

# Capítulo 11

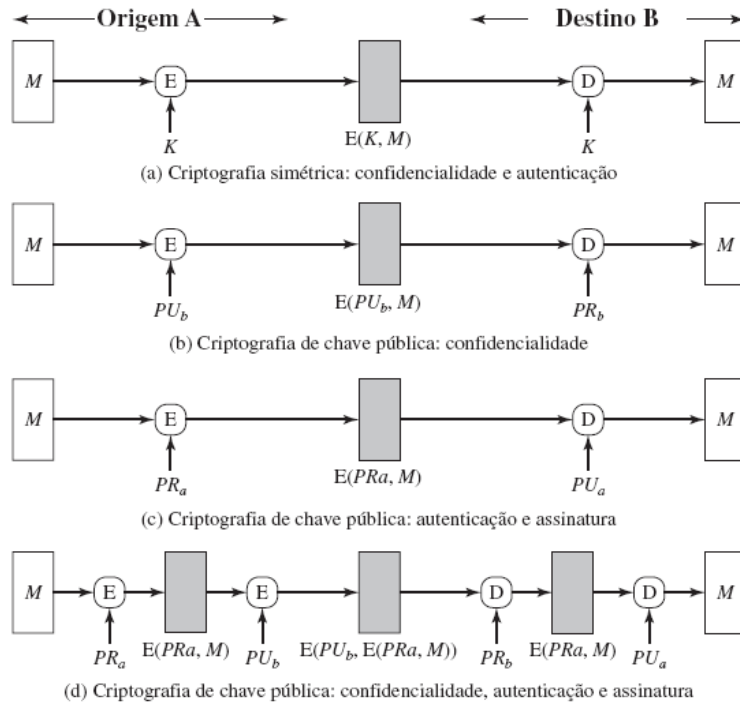


Figura 11.1 Usos básicos da criptografia de mensagens.

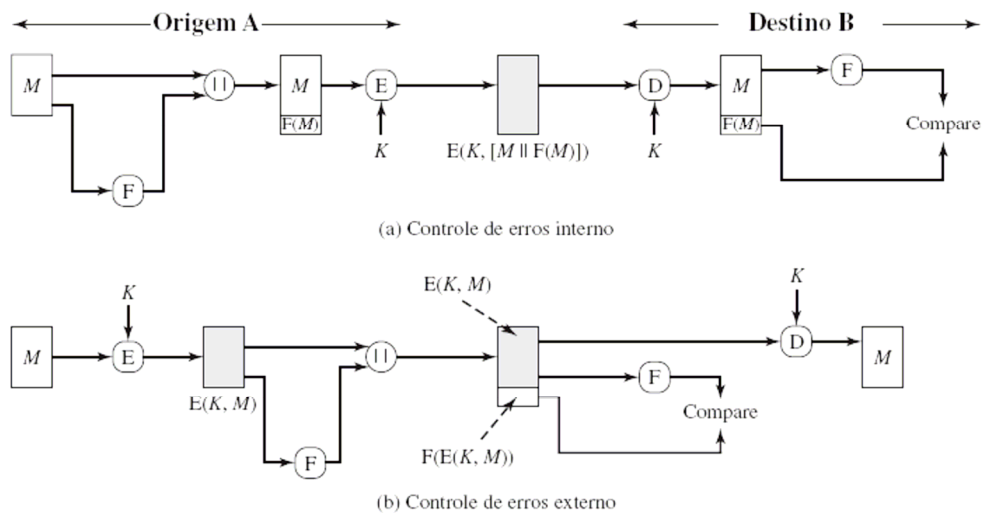


Figura 11.2 Controle de erros interno e externo.

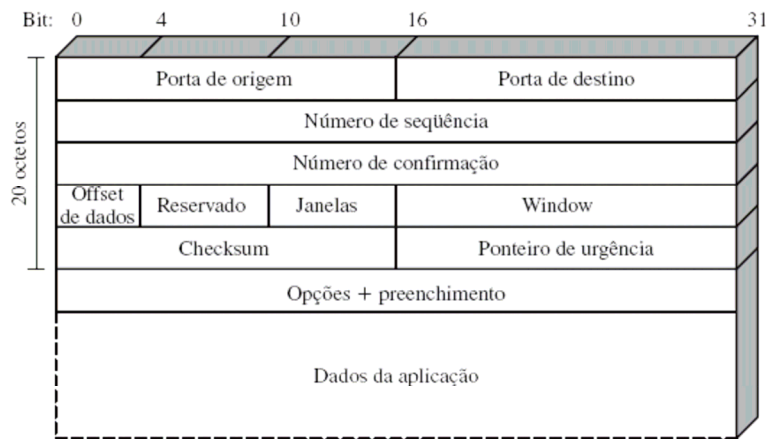


Figura 11.3 Segmento TCP.

