decriptografar
• Não oferece autenticação — Qualquer parte poderia usar PU_b para criptografar a mensagem e afirmar ser A

(b) Criptografia de chave pública (simétrica): confidencialidade

$A \rightarrow B: E(PR_a, M)$
• Oferece autenticação e assinatura — Somente A tem PR_a para criptografar — Não foi alterada em trânsito — Requer alguma formatação/redundância — Qualquer parte pode usar PU_a para verificar a assinatura

(c) Criptografia de chave pública: autenticação e assinatura

$A \rightarrow B: E(PU_b, E(PR_a, M))$
• Oferece confidencialidade por causa de PU_b
• Oferece autenticação e assinatura por causa de PR_a

(d) Criptografia de chave pública: confidencialidade, autenticação e assinatura

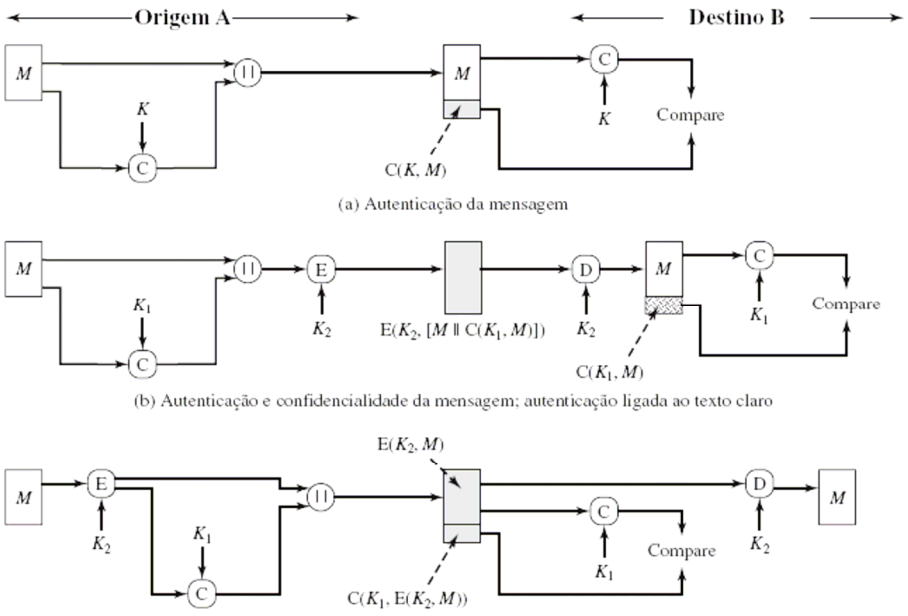


Figura 11.4 Usos básicos do código de autenticação de mensagens (MAC).

Tabela 11.2 Usos básicos do código de autenticação de mensagens C (ver Figura 11.4)

$A \rightarrow B: M \| C(K, M)$ • Oferece autenticação — Somente A e B compartilham K

(a) Autenticação da mensagem

$A \rightarrow B: E(K_2, [M \| C(K, M)])$ • Oferece autenticação — Somente A e B compartilham K_1 • Oferece confidencialidade — Somente A e B compartilham K_2

(b) Autenticação e confidencialidade da mensagem: autenticação ligada ao texto claro

$A \rightarrow B: E(K_2, M) \| C(K_1, E(K_2, M))$ • Oferece autenticação — Usando K_1 • Oferece confidencialidade — Usando K_2

(c) Autenticação e confidencialidade da mensagem: autenticação ligada ao texto cifrado

