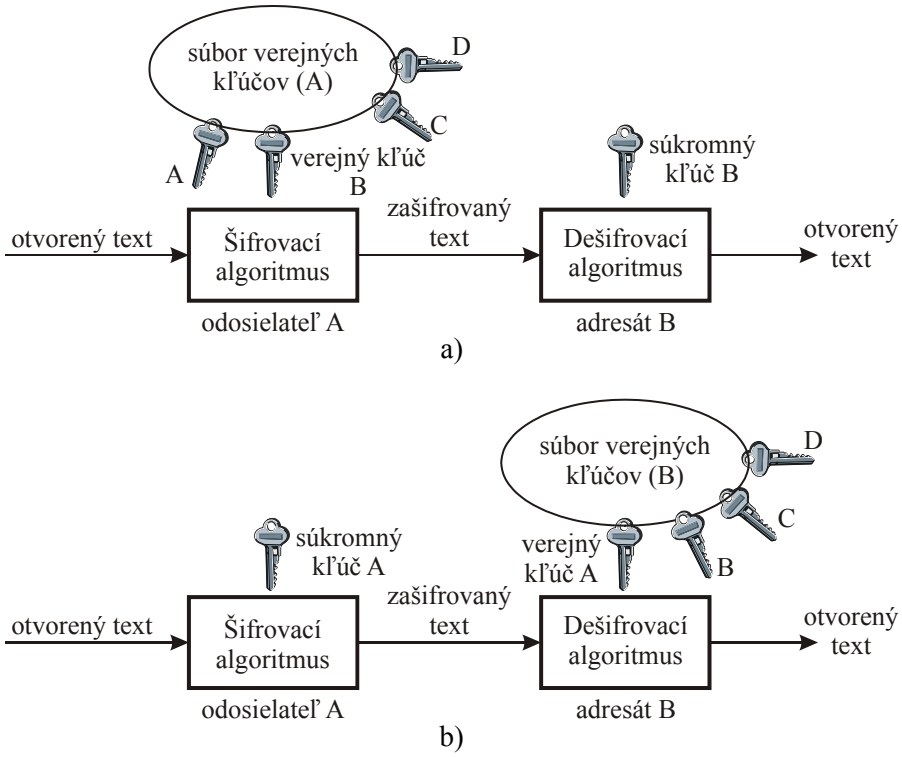
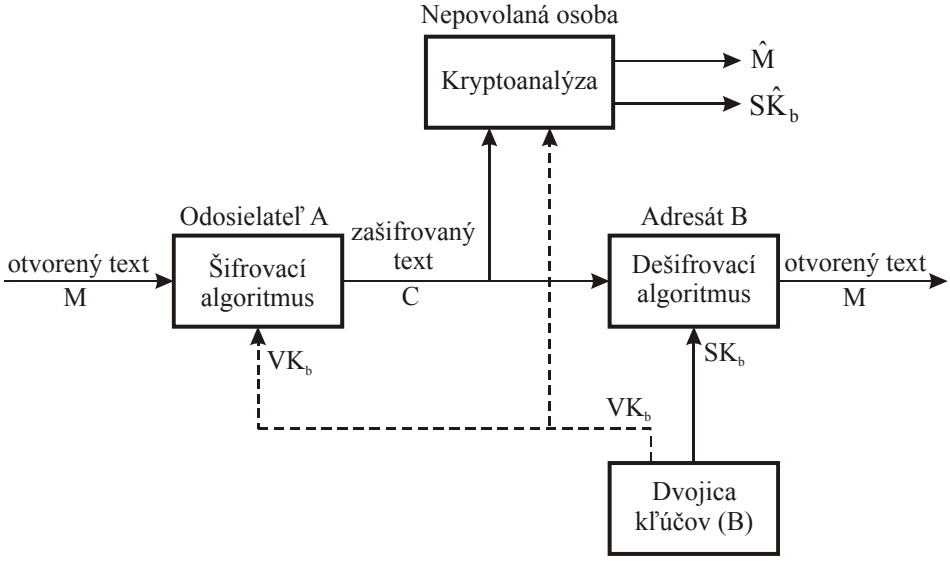
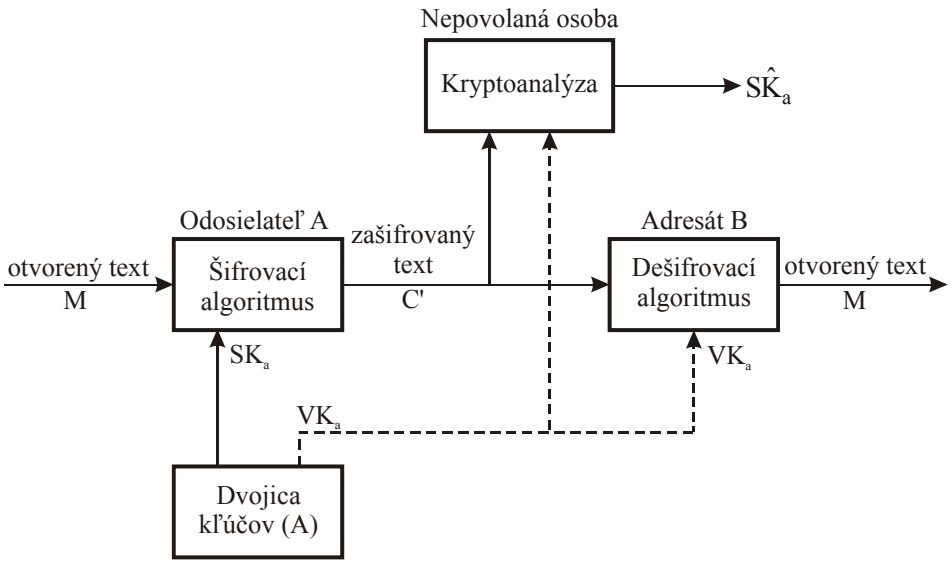