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 decryptografar
- 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

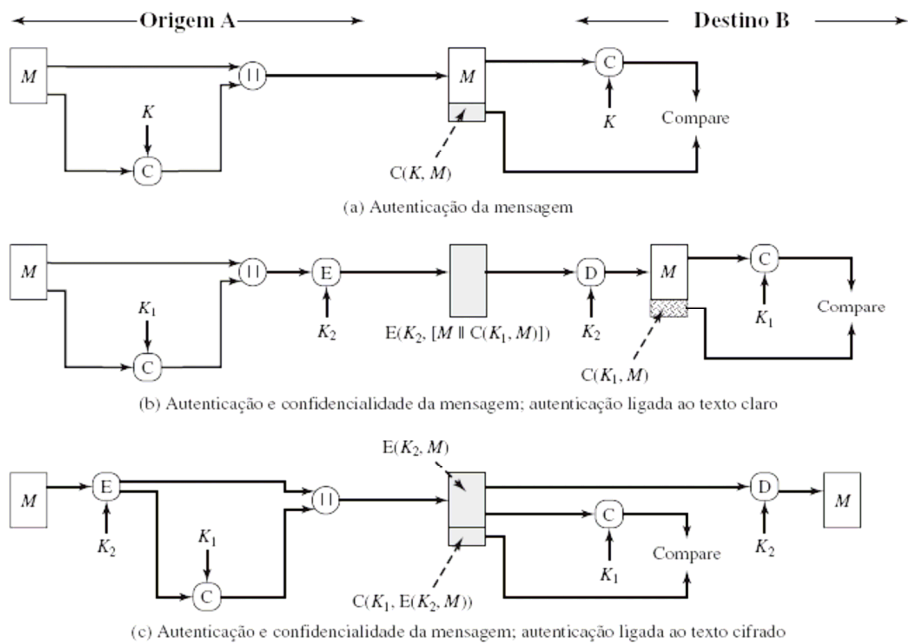


Figura 11.4 Usos básicos do código de autenticação de mensagens (MAC).

