Capítulo 13

Tabela 13.1 Técnicas de assinatura digital arbitrada

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

(a) Criptografia convencional, árbitro vê mensagem

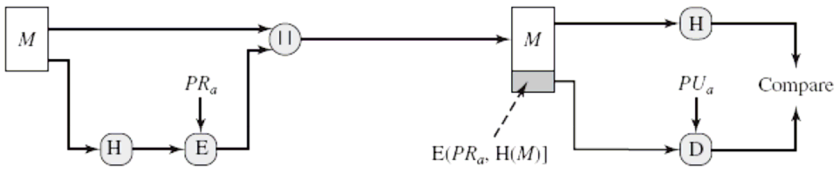
(1) X → A: $ID_X \| \mathrm{E}(K_{xy}, M) \| \mathrm{E}(K_{xa}, [ID_X \| \mathrm{H}(\mathrm{E}(K_{xy}, M))])$ **(2)** A → Y: $\mathrm{E}(K_{ay}, [ID_X \| \mathrm{E}(K_{xy}, M)]) \| \mathrm{E}(K_{xa}, [ID_X \| \mathrm{H}(\mathrm{E}(K_{xy}, M)) \| T])$

(b) Criptografia convencional, árbitro não vê mensagem

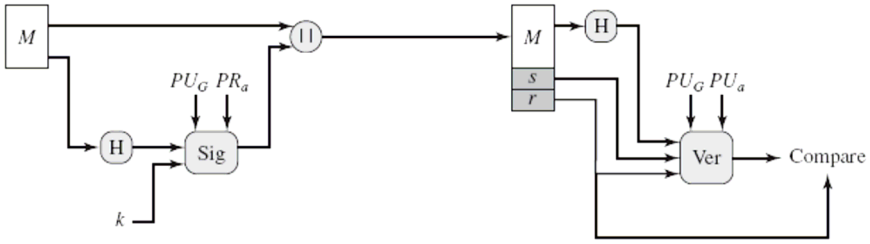
(1) X → A: $ID_X \| \mathrm{E}(PR_x, [ID_X \| \mathrm{E}(PU_y, \mathrm{E}(PR_x, M))])$ **(2)** A → Y: $\mathrm{E}(PR_a, [ID_X \| \mathrm{E}(PU_y, \mathrm{E}(PR_x, M)) \| T])$

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

Legenda
X = emissor
Y = receptor
A = Árbitro
M = Mensagem
T = Carimbo de tempo



(a) Técnica do RSA



(b) Técnica do DSS

Figura 13.1 Duas técnicas para assinaturas digitais.

Componentes globais da chave pública

p número primo onde $2^{L-1} < p < 2^L$
para $512 \leq L \leq 1024$ e L um múltiplo de 64;
ou seja, o tamanho entre 512 e 1024 bits
em incrementos de 64 bits

q divisor primo de $(p - 1)$, where $2^{159} < q < 2^{160}$;
isto é, comprimento de 160 bits

g $= h^{(p-1)/q} \bmod p$,
onde h é qualquer inteiro com $1 < h < (p - 1)$
tal que $h^{(p-1)/q} \bmod p > 1$

Chave privada do usuário

x random or pseudorandom integer with $0 < x < q$

Chave pública do usuário

$y = g^x \bmod p$

Número secreto por mensagem do usuário

k = inteiro aleatório ou pseudoaleatório com $0 < k < q$

Assinatura

$r = (g^k \bmod p) \bmod q$

$s = [k^{-1} (\mathrm{H(M)} + xr)] \bmod q$

Signature = (r, s)

Verificação

$w = (s')^{-1} \bmod q$

$u_1 = [\mathrm{H}(M')w] \bmod q$

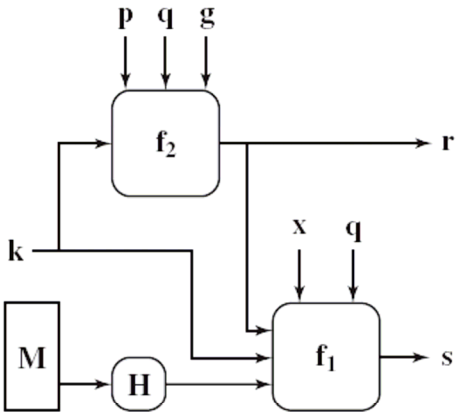
$u_2 = (r')w \bmod q$

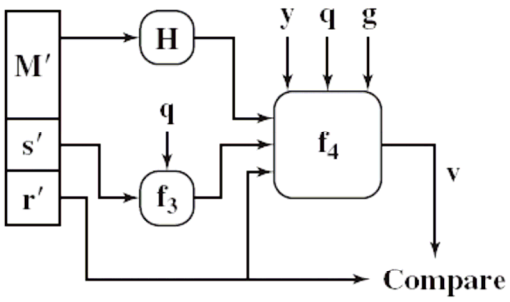
$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$

TESTe: $v = r'$

M = mensagem a ser assinada
$\mathrm{H}(M)$ = hash de M usando SHA-1
M', r', s' = versões recebidas de M, r, s

Figura 13.2 O algoritmo de assinatura digital (DSA).





$s = f_1(\mathrm{H(M)}, k, x, r, q) = (k^{-1} (\mathrm{H(M)} + xr)) \bmod q$

$r = f_2(k, p, q, g) = (g^k \bmod p) \bmod q$

(a) Assinatura

$w = f_3(s', q) = (s')^{-1} \bmod q$

$v = f_4(y, q, g, \mathrm{H}(M'), w, r')$
$= ((g^{(\mathrm{H}(M')w) \bmod q} y^{r'w \bmod q}) \bmod p) \bmod q$

(b) Verificação

Figura 13.3 Assinatura e verificação do DSS.