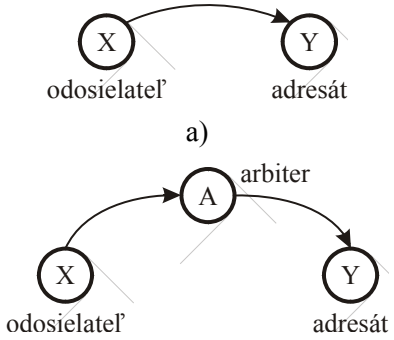
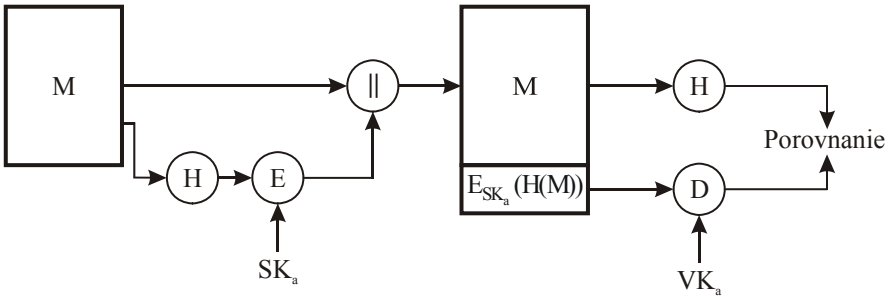
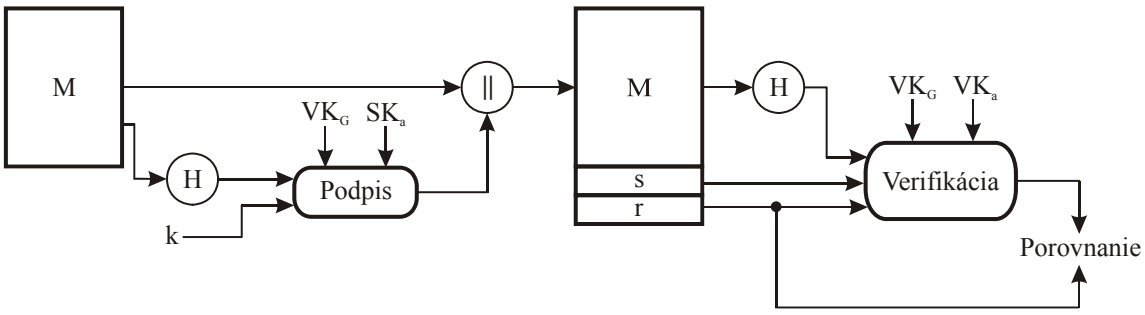
11 DIGITÁLNE PODPISY



Obr. 11.1 a – komunikácia na báze priamych digitálnych podpisov
b – komunikácia na báze verifikovaných digitálnych podpisov





Obr. 11.2 Postupy v digitálnych podpisoch
a) Digitálny podpis na báze RSA
b) Digitálny podpis na báze DSS

Generovanie kľúčov	
Výber p	p – prvočíslo
Zvoľ g, x	náhodné čísla $g<p$ $x<p$
Verejný kľúč	$VK=\{y, g, p\}$
Súkromný kľúč	$SK=\{x\}$

Generovanie digitálneho podpisu	
Výber k	náhodné číslo, ktoré nie je súdeliteľné s $(p–1)$
Originálna správa	M
Podpis (dvojica a,b)	$a = g^k \bmod p$ b je číslo, pre ktoré platí $M = (x.a + k.b) \bmod (p-1)$

Verifikácia podpisu	
Podpis	a, b
Platnosť ak	$y^a a^b \bmod p = g^{M'} \bmod p$
M'	prijatá správa