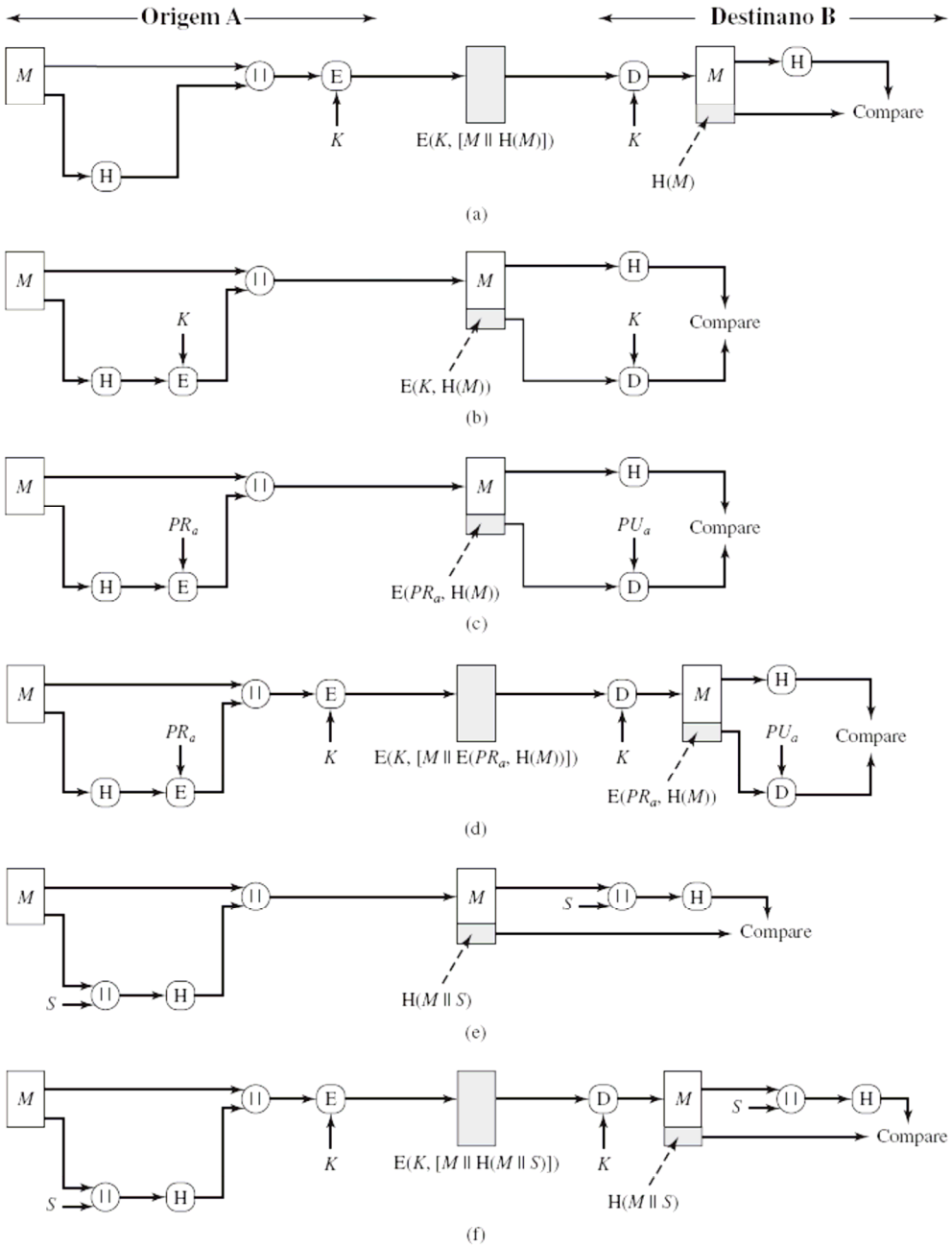


Figura 11.5 Usos básicos da função de hash.

Tabela 11.3 Usos básicos da função de hash H (ver Figura 11.5).

A → B: E(K, [M‖H(M)])	A → B: E(K, [M‖E(PR_a, H(M))])
• Oferece confidencialidade Somente A e B compartilham K	• Oferece autenticação e assinatura digital • Oferece confidencialidade — Somente A e B compartilham K
• Oferece autenticação — H(M) é protegido criptograficamente	
(a) Criptografia de mensagem mais código de hash	(d) Criptografia do resultado de (c) — chave secreta compartilhada
A → B: M‖E(K, H(M))	A → B: M‖H(M‖S)
• Oferece autenticação — H(M) é criptograficamente protegido	• Oferece autenticação — Somente A e B compartilham S
(b) Criptografia do código de hash — chave secreta compartilhada	(e) Cálculo do código de hash da mensagem mais o valor secreto
A → B: M‖E(PR_a, H(M))	A → B: E(K, [M‖H(M‖S])
• Oferece autenticação e assinatura digital — H(M) é criptograficamente protegido — Somente A poderia criar E(PR_a,H(M))	• Oferece autenticação — Somente A e B compartilham S • Oferece confidencialidade — Somente A e B compartilham K
(c) Criptografia do código de hash — chave privada do emissor	(f) Encrypt result of (e) Criptografia do resultado de (e)