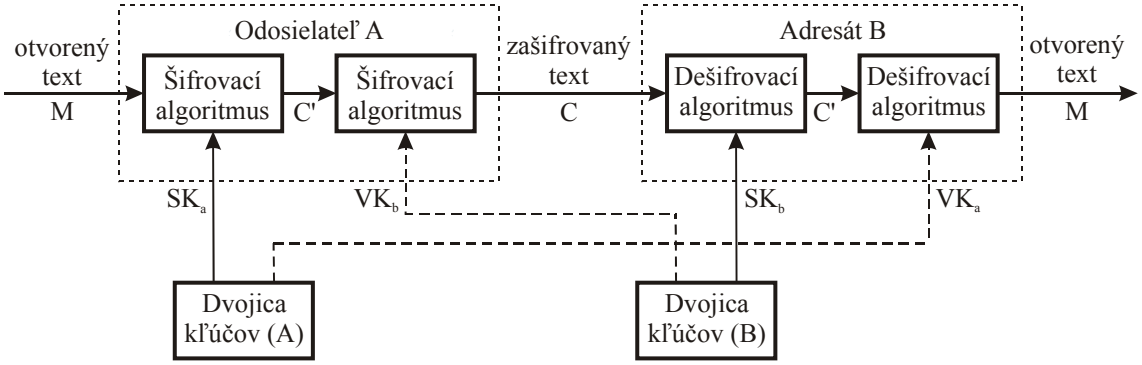
Kryptografia s verejným kľúčom, a) šifrovanie, b) autentizácia



Kryptografický systém s verejným kľúčom (utajenie)



Kryptografický systém s verejným kľúčom (autentizácia)



Kryptografický systém s verejným kľúčom (utajenie a autentizácia)

Voľba verejných prvkov	
q	prvočíslo
α	α<q a je jednoduchým koreňom q

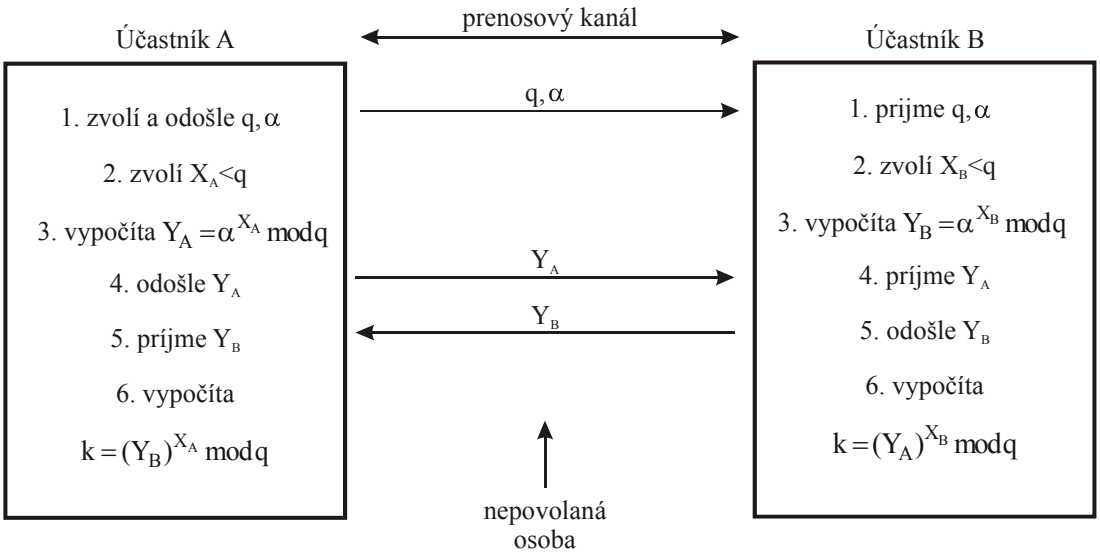
Generovanie parametra kľúča účastníkom A	
Voľba čísla X_A	$X_A < q$
Výpočet Y_A	$Y_A = \alpha^{X_A} \bmod q$

Generovanie parametra kľúča účastníkom B	
Voľba X_B	$X_B < q$
Výpočet Y_B	$Y_B = \alpha^{X_B} \bmod q$

Generovanie tajného kľúča k účastníkom A
$k = (Y_B)^{X_A} \bmod q$

Generovanie tajného kľúča k účastníkom B
$k = (Y_A)^{X_B} \bmod q$

Princíp algoritmu Diffie – Hellman



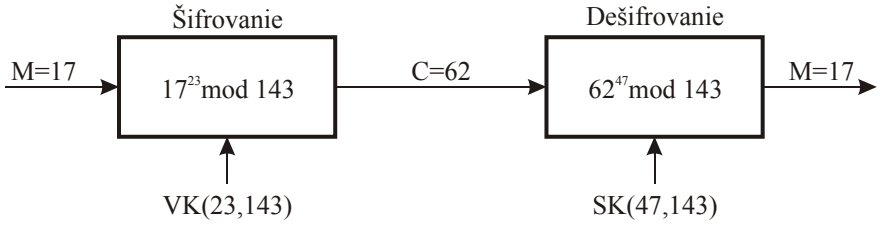
Protokol algoritmu Diffie–Hellman

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

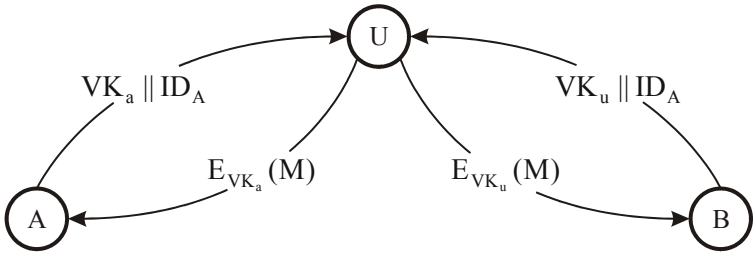
Šifrovanie	
Vyber k	náhodné číslo k, ktoré nie je súdeliteľné s (p-1)
Otvorený text	M
Zašifrovaný text	$a = g^k \bmod p$
(dvojica a,b)	$b = y^k M \bmod p$