Obr. 11.3 Princíp digitálneho podpisu na báze algoritmu El Gamal

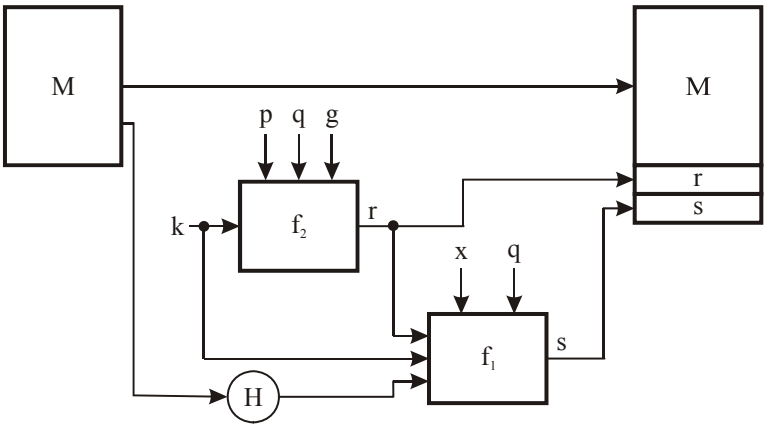
Generovanie spoločných prvkov verejného kľúča	
p	prvočíslo, pričom $2^{L-1} \le p \le 2^L$ a zároveň platí $512 \le L \le 1024$, pričom L je vždy násobkom 64
q	prvočíslo, ktoré je deliteľom čísla (p–1), pričom platí $2^{159} < q < 2^{160}$, t.j. q má dĺžku 160 bitov
g	číslo, pre ktoré platí $g = h^{(p-1)/q}$ pričom 1<h<(p–1) a zároveň $h^{(p-1)/q} \bmod p > 1$

Generovanie kľúčov odosielateľa	
Súkromný kľúč	SK_a={x}, pričom x je náhodné, resp. pseudonáhodné číslo, pre ktoré platí 0<x<q
Verejný kľúč	VK_a{y}, pričom $y = g^x \bmod p$
k	náhodné, resp. pseudonáhodné číslo, pričom 0<k<q

Generovanie digitálneho podpisu	
Podpis (dvojica r,s)	$r = \left(g^k \bmod p\right) \bmod q$ $s = \left(k^{-1}\left(H(M) + x \cdot r\right)\right) \bmod q$ $H(M)$–hašovacia funkcia SHA–1

Verifikácia digitálneho podpisu	
Výpočet w, u_1, u_2, v	$w = (s')^{-1} \bmod q$ $u_1 = \left(H(M') \cdot w\right) \bmod q$ $u_2 = \left(r' \cdot w\right) \bmod q$ $v = \left(\left(g^{u_1} \cdot y^{u_2}\right) \bmod q\right) \bmod p$
Test $v \stackrel{?}{=} r'$, pričom M', r', s' – prijaté verzie M, r, s	

Obr. 11.4 Algoritmus DSA

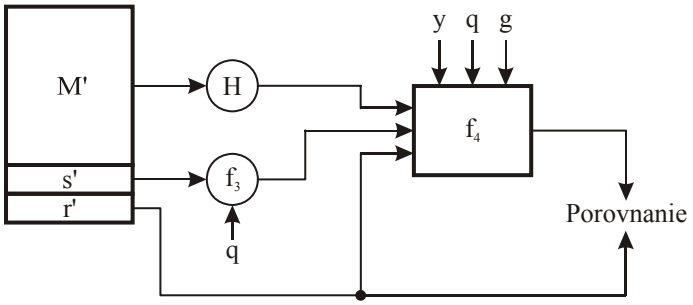


a)

$$s = f_1\left(H\left(M\right),k,x,r,g\right) = \left(k^{-1}\left(H\left(M\right)+x\cdot r\right)\right)\bmod q$$

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

$H(M)$ – hašovacia funkcia SHA–1



b)

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

$$v = f_4\left(y,q,g,H\left(M\right),w,r'\right)$$

Obr. 11.5 a) generovanie digitálneho podpisu pomocou DSA
b) verifikácia digitálneho podpisu pomocou DSA