Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Kryptológia

M. Stanek / M. Rjaško

2013

KPMG
cutting through complexity™

KRYPTOLÓGIA

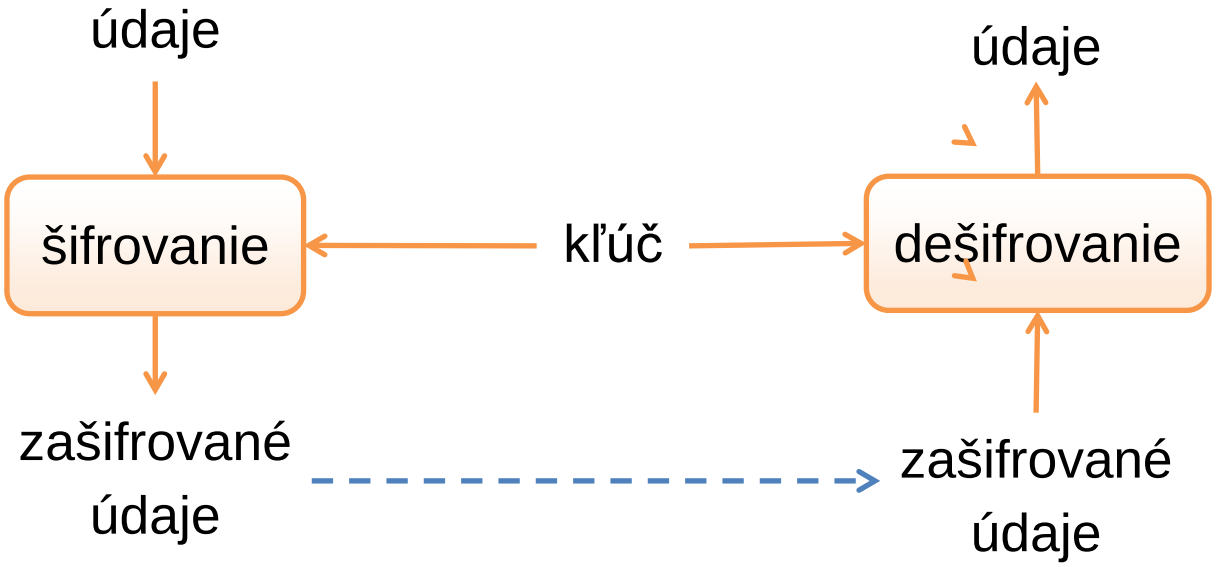
Martin Stanek

Úvod

- Kryptografické konštrukcie, kryptoanalýza
- Symetrické a asymetrické šifrovanie
- Hašovacie funkcie a autentizačné kódy správ
- Digitálne podpisy
- Protokoly
- Heslá a kryptografické kľúče
- Infraštruktúra verejných kľúčov
- Zraniteľnosti a kryptografia
- Štandardy a legislatíva

Symetrické šifrovanie

- Dôvernosť údajov
- Šifrovanie aj dešifrovanie využíva rovnaký kľúč
- Blokové a prúdové šifry



Blokové šifry

- Definované na blokoch pevnej dĺžky (napr. 128 bitov)
- Kľúč obvykle náhodne volený reťazec bitov pevnej dĺžky
- Najpoužívanejší typ symetrických šifier (štandardy, flexibilita)
- Spôsob konštrukcie: iterácia viacerých kôl
- Najpoužívanejšie blokové šifry:

	dĺžka bloku	dĺžka kľúča	počet kôl
AES	128	128, 192, 256	10, 12, 14
3DES	64	112, 168	3 x 16

Poznámky k AES a 3DES

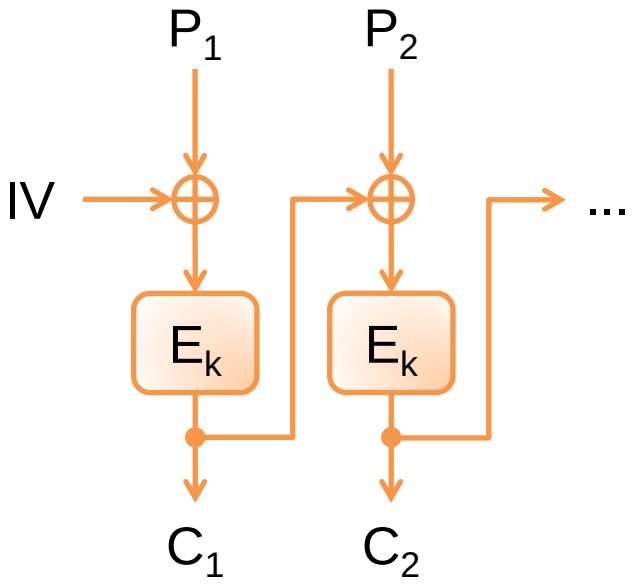
- Oba algoritmy schválené NIST
- Novšie procesory s HW podporou pre AES
  - podstatne vyšší výkon ako pri SW implementácii
- Rastúca dĺžka kľúča $\Rightarrow$ mierne klesá výkon AES (viac kôl)
- 3DES – sekvenčné zreťazenie 3 DES transformácií
  - 3 nezávislé kľúče – 168 bitov dlhý kľúč (3 x 56)
  - Efektívna dĺžka kľúča (len) 112 bitov