Dešifrovanie	
Zašifrovaný text	a,b
Otvorený text	$M = b / a^x \bmod p$

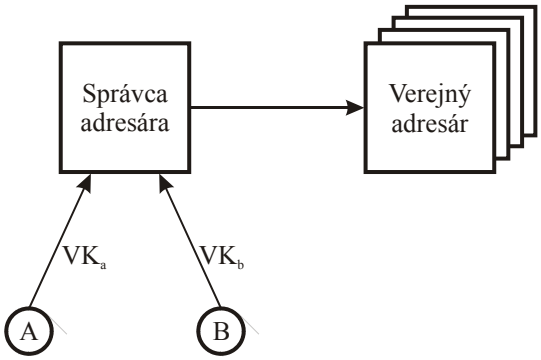
Princíp algoritmu El Gamal



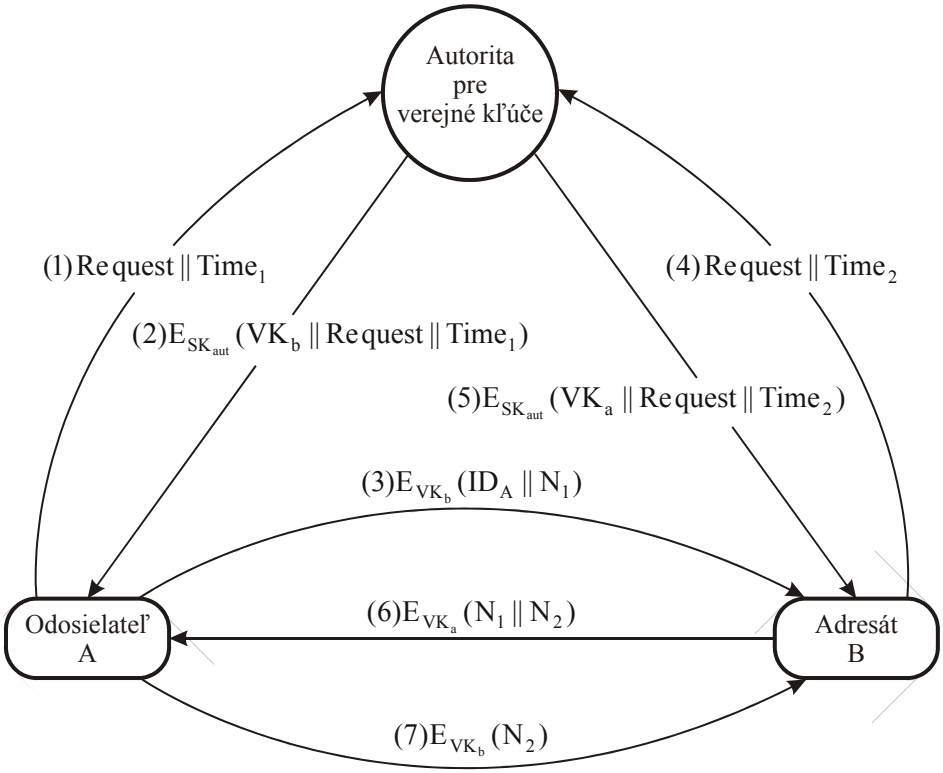
Príklad šifrovania a dešifrovania RSA algoritmom