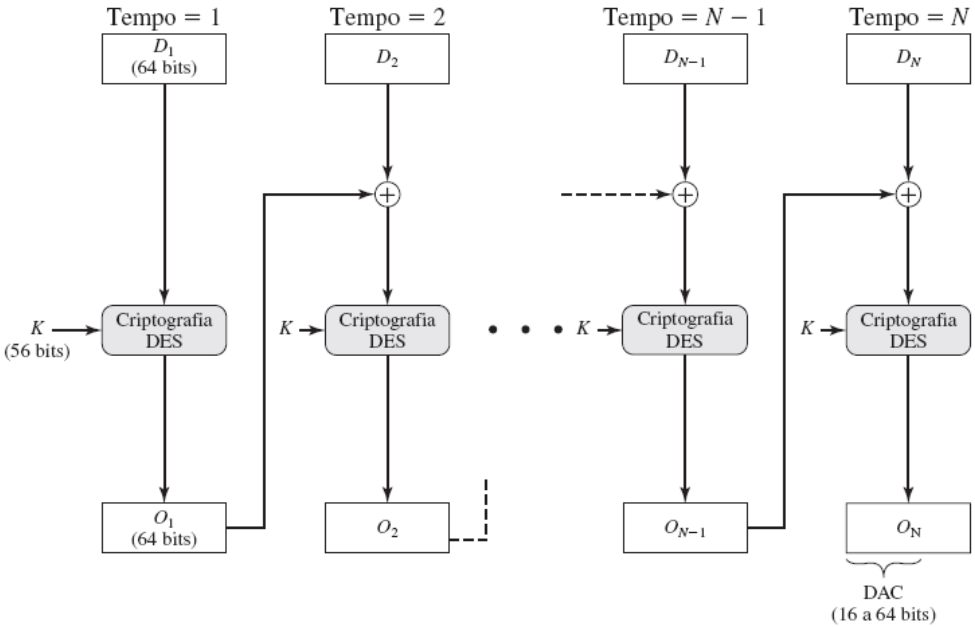


Figura 11.6 Algoritmo de autenticação de dados (FIPS PUB 113).

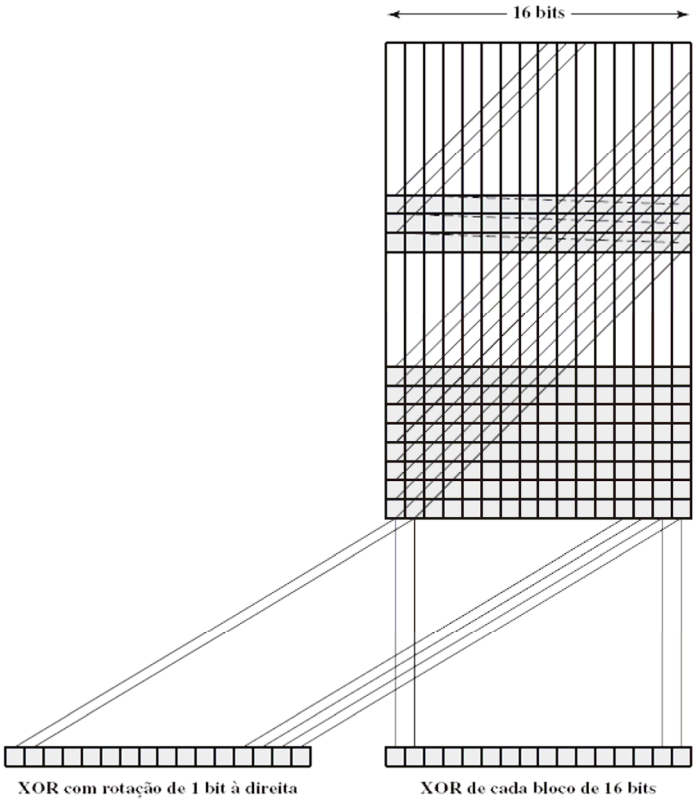


Figura 11.7 Duas funções de hash simples.