Operačné módy blokových šifier

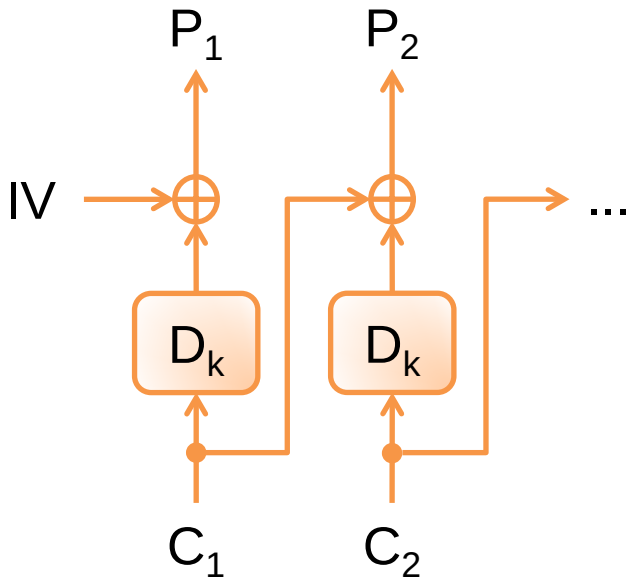
- Flexibilné použitie blokových šifier
- Rôzne módy pre rôzne bezpečnostné požiadavky (módy schválené NIST):
  - dôvernosť (celkovo 5 módov: ECB, CBC, OFB, CFB, CTR)
  - autentickosť (CMAC)
  - autentizované šifrovanie (CCM) a autentizované šifrovanie s vysokou priepustnosťou (GCM)
  - dôvernosť pre blokové úložiská dát, napr. disky (XTS)
  - dôvernosť a integrita kľúčov (KW, KWP, TKW)

  ... a ďalšie
- Rôzne módy majú rôzne vlastnosti a predpoklady

CBC



šifrovanie v CBC móde



dešifrovanie v CBC móde

- Často používaný mód
- napr. AES-128 v CBC móde je povinná súčasť TLS 1.2

Prúdové šifry

- Generátor pseudonáhodných bitov (bajtov)
- Obvykle sčítanie mod 2 s bitmi vstupných dát
- Niektoré módy blokových šifier vytvárajú prúdovú šifru (OFB, CTR, CFB)
- Najznámejšia prúdová šifra: RC4

Asymetrické šifrovanie

- Dvojica kľúčov: verejný a súkromný
- Šifrovanie s verejným kľúčom (ktokoľvek vie šifrovať)
- Dešifrovanie so súkromným kľúčom
- Bezpečnosť sa opiera o zložitosť matematických problémov
  - faktorizácia, diskrétny logaritmus a iné
- Najpoužívanejší systém: RSA (problém faktorizácie)
- Ekvivalentná dĺžka kľúča:
  - NIST SP 800-57: 3072 bitov RSA ~ 128 bitov symetrického kľúča

RSA

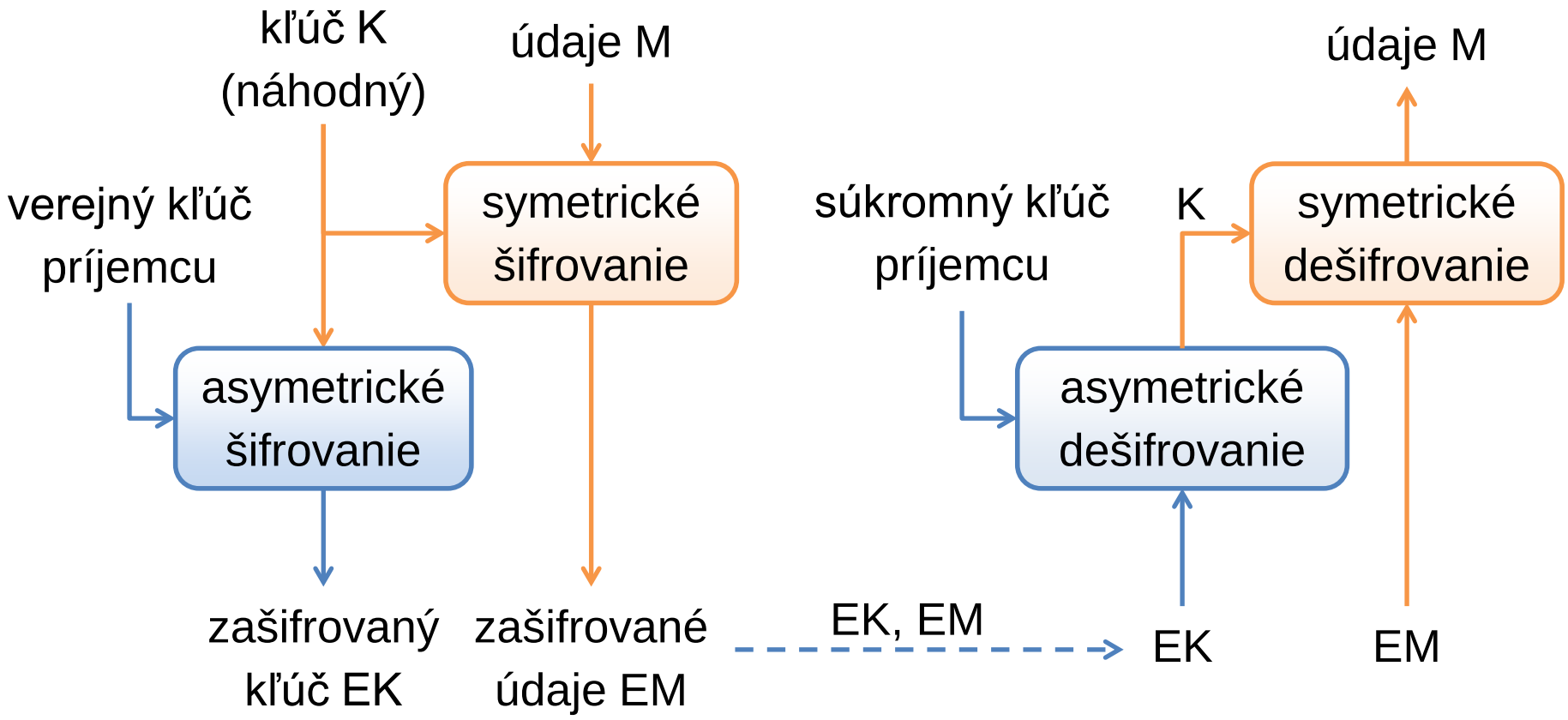
- Verejný kľúč: (e, n)
  - $n = p \cdot q$, kde p, q sú veľké prvočísla
  - e je nesúdeliteľné s $(p-1)(q-1)$
  - najčastejšia voľba $e = 65537$
- Súkromný kľúč: d
  - pričom platí $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$
  - pre urýchlenie súkromnej transfromácie sú súčasťou obvykle aj ďalšie parametre
- Šifrovanie (verejná transformácia): $E(m) = m^e \bmod n$
  - pre vstup $m \in \{0, 1, \ldots, n-1\}$
- Dešifrovanie (súkromná transformácia): $D(c) = c^d \bmod n$
- Šifrovanie rýchlejšie ako dešifrovanie