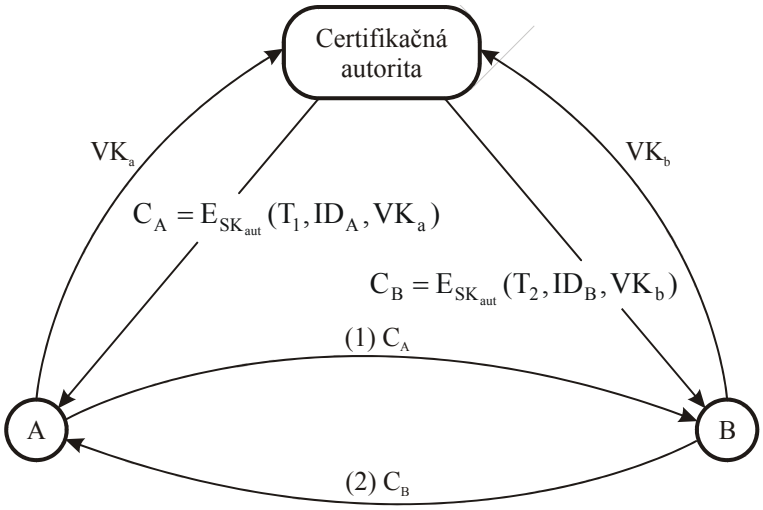
Podvrhnutie verejného kľúča



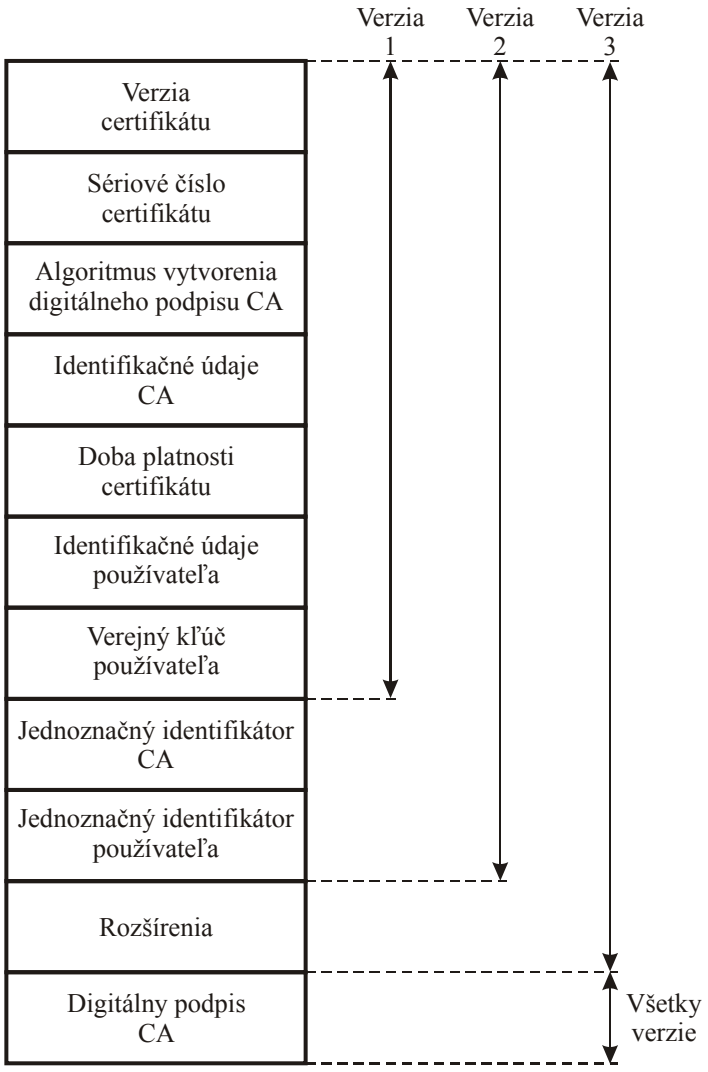
Princíp verejne dostupného adresára



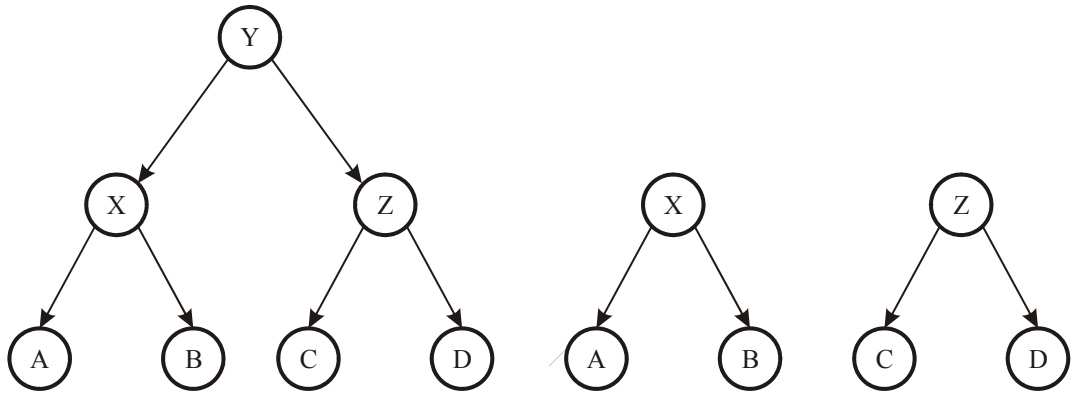
Distribúcia verejných kľúčov pomocou autority pre verejné kľúče



Distribúcia verejných kľúčov pomocou certifikátov

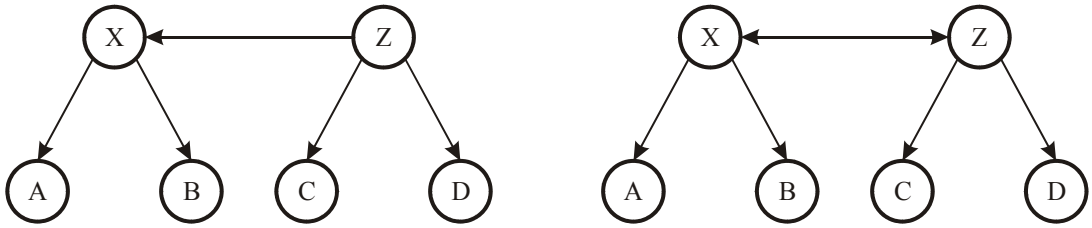


Formáty certifikátov podľa odporúčania X.509



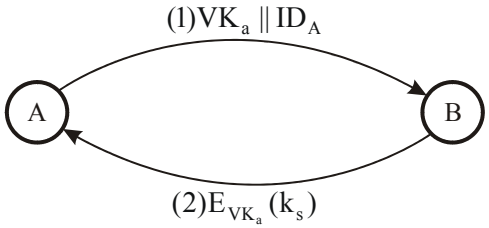
a) b)

a) stromová štruktúra používateľov
b) krížová štruktúra používateľov

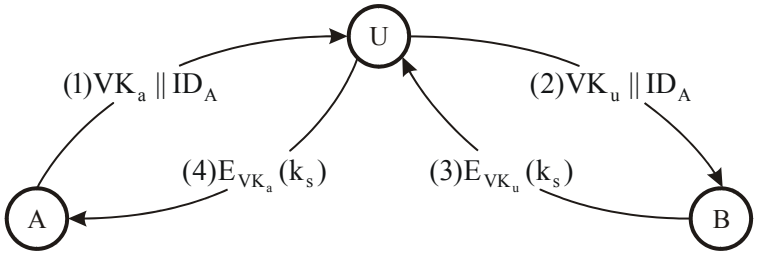


a) b)