Dear Anthony,

{This letter is / I am writing} to introduce {you to / to you} {Mr. / --} Alfred {P. / --}

Barton, the {new / newly appointed} {chief / senior} jewellery buyer for {our / the}

Northern {European / Europe} {area / division}. He {will take / has taken} over {the / --}

responsibility for {all / the whole of} our interests in {watches and jewellery / jewellery and watches}

in the {area / region}. Please {afford / give} him {every / all the} help he {may need / needs}

to {seek out / find} the most {modern / up to date} lines for the {top / high} end of the

market. He is {empowered / authorized} to receive on our behalf {samples / specimens} of the

{latest / newest} {watch and jewellery / jewellery and watch} products, {up / subject} to a {limit / maximum}

of ten thousand dollars. He will {carry / hold} a signed copy of this {letter / document}

as proof of identity. An order with his signature, which is {appended / attached}

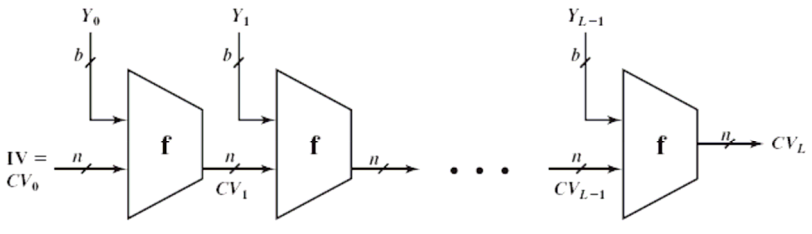
{authorizes / allows} you to charge the cost to this company at the {above / head office}

address. We {fully / --} expect that our {level / volume} of orders will increase in

the {following / next} year and {trust / hope} that the new appointment will {be / prove}

{advantageous / an advantage} to both our companies.

Figura 11.8 Uma carta com 2^{37} variações [DAVI89].



IV = valor inicial
CV_i = Variável de encadeamento
Y_i = i-ésimo bloco de entrada
f = Função de compressão
L = Número de blocos de entrada
n = Comprimento do código de hash
b = Comprimento do bloco de entrada

Figura 11.9 Estrutura geral do código de hash seguro.

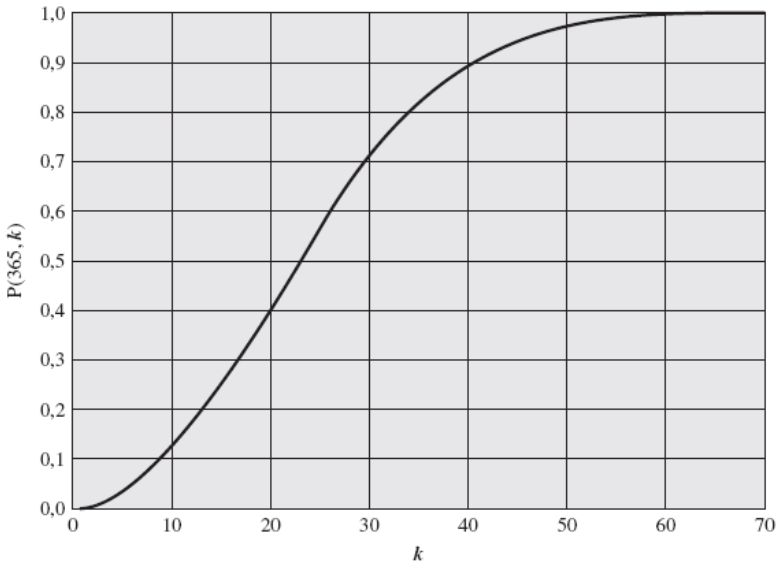


Figura 11.10 O paradoxo do aniversário.

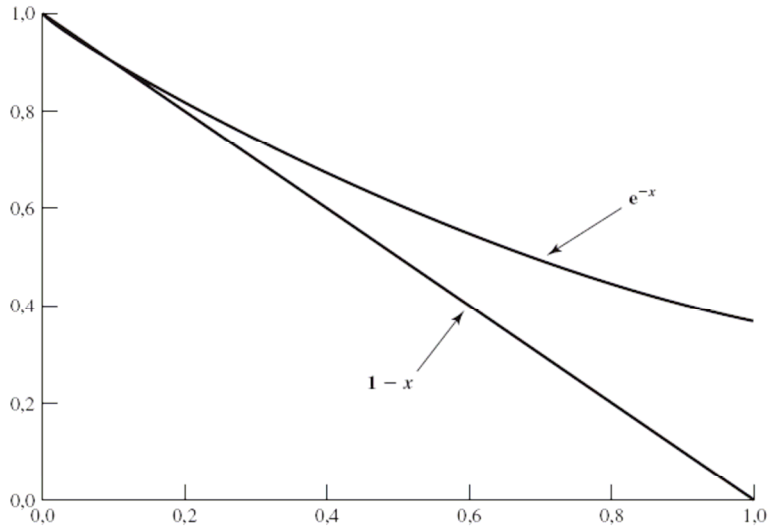


Figura 11.11 Uma desigualdade útil.