

## Capítulo 13

Tabela 13.1 Técnicas de assinatura digital arbitrada

- (1)  $X \rightarrow A: M \| E(K_{xa}, [ID_X \| H(M)])$   
 (2)  $A \rightarrow Y: E(K_{ay}, [ID_X \| M \| E(K_{xa}, [ID_X \| H(M)]) \| T])$

(a) Criptografia convencional, árbitro vê mensagem

- (1)  $X \rightarrow A: ID_X \| E(K_{xy}, M) \| E(K_{xa}, [ID_X \| H(E(K_{xy}, M))])$   
 (2)  $A \rightarrow Y: E(K_{ay}, [ID_X \| E(K_{xy}, M)]) \| E(K_{xa}, [ID_X \| H(E(K_{xy}, M)) \| T])$

(b) Criptografia convencional, árbitro não vê mensagem

- (1)  $X \rightarrow A: ID_X \| E(PR_x, [ID_X \| E(PU_y, E(PR_x, M))])$   
 (2)  $A \rightarrow Y: E(PR_a, [ID_X \| E(PU_y, E(PR_x, M)) \| T])$

(c) Criptografia de chave pública, árbitro não vê mensagem

Legenda

X = emissor  
 Y = receptor

A = Árbitro  
 M = Mensagem  
 T = Carimbo de tempo

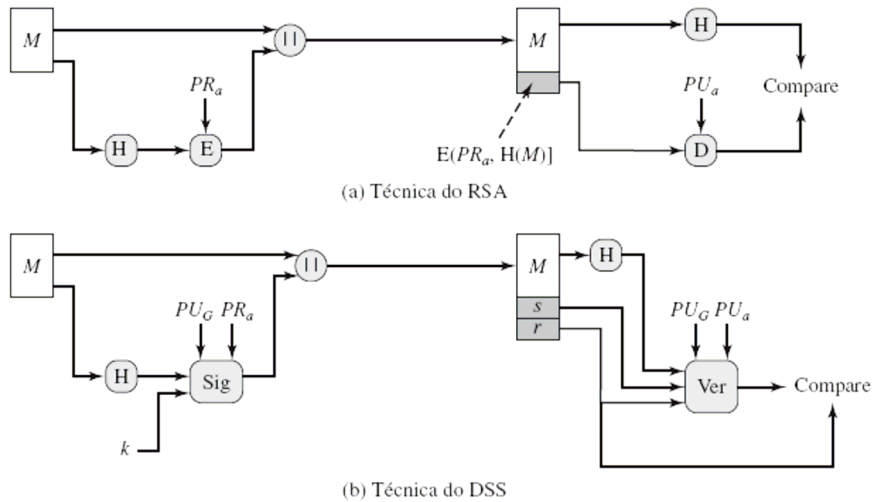


Figura 13.1 Duas técnicas para assinaturas digitais.

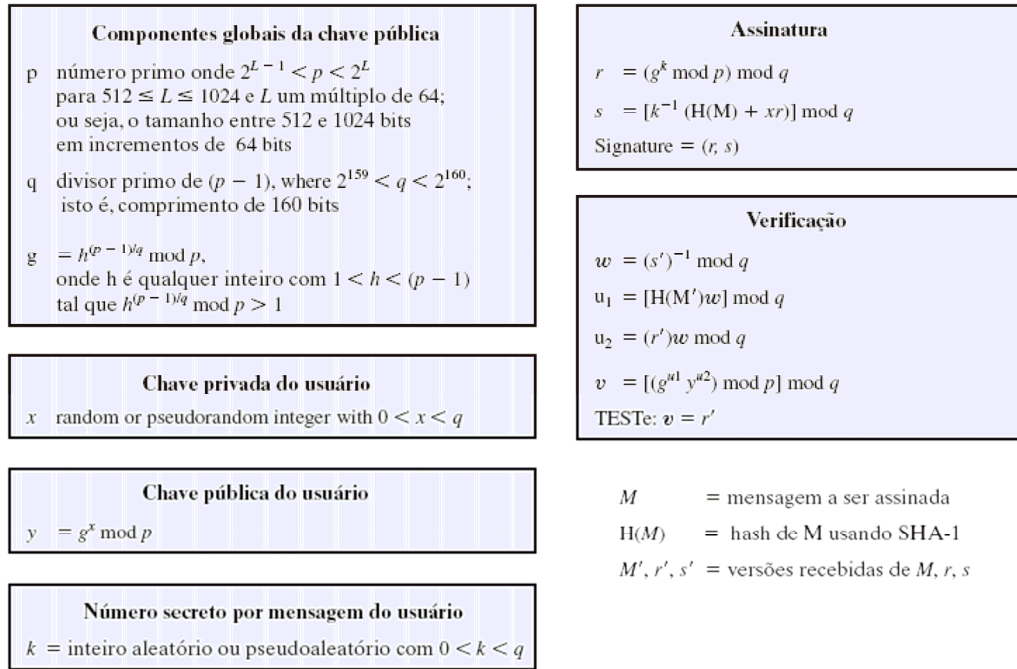


Figura 13.2 O algoritmo de assinatura digital (DSA).

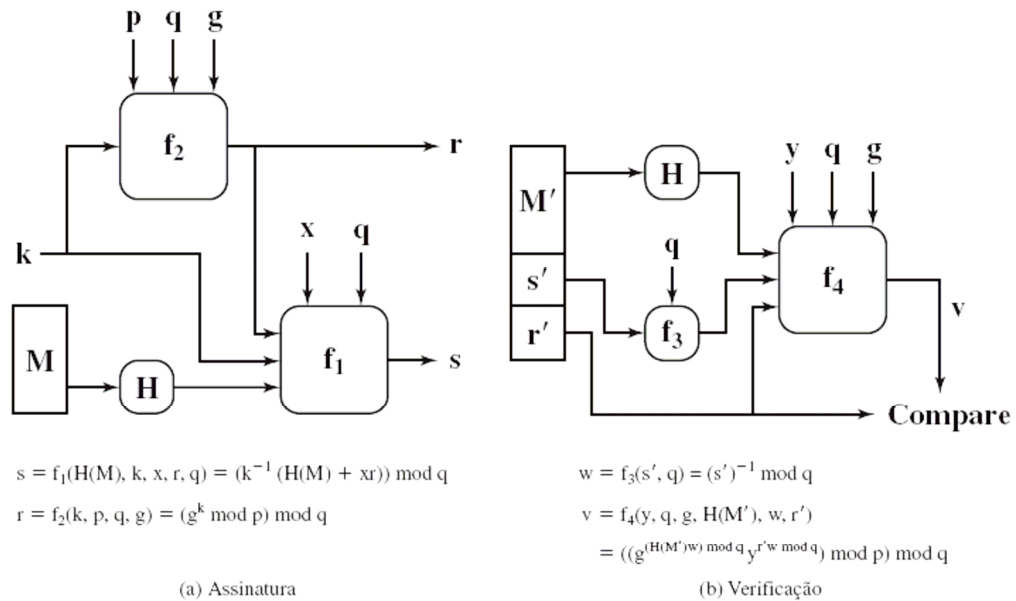


Figura 13.3 Assinatura e verificação do DSS.