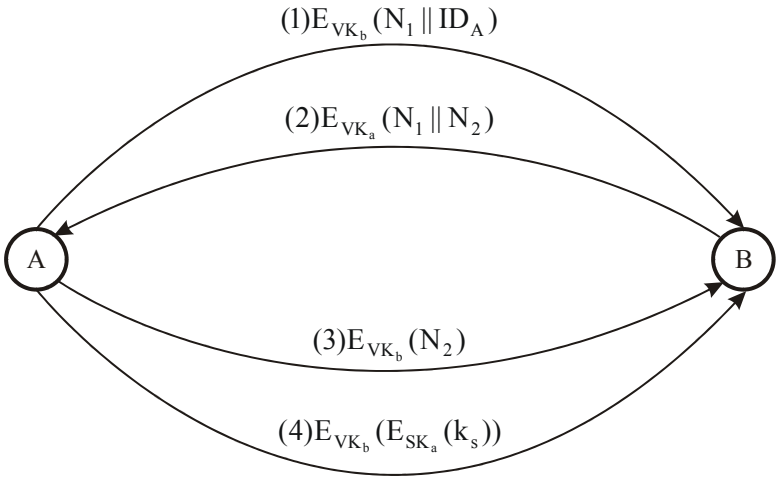
Krížová certifikácia, a) jednosmerná certifikácia X certifikačnou autoritou Z
b) obojsmerná krížová certifikácia X a Z



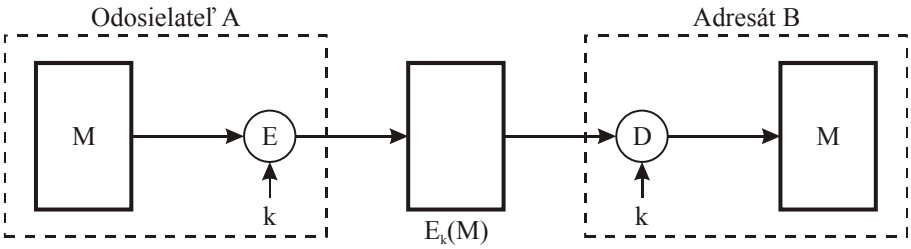
Jednoduchá distribúcia tajných kľúčov



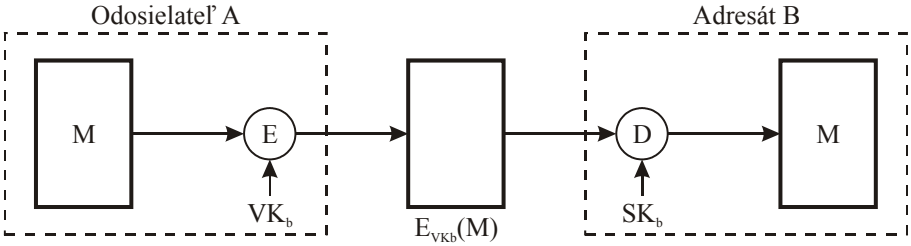
Získanie tajného kľúča podvrhnutím verejného kľúča



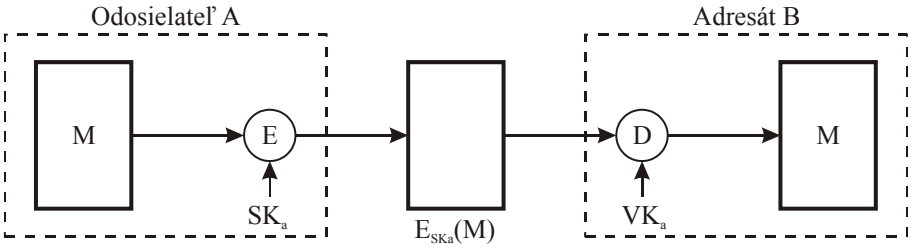
Výmena tajných kľúčov s utajením a autentizáciou



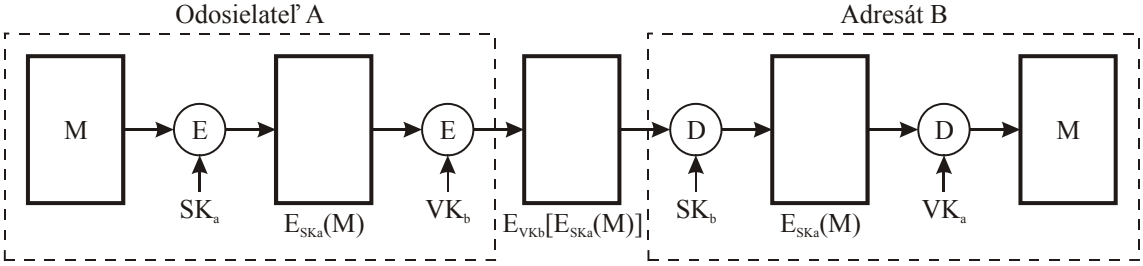
a) Symetrické šifrovanie: utajenie a autentizácia