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

$A \rightarrow B: E(K_2, [M \| C(K_1, M)])$

- 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

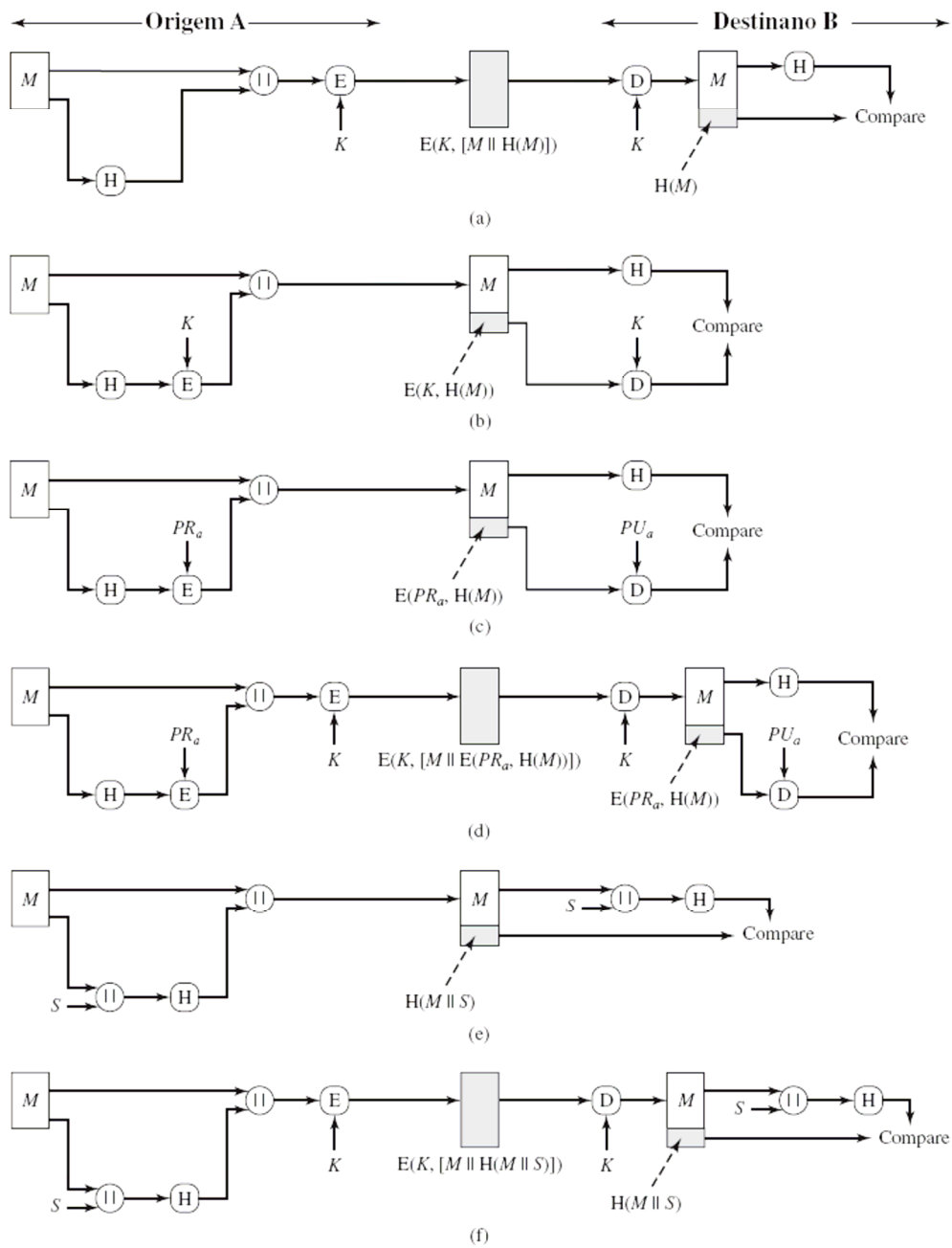


Figura 11.5 Usos básicos da função de hash.

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

$A \rightarrow B: E(K, [M  H(M)])$ <ul style="list-style-type: none"> <li>• Oferece confidencialidade</li> <li>— Somente A e B compartilham <math>K</math></li> <li>• Oferece autenticação</li> <li>— <math>H(M)</math> é protegido criptograficamente</li> </ul>	$A \rightarrow B: E(K, [M  E(PR_s, H(M))])$ <ul style="list-style-type: none"> <li>• Oferece autenticação e assinatura digital</li> <li>• Oferece confidencialidade</li> <li>— Somente A e B compartilham <math>K</math></li> </ul>
(a) Criptografia de mensagem mais código de hash	(d) Criptografia do resultado de (c) — chave secreta compartilhada
$A \rightarrow B: M  E(K, H(M))$ <ul style="list-style-type: none"> <li>• Oferece autenticação</li> <li>— <math>H(M)</math> é criptograficamente protegido</li> </ul>	$A \rightarrow B: M  H(M  S)$ <ul style="list-style-type: none"> <li>• Oferece autenticação</li> <li>— Somente A e B compartilham <math>S</math></li> </ul>
(b) Criptografia do código de hash — chave secreta compartilhada	(e) Cálculo do código de hash da mensagem mais o valor secreto
$A \rightarrow B: M  E(PR_s, H(M))$ <ul style="list-style-type: none"> <li>• Oferece autenticação e assinatura digital</li> <li>— <math>H(M)</math> é criptograficamente protegido</li> <li>— Somente A poderia criar <math>E(PR_s, H(M))</math></li> </ul>	$A \rightarrow B: E(K, [M  H(M  S)])$ <ul style="list-style-type: none"> <li>• Oferece autenticação</li> <li>— Somente A e B compartilham <math>S</math></li> <li>• Oferece confidencialidade</li> <li>— Somente A e B compartilham <math>K</math></li> </ul>
(c) Criptografia do código de hash — chave privada do emissor	(f) Encrypt result of (e) Criptografia do resultado de (e)