RSA šifrovanie v praxi

- Padding – výplň/zarovnanie
  - pred šifrovaním
  - po dešifrovaní
- Najčastejšie používané schémy:
  - PKCS #1 v1.5
  - OAEP (lepšie bezpečnostné vlastnosti)

Hybridné šifrovanie

- Kombinácia asymetrického a symetrického šifrovania



Symetrické vs. asymetrické šifrovanie

	Symetrické šifrovanie	Asymetrické šifrovanie
Primárne použitie	dôvernosť údajov ľubovoľného rozsahu	dôvernosť krátkych dát (typicky napr. kľúče pre symetrické šifrovanie)
Komunikácia	1:1 – obvykle dvaja účastníci	N:1 – ľubovoľný počet odosielateľov (šifrovací kľúč je verejný), jeden príjemca (súkromný dešifrovací kľúč)
Efektívnosť	rýchle šifrovanie aj dešifrovanie	pomalé šifrovanie aj dešifrovanie
Dĺžka kľúčov	obvykle 112 až 256 bitov (náhodný reťazec bitov)	v závislosti na konkrétnom algoritme, niekoľko sto až niekoľko tisíc bitov

Hašovacie funkcie

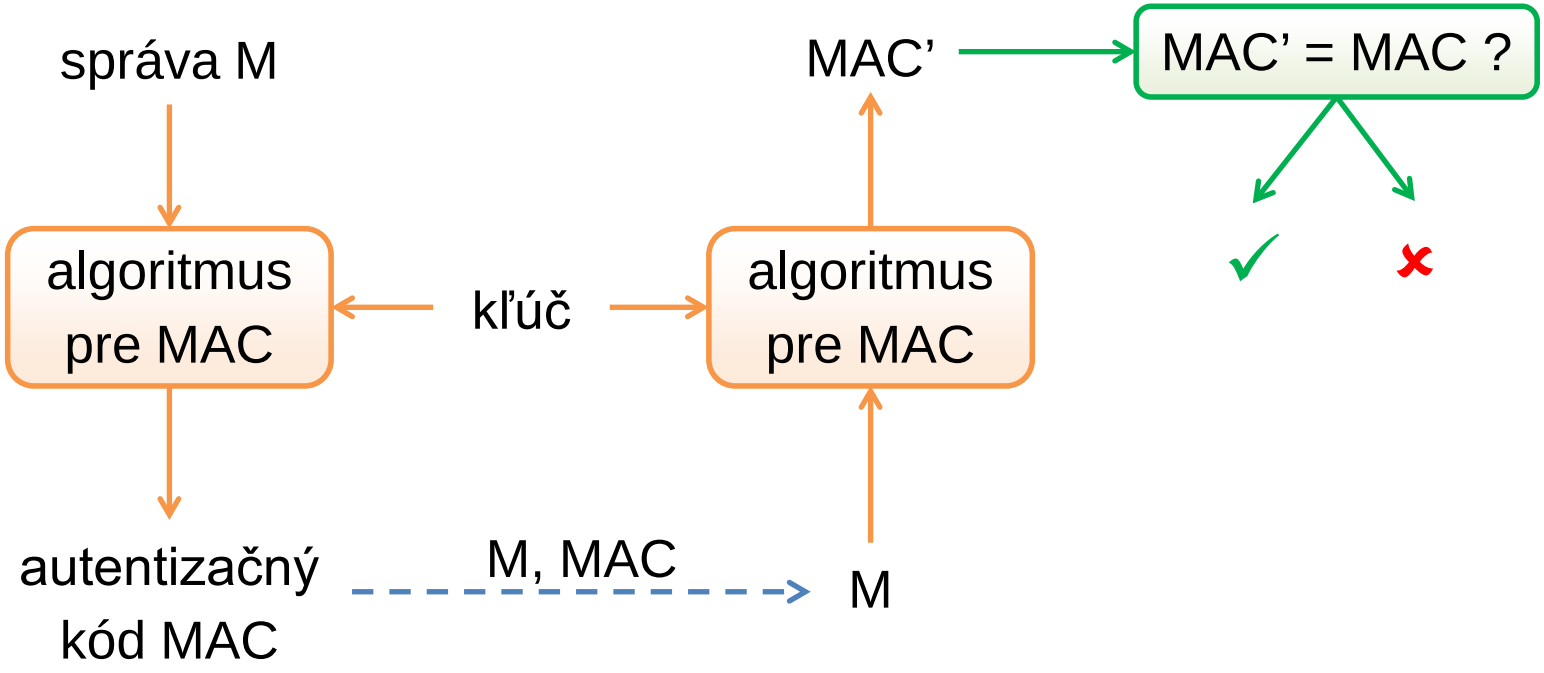
- Transformácia vstupu na odtlačok fixnej dĺžky
- Najpoužívanejšie: SHA-1 (160 bitov), SHA-256, SHA-512
- Žiadny kľúč
- Zabezpečenie integrity dát
- Detekcia *náhodnej/neúmyselnej* zmeny dát
- Požadované vlastnosti:
  - odolnosť vzoru (jednosmernosť)
  - odolnosť voči kolíziám
- Rôznorodé použitie
  - digitálne podpisy, paddingové schémy, autentizačné kódy správ, PBKDF (odvodenie symetrických kľúčov z hesiel, uloženie hesiel)