b) Asymetrické šifrovanie: utajenie

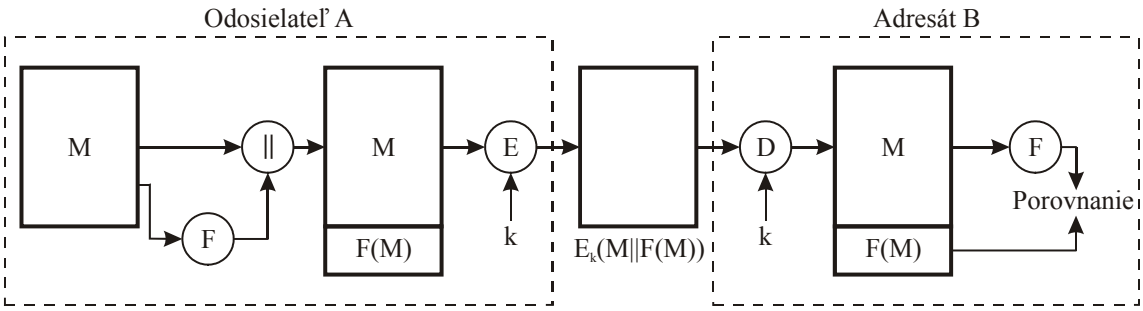


c) Asymetrické šifrovanie: autentizácia a podpis

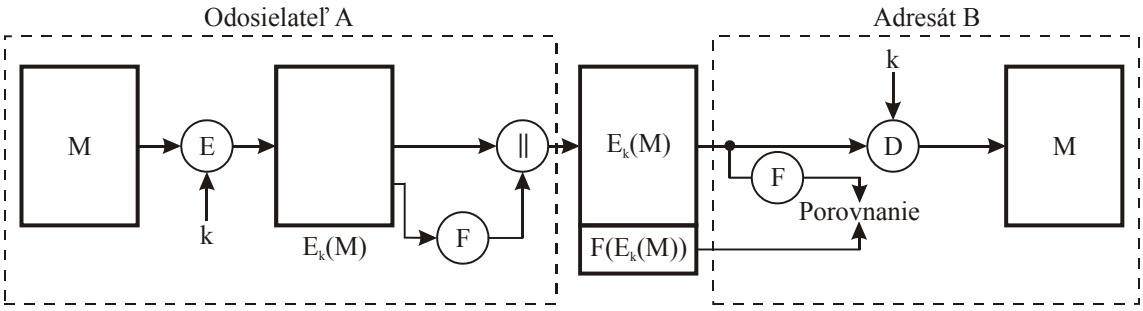


d) Asymetrické šifrovanie: utajenie, autentizácia a podpis

Šifrovanie a dešifrovanie správy

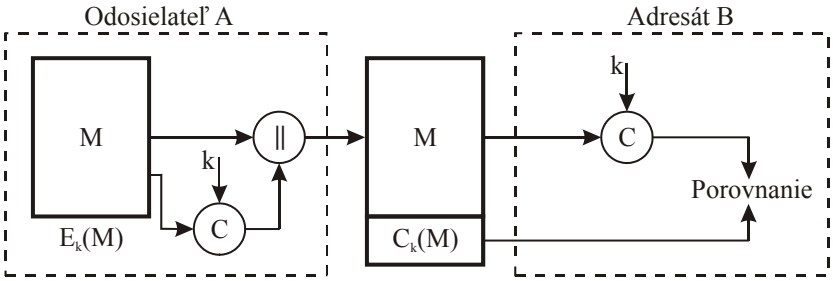


a) interný

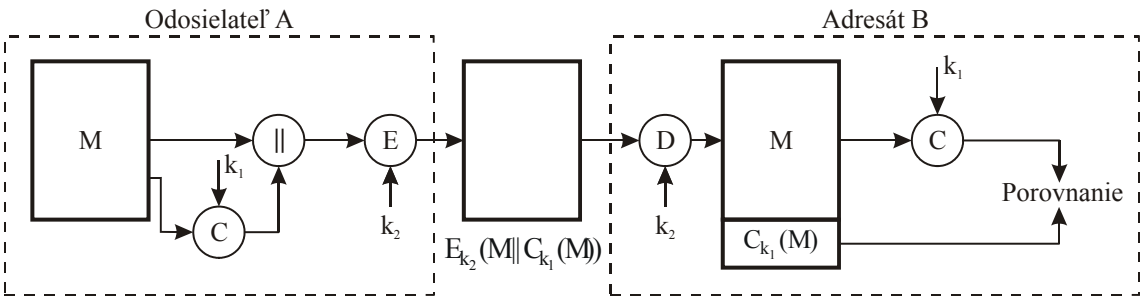


b) externý

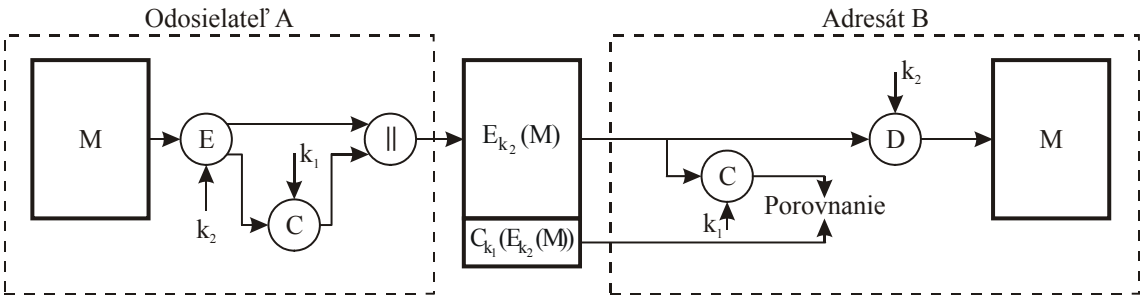
Kryptografický kontrolný súčet, a–interný, b–externý