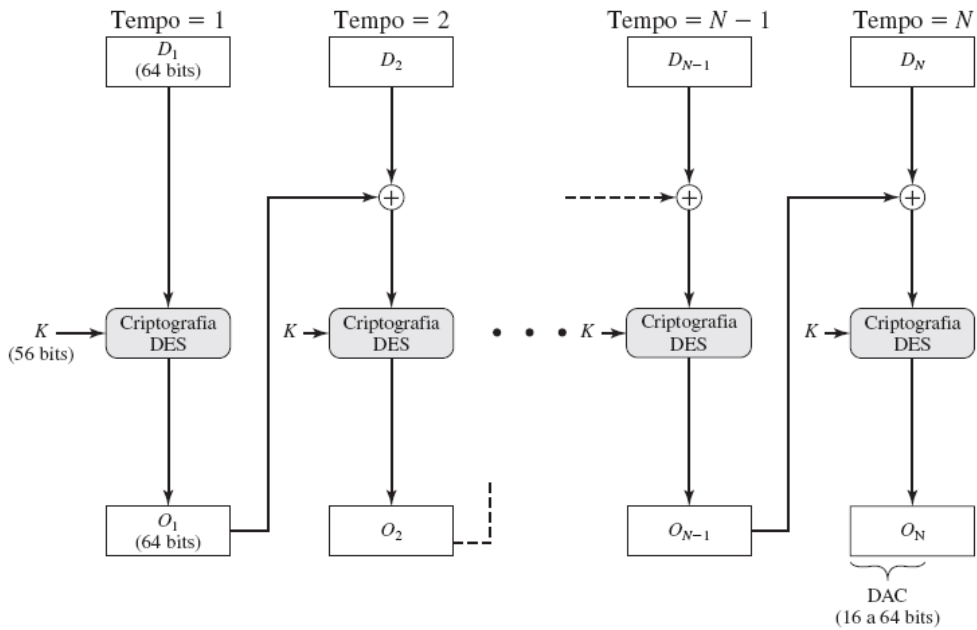


Figura 11.6 Algoritmo de autenticação de dados (FIPS PUB 113).

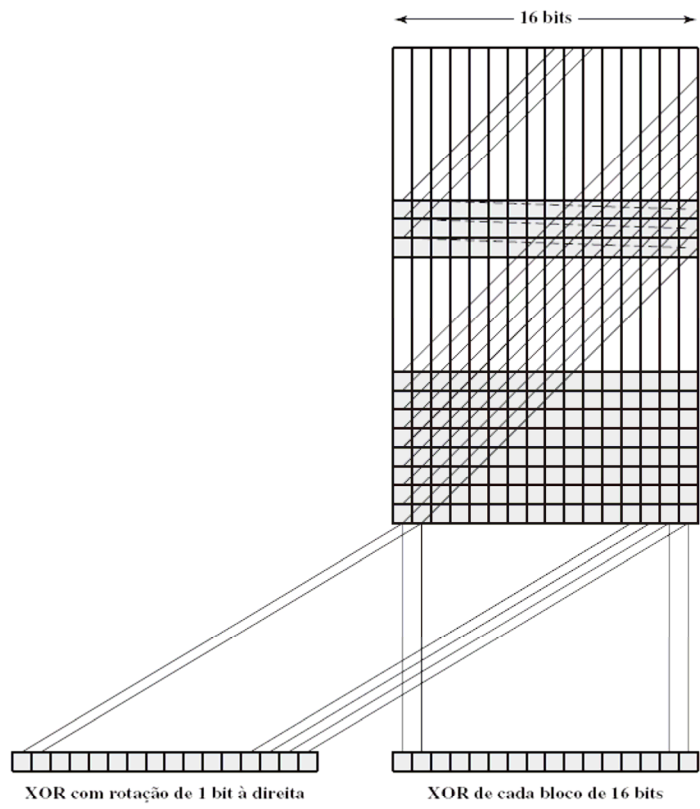


Figura 11.7 Duas funções de hash simples.

Dear Anthony,

{ This letter is } to introduce { you to } { Mr. } Alfred { P. }  
 { I am writing } { to you } { -- }  
 Barton, the { new } { chief } jewellery buyer for { our }  
 { newly appointed } { senior } { the }  
 Northern { European } { area } . He { will take } over { the }  
 { Europe } { division } { has taken } { -- }  
 responsibility for { all } our interests in { watches and jewellery }  
 { the whole of } { jewellery and watches }  
 in the { area } . Please { afford } him { every } help he { may need }  
 { region } { give } { all the } { needs }  
 to { seek out } the most { modern } lines for the { top } end of the  
 { find } { up to date } { high }  
 market. He is { empowered } to receive on our behalf { samples } of the  
 { authorized } { specimens }  
 { latest } { watch and jewellery } products, { up } to a { limit }  
 { newest } { jewellery and watch } { subject } { maximum }  
 of ten thousand dollars. He will { carry } a signed copy of this { letter }  
 { hold } { document }  
 as proof of identity. An order with his signature, which is { appended }  
 { attached }  
 { authorizes } you to charge the cost to this company at the { above }  
 { allows } { head office }  
 address. We { fully } expect that our { level } of orders will increase in  
 { -- } { volume }  
 the { following } year and { trust } that the new appointment will { be }  
 { next } { hope } { prove }  
 { advantageous } to both our companies.  
 { an advantage }