Hašovacie funkcie (2)

- Narodeninový útok – generické hľadanie kolízií
- Zložitosť $2^{n/2}$, kde n je dĺžka odtlačku
- Dĺžka odtlačku ~ 2 x dĺžka symetrického kľúča
- SHA-3 nový štandard
  - Keccak – víťazný algoritmus
  - štandard očakávaný v 2014
  - predpokladaná koexistencia s rodinou SHA-2 funkcií

Autentizačné kódy správ

- Symetrický kľúč (odosielateľ a príjemca)
- Integrita a autentickosť dát; nie však nepopierateľnosť autorstva
- Rýchlosť – v sieťových protokoloch pre každý paket



HMAC

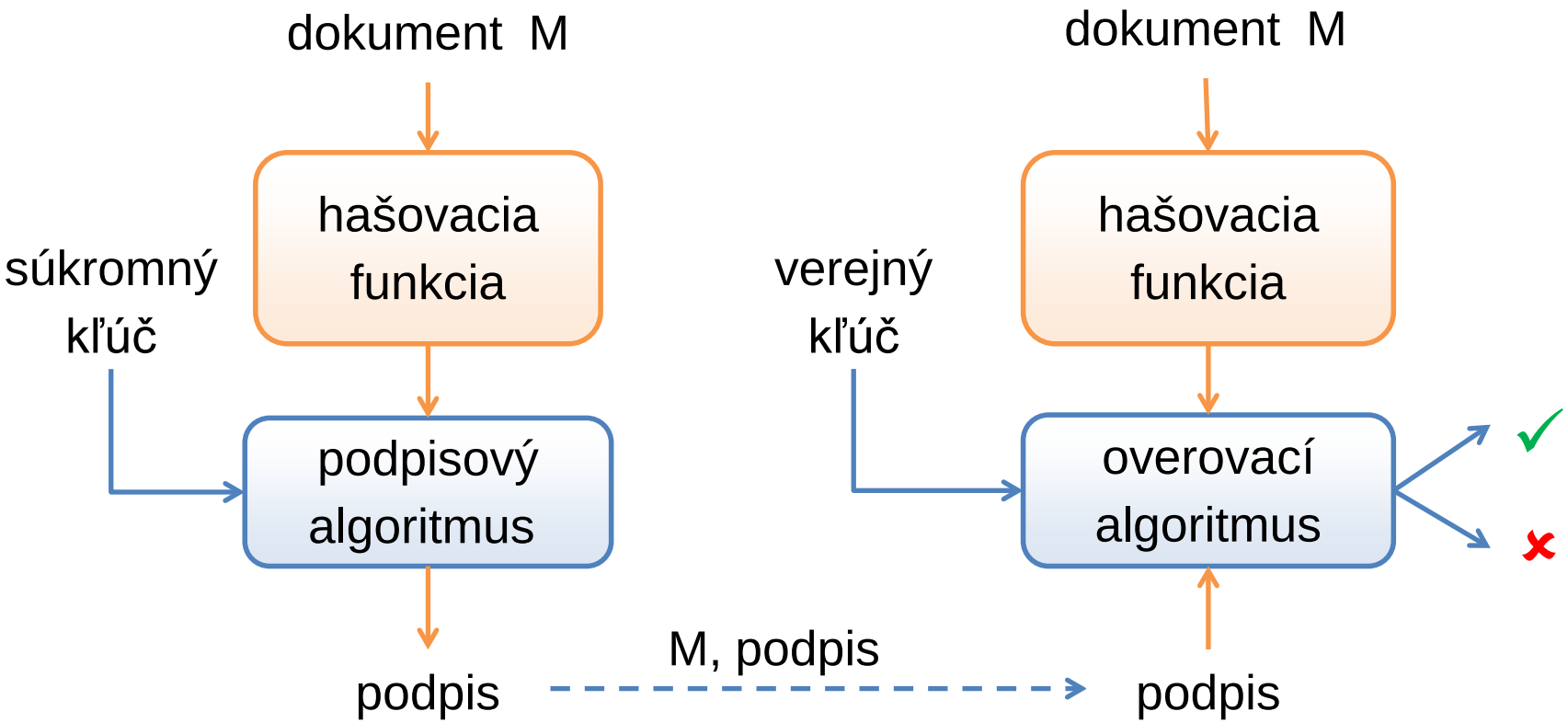
- Najpoužívanejšia konštrukcia MAC (z hašovacích funkcií)
  - IPSec, SSL/TLS, SSH, ...

$$\mathrm{HMAC}(k, m) = \mathrm{H}((k \oplus opad) \,||\, \mathrm{H}((k \oplus ipad) \,||\, m))$$

  - H – hašovacia funkcia
  - *k* – kľúč
  - *M* – správa
  - opad/ipad – konštanty
- Dĺžka výstupu HMAC je rovnaká ako dĺžka odtlačku H
  - Orezanie výstupu, napr. HMAC-SHA1-96 (IPSec)
- Pre bezpečnosť HMAC nie je potrebná odolnosť H voči kolíziám

Schémy digitálnych podpisov

- Asymetrická konštrukcia (verejný a súkromný kľúč)
- Integrita a autentickosť dát, nepopierateľnosť autorstva
- Najpoužívanejšie konštrukcie: RSA, DSA, ECDSA



RSA podpisová schéma

- Rovnaké parametre ako pri RSA šifrovaní
  - použitie rovnakej inštancie na oba účely sa neodporúča
- Podpisovanie: $s = H(m)^d \bmod n$
- Overenie podpisu: $s^e \bmod n = H(m)$?
- V praxi sa používajú výplňové schémy (padding):
  - PKCS #1 v1.5 (iná ako pri šifrovaní)
  - PSS

Porovnanie

	Hašovacie funkcie	Autentizačné kódy	Digitálne podpisy
Integrita	áno	áno	áno
Autentickosť	nie	áno	áno
Nepopierateľnosť autorstva	nie	nie	áno
Kľúče	žiadne	symetrické	asymetrický pár kľúčov
Efektívnosť	rýchle	rýchle	pomalé
Typická aplikácia	kontrola integrity statických dát	autentickosť jednotlivých paketov v sieti	autentickosť dokumentov

Bezpečný komunikačný kanál

- Dôvernosť & autentickosť ~ symetrické šifrovanie & MAC
- Šifruj potom MAC (napr. IPSec):

$$E_{k1}(m), MAC_{k2}(c)$$

- MAC potom šifruj (napr. SSL/TLS):

$$E_{k1}(m, MAC_{k2}(m))$$

- Šifruj a MAC (napr. SSH2):

$$E_{k1}(m), MAC_{k2}(m)$$

Protokoly

- Protokoly pre autentizáciu a dohodnutie kľúčov
- Následne realizujú bezpečný komunikačný kanál
- Najznámejšie: SSL/TLS, IPSec, SSH a pod.
- Viaceré varianty – algoritmy, spôsoby autentizácie
- Prostriedky autentizácie účastníka protokolu:
  - Zdieľaná tajná informácia (heslo/kľúč)
  - Znalosť súkromného kľúča k verejnému kľúču uvedenom v certifikáte

Diffieho-Hellmanov protokol

- Protokol na dohodnutie kľúča
  1. A $\rightarrow$ B: $p, g, g^x \bmod p$
  2. B $\rightarrow$ A: $g^y \bmod p$
  3. A vypočíta $K = (g^y)^x = g^{xy}$, B vypočíta $K = (g^x)^y = g^{xy}$
- Varianty DH protokolu použité v SSL/TLS (jedna z možností) a inde
- Bezpečnosť
  - pri pasívnom útočníkovi
  - nie je bezpečný pri aktívnom útočníkovi uprostred (MITM)
  - ochrana spočíva v zabezpečení autentickosti správ

Varianty DH protokolu

- TLS
  - DH_anon – anonymný DH (možný MITM útok)
  - DHE_RSA, DHE_DSS – server svoje parametre podpíše
  - DH_RSA, DH_DSS – parametre súčasťou certifikátu
  - EC* verzie
- IPSec
  - Protokoly IKEv1, IKEv2 – dohodnutie kľúča
  - DH protokol – autentizácia šifrovaním, digitálnym podpisom, MAC
- SSH2
  - DH je jedna z metód, server podpisuje svoje parametre

Základné charakteristiky TLS (SSL)

Autentizácia servera	povinná (znalosť súkromného kľúča k verejnému kľúču z certifikátu)
Autentizácia klienta	voliteľná (málokedy používané, obvykle riešené po vytvorení TLS spojenia)
Distribúcia kľúčov	viaceré protokoly (odvodenie kľúčov pre šifrovanie a autentizačné kódy)
Dôvernosť	symetrické šifrovanie (podpora rôznych algoritmov a módov)
Autentickosť	autentizačné kódy (podpora rôznych algoritmov)
Úprava aplikácie	zvyčajne potrebné v aplikácii špecificky inicializovať komunikačný kanál

S/MIME

- S/MIME (Secure/Multipurpose Internet Mail Extensions)
- Šifrovanie & podpisovanie elektronickej pošty
  - Štandard, široká podpora mailových klientov
  - Verejné kľúče vo forme X.509 certifikátov
  - Formát správy CMS (Cryptographic Message Syntax)
- Alternatíva: OpenPGP (PGP, GnuPG)
  - Priamočiarejšia správa kúčov

S/MIME (2)

Evolúcia povinne implementovaných kryptografických algoritmov:

Povinné v CMS („MUST“)	3.0 (RFC 2633) 1999	3.1 (RFC 3851) 2004	3.2 (RFC 5751) 2010
Hašovacia funkcia	SHA-1	SHA-1	SHA-256
Podpisová schéma	DSA	RSA, DSA	RSA
Asymetrické šifrovanie kľúča	DH	RSA	RSA
Symetrické šifrovanie	3DES CBC	3DES CBC	AES-128 CBC

Kryptografické kľúče

- Správa kľúčov (ako – algoritmy a postupy)
  - Generovanie
  - Distribúcia
  - Ukladanie a prístup
  - Ničenie kľúčov
  - Postupy pri kompromitácii kľúčov
- Dĺžka kľúčov – nutná ale nepostačujúca podmienka bezpečnosti

Útok prehľadávaním priestoru kľúčov

Čas útoku	Individuálny útočník 1 procesor	Stredne veľká firma 500 procesorov	Príjmy SR za 1 rok (53,8 mil. procesorov)
1 minúta	33,7	42,6	59,3
1 hodina	39,6	48,5	65,2
1 deň	44,1	53,1	69,8
30 dní	49,1	58,0	74,7
1 rok	52,7	61,6	78,3
100 rokov	59,3	68,3	85,0

- Ilustračný príklad pre konkrétny procesor (i7-2600)

Generické útoky

Konštrukcia	Generický útok (k dĺžka kľúča, n veľkosť odtlačku/výstupu)
Symetrická šifra	Prehľadávanie priestoru všetkých kľúčov $\sim 2^k$
Hašovacia funkcia	Hľadanie kolízií: narodeninový útok $\sim 2^{n/2}$ Hľadanie vzoru: prehľadanie a vyskúšanie vzorov $\sim 2^n$
MAC	Prehľadávanie priestoru všetkých kľúčov $\sim 2^k$, resp. uhádnutie korektného autentizačného kódu k správe $\sim 2^n$.
Asymetrická šifra	Riešenie konkrétneho ťažkého problému (faktorizácia, výpočet diskrétneho logaritmu a pod.)
Podpisová schéma	Riešenie konkrétneho ťažkého problému, resp. útok na hašovaciu funkciu.

Ekvivalentné dĺžky kľúčov

Ochrana	Symetrický kľúč	Výstup hašovacej funkcie	RSA modul	Eliptická krivka
~ 4 roky	80	160	1248	160
~ 20 rokov	112	224	2432	224
~ 30 rokov	128	256	3248	256
	256	512	15424	512

- Podľa správy ECRYPT II (2012)
- Porovnanie rôznych metód: www.keylength.com
- Bezpečnosť vs. výpočtové nároky

Výkonové porovnanie (1)

	SW impl. [MB/s]	HW podpora AES-NI (encrypt) [MB/s]	HW podpora AES-NI (decrypt) [MB/s]
AES-128-CTR		4 125	4 121
AES-128-CBC	127	749	4 064
AES-192-CBC	106	623	3 509
AES-256-CBC	90	537	3 055
3DES-CBC	28		
RC4	891		
SHA-1	717		
SHA-256	215		
SHA-512	335		

i7-2600, 3.40GHz, Ubuntu 12.04 LTS 64-bit, openssl 1.0.1, 8kB bloky

Výkonové porovnanie (2)

	podpisovanie [operácie/s]	overovanie [operácie/s]
RSA-1024	6 100	93 281
RSA-2048	857	27 496
RSA-4096	118	7 370
ECDSA-224 (nistp224)	15 375	7 349
ECDSA-256 (nistp256)	9 024	3 697
ECDSA-521 (nistp521)	3 252	1 501

Infraštruktúra verejných kľúčov (PKI)

- Certifikačná autorita
- Certifikát verejného kľúča:
  - Sériové číslo
  - Identifikácia subjektu
  - Verejný kľúč (vrátane identifikácie algoritmu)
  - Účel použitia (podpisová schéma, šifrovanie a pod.)
  - Interval platnosti
  - ... <ďalšie údaje: SAN, URL pre CRL/OCSP atď.>
  - Podpis CA
- Reťaz certifikátov (nekoreňové CA)
- Certifikačný poriadok (Certification Practice Statement)

PKI

- Vydanie certifikátu
  - CSR (Certificate signing request), podpísaný žiadateľom
  - preverenie atribútov žiadateľa v CA (resp. RA)
- Overenie certifikátu (v aplikácii, v prehliadači)
  - atribúty (dátum platnosti, meno subjektu, korektnosť podpisu a pod.)
  - platnosť voči CRL/OCSP
- Zneplatňovanie certifikátov
- Dôvera v CA
  - reťaz certifikátov až po koreňovú CA
  - dôvera v koreňovú CA

PKI (2)

- EV certifikáty (Extended Validation)
  - dôkladnejšie overenie subjektu
  - striktnejšie pravidlá pre niektoré atribúty (napr. bez „*” v mene)
  - explicitný zoznam CA uvedený v prehliadači (Firefox, Chrome)
- Zneplatnené certifikáty – CRL vs. OCSP
- CRL – zoznam zneplatnených certifikátov
  - podpísaný CA, pravidelne vydávaný (napr. denne)
  - potrebné použiť aktuálny CRL
- OCSP – protokol pre zisťovanie stavu certifikátu
  - otázka na aktuálnu platnosť konkrétneho certifikátu
  - odpoveď podpísaná CA
- Čo ak CRL nevieme získať a OCSP server nie je dostupný?

Heslá

- Najčastejší prostriedok autentizácie
  - samostatne alebo v kombinácii s inými metódami
- Prostriedok pre zabezpečenie dôvernosti / integrity
  - napr. súkromných kľúčov v súboroch
- Problémy s použitím hesiel:
  - default heslá (zoznamy k dispozícii na webe)
  - ľahko uhádnuteľné heslá (nízka entropia v porovnaní s kľúčmi)
  - tažko zapamätateľné heslá (poznačené)
  - nevhodne uložené heslá (napr. v otvorenom tvare v DB)
  - prenášané cez nezabezpečený kanál (napr. telnet)
  - zdieľanie medzi systémami (dopady kompromitácie)

Heslá (2)

- Techniky útokov:
  - úplné preberanie (brute-force), slovníkové metódy, predvýpočty (napr. dúhové tabuľky)
- Politika hesiel a techniky pre bezpečné používanie hesiel:
  - dĺžka hesla, “pestrosť” použitých znakov (skupiny)
  - max. doba platnosti hesla, min. doba platnosti hesla
  - novosť hesla (história hesiel), odlišnosť od mena a iných dát
  - blokovanie prístupu po x neúspešných prihláseniach
  - spomaľovanie odozvy po neúspšnom prihásení, atď.
- Voľba hesla:
  - náhodne vygenerované (ťažké pamätať)
  - používateľ volí (predikovateľnosť, podobnosť atď.)
  - použitie hesiel odvodených z fráz, a pod.

Náhodnosť používateľských hesiel

Dĺžka hesla	PIN (10 znaková abeceda)	Všeobecné heslá (94 znaková abeceda)
4	9	10
8	13	18
10	15	21
16	21	30
22	27	38

- Príklad: 2012, LinkedIn, 6,5 mil. používateľských účtov
- 4 hodiny + slovníkový útok → cca. 900 tisíc hesiel
- Pokračovanie slovníkového útoku → cca. 2 mil. hesiel

Reálne heslá

1. password
2. 123456
3. 12345678
4. abc123 (+ 1)
5. qwerty (- 1)
6. monkey
7. letmein (+ 1)
8. dragon (+ 2)
9. 111111 (+ 3)
10. baseball (+ 1)
11. iloveyou (+ 2)
12. trustno1 (- 3)
13. 1234567 (- 6)
14. sunshine (+ 1)
15. master (- 1)
16. 123123 (+ 4)
17. welcome (nové)
18. shadow (+ 1)
19. ashley (- 3)
20. football (+ 5)
21. jesus (nové)
22. michael (+ 2)
23. ninja (nové)
24. mustang (nové)
25. password1 (nové)

Splashdata 2012 a porovnanie s 2011

Uloženie hesiel

- Zle:
  - V otvorenom tvare
  - Šifrované
  - Odtlačok s jednoduchou aplikáciou hašovacej funkcie
- Dobre: ireverzibilne + soľ + iterácie
- Soľ – (náhodný) individuálny reťazec
  - Pridávaná pri výpočte odtlačku
  - Znemožňuje útočníkovi predvýpočty, paralelné prehľadávanie rovnakých hesiel (vedú k rôznym odtlačkom)
- Iterácie – spomalenie výpočtu odtlačku
  - Spomalenie overenia hesla (nevadí), spomalenie útoku (vyhovuje)
- Vhodné algoritmy: PBKDF2, bcrypt, scrypt
- Zlé heslo je zlé bez ohľadu na uloženie (slovníkový útok)

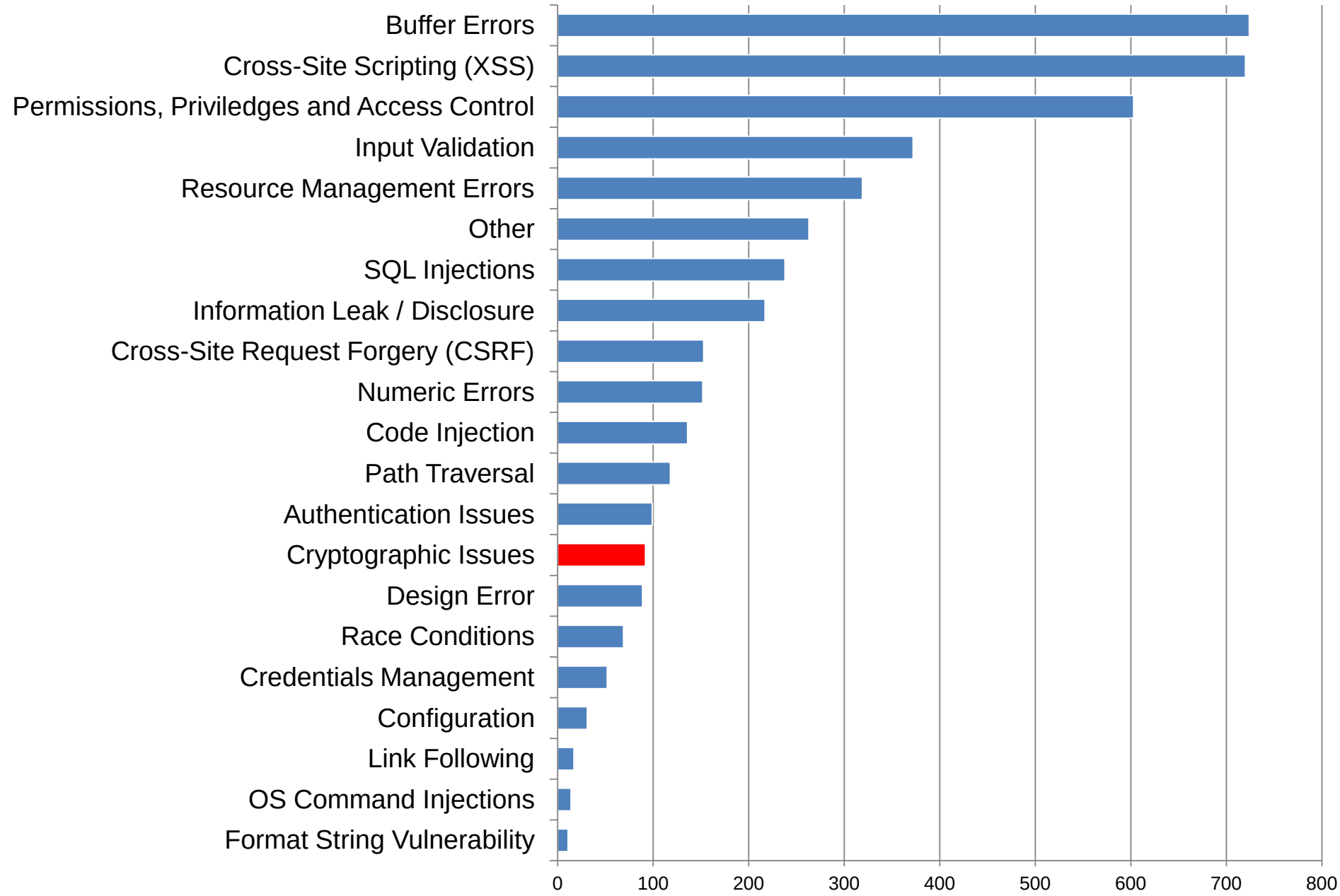
Implementácia a prevádzka

- Útoky na kryptografické mechanizmy
  - Obvykle sú slabiny v správe kľúčov a v implementácii
  - Protokoly – zvyčajne slabiny v protokole, bez ohľadu na algoritmy
- Niektoré implementačné slabiny/útoky
  - Útok postrannými kanálmi (napr. timing útok)
  - Nesplnenie bezpečnostných predpokladov (napr. náhodnosť)
  - Slabiny v protokoloch (napr. útoky na SSL/TLS)
  - Slabé algoritmy (napr. proprietárne algoritmy ako CCS)

Kryptografia a zraniteľnosti

- NIST: NVD (National Vulnerability Database)
  - SW zraniteľnosti a ich klasifikácia (typ, závažnosť a pod.)
- Najčastejšie zraniteľnosti v „Cryptographic Issues“:
  - použitie nekvalitného zdroja náhodnosti pri generovaní kľúčov,
  - nedostatočná (neúplná) kontrola certifikátov,
  - nekorektná implementácia kryptografických algoritmov alebo protokolov,
  - fixné heslá servisných účtov alebo heslá odvodené z verejne známych údajov

Počty zraniteľností publikovaných v roku 2012 podľa NVD



Štandardy

- Kryptografické algoritmy (šifry, podpisové schémy, hašovacie funkcie)
  - Primárne NIST, široká akceptácia
- Protokoly
  - Zvyčajne RFC
- Štandardy v IB riešia kryptografiu len okrajovo
- ISO/IEC 27000:
  - Politika používania kryptografických opatrení
  - Riadenie kľúčov
- ISO/IEC 15408 (Common Criteria):
  - Správa kryptografických kľúčov
  - Prevádzka kryptografie

FIPS PUB 140-2

- Security Requirements for Cryptographic Modules
- 4 bezpečnostné úrovne
- Oblasti: špecifikácia modulu, role, služby, autentizácia, fyzická bezpečnosť modulu, samotestovanie, správa kľúčov, elektromagnetické vyžarovanie a ďalšie
- Certifikované moduly v roku 2012
  - 68 osvedčení na úrovni 1, 95 na úrovni 2, 37 na úrovni 3 a žiadne na úrovni 4
- Certifikácia nie je zárukou bezpečnosti
  - Príklad: certifikované USB kľúče

Legislatíva SR

- Výnos Ministerstva financií SR č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy (časť Technické štandardy):
  - IPSec, SSL alebo TLS, S/MIME
  - Zmienky o ďalších konštrukciách ... bez konkrétnych detailov
- Zákon č. 215/2002 o elektronickom podpise
  - Bez technických podrobností
  - Vyhlášky NBÚ SR, najmä č. 135/2009 (formáty, algoritmy a pod.)
- Zákon č. 215/2004 o ochrane utajovaných skutočností
  - Šifrová ochrana informácií
  - Podrobnosti sú utajovanou skutočnosťou

Odporúčania 1

- ✓ Používajte štandardné kryptografické algoritmy, schémy a protokoly
- ✓ Používajte dostatočné dĺžky kľúčov
- ✓ Pravidelne meňte kľúče a heslá
- ✓ Dbajte na kvalitné generovanie kľúčov a voľbu hesiel
- ✓ Majte premyslené, čo robiť po kompromitácii kľúčov alebo hesiel
- ✓ Ak môžete, použite certifikované riešenia
- ✓ Poznajte konfiguračné možnosti kryptografických riešení a ich bezpečnostné dopady
- ✓ Dôsledne overujte certifikáty verejných kľúčov
- ✓ Koreňové certifikáty získajte dôveryhodným spôsobom

Odporúčania 2

- ✓ Uprednostnite AES-256 a SHA-512 pred inými symetrickými šiframi a hašovacími funkciami
- ✓ Ak môžete, uprednostnite schémy založené na eliptických krivkách
- ✓ Ak používate RSA schémy