a) Autentizácia správy

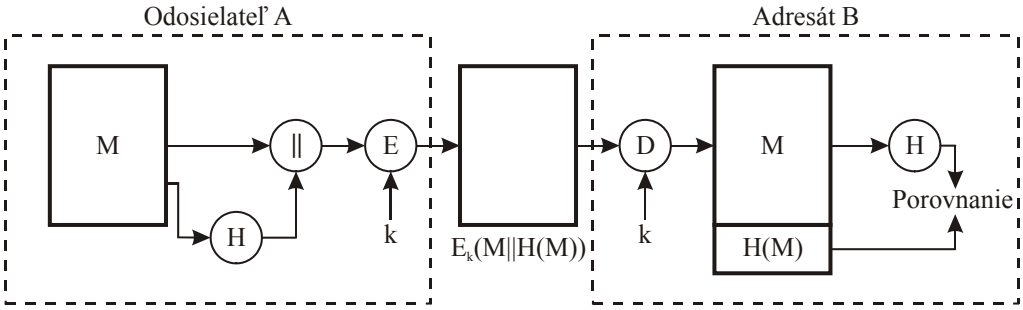


b) Utajenie a autentizácia správy pripojená k otvorenému textu

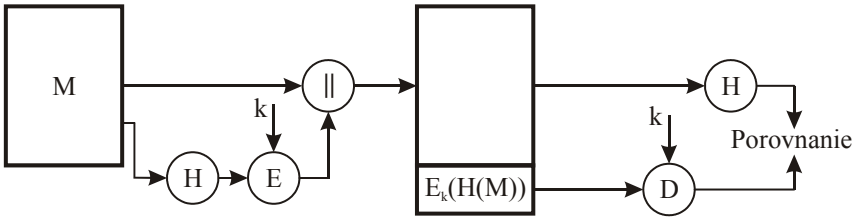


c) Utajenie a autentizácia správy pripojená k zašifrovanému textu

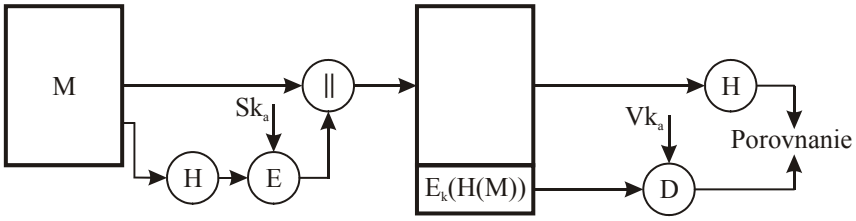
Media Access Control (MAC)



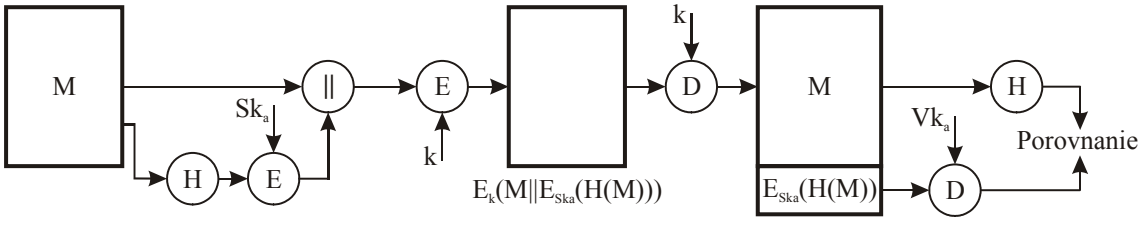
a)



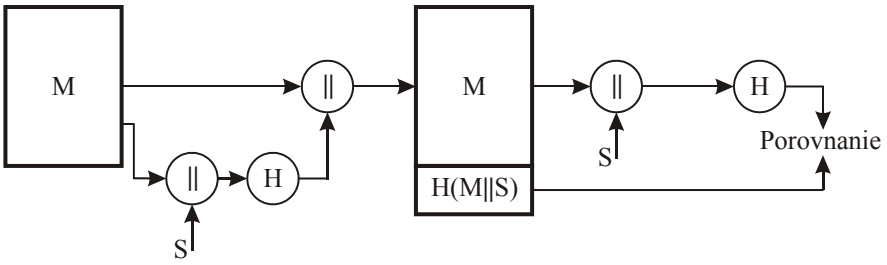
b)



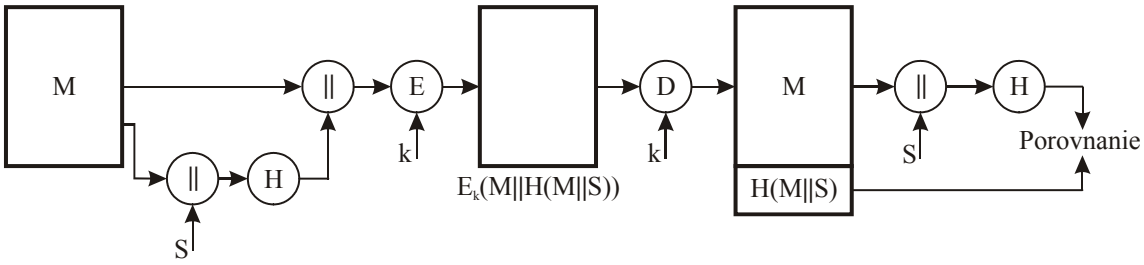
c)



d)



e)

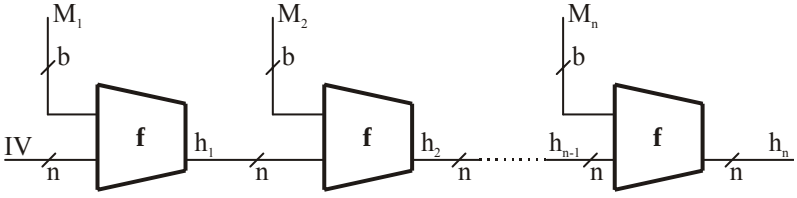


f)

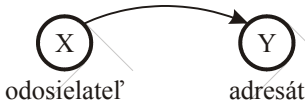
Hašovacie funkcie

	bit 1	bit 2	bit 3	. . .	bit n
Blok 1	b_{11}	b_{21}	b_{31}	. . .	b_{n1}
Blok 2	b_{12}	b_{22}	b_{32}	. . .	b_{n2}
Blok 3	b_{13}	b_{23}	b_{33}	. . .	b_{n3}
	⋮	⋮	⋮	⋮	⋮
Blok m	b_{1m}	b_{2m}	b_{3m}	. . .	b_{nm}
Hašovací kód h	h_1	h_2	h_3	. . .	h_n

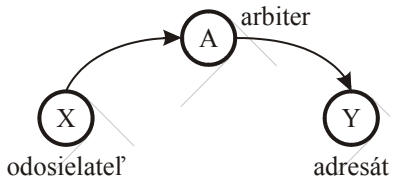
Jednoduchá hašovacia funkcia s využitím operácie XOR



Štruktúra iteračných hašovacích funkcií

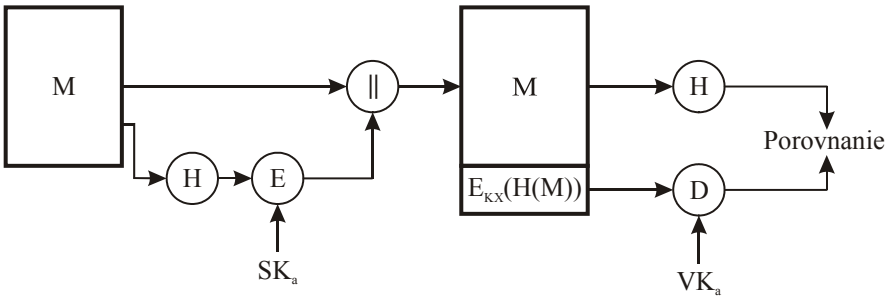


a)

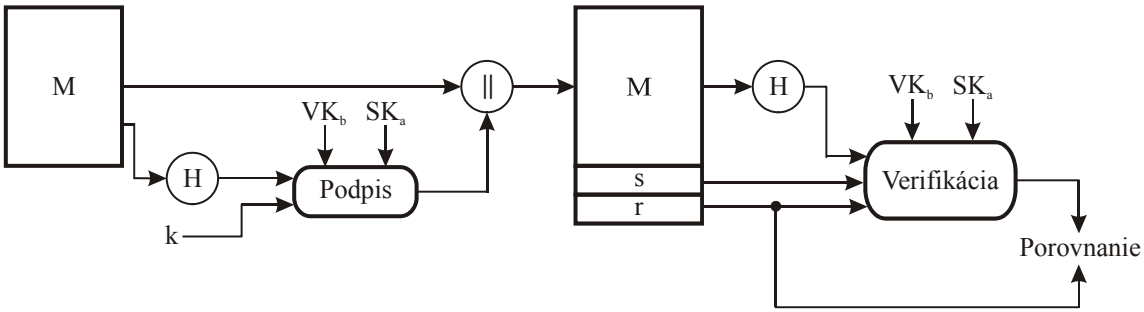


b)

a – komunikácia na báze priamych digitálnych podpisov
b – komunikácia na báze verifikovaných digitálnych podpisov



a) Digitálny podpis na báze RSA



b) Digitálny podpis na báze DSS

Postupy v digitálnych podpisoch

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

Princíp digitálneho podpisu na báze algoritmu El Gamal

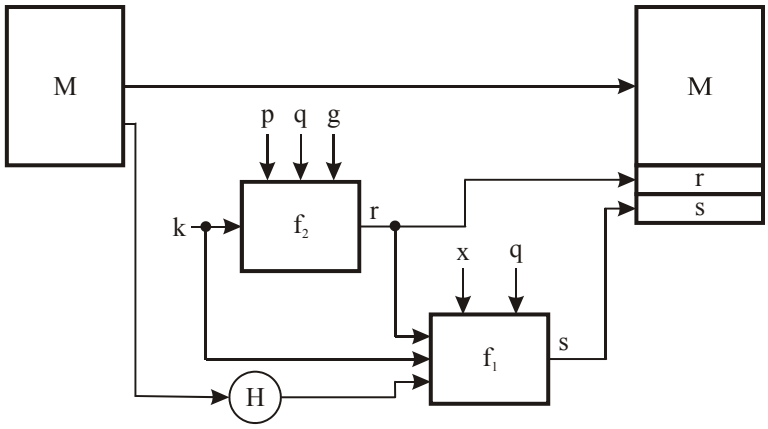
Generovanie spoločných prvkov verejného kľúča	
p	prvočíslo, pričom $2^{L-1} \le p \le 2^{L}$ a zároveň platí $512 \le L \le 1024$, pričom L je vždy násobkom 64
q	prvočíslo, ktoré je deliteľom čísla (p–1), pričom platí $2^{159} < q < 2^{160}$, t.j. q má dĺžku 160 bitov
g	číslo, pre ktoré platí $g = h^{(p-1)/q}$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

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

Algoritmus DSA

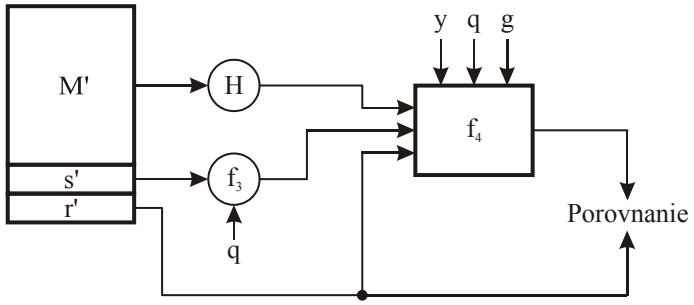


a)

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

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

H(M) – hašovacia funkcia SHA–1



b)

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

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

a) generovanie digitálneho podpisu pomocou DSA
b) verifikácia digitálneho podpisu pomocou DSA