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

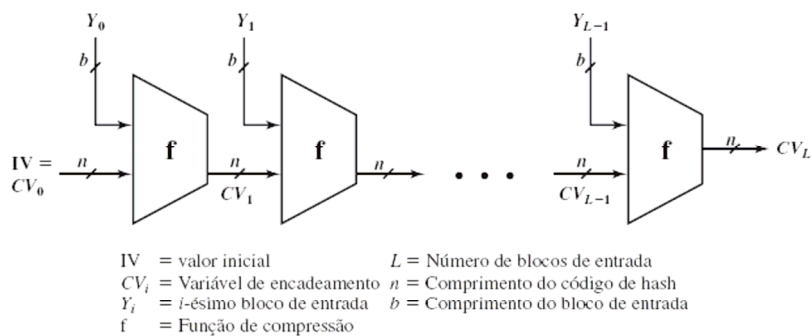


Figura 11.9 Estrutura geral do código de hash seguro.



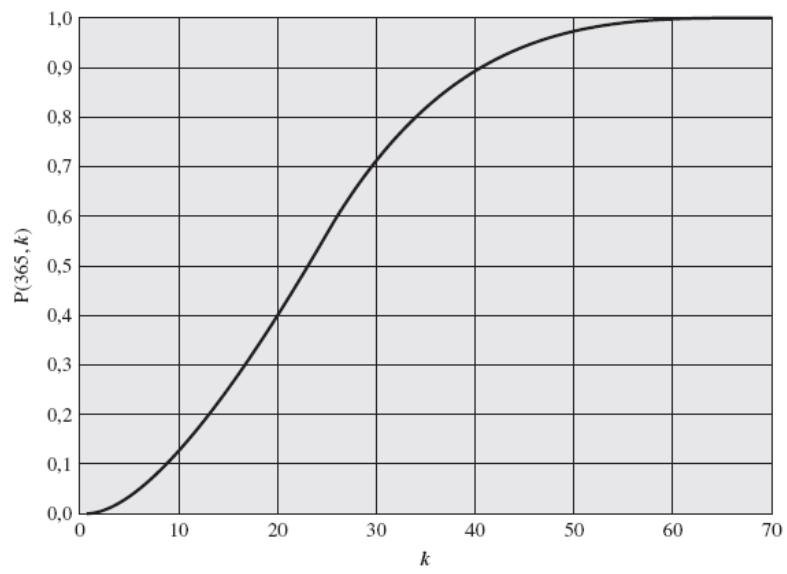


Figura 11.10 O paradoxo do aniversário.

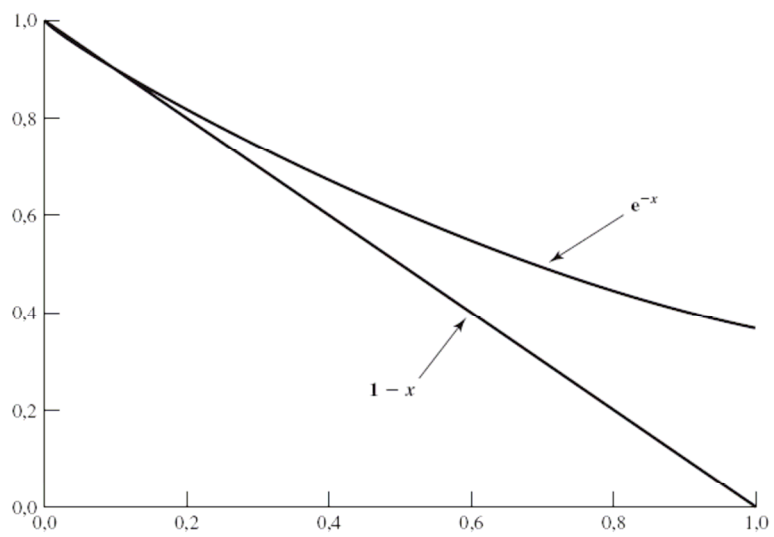


Figura 11.11 Uma desigualdade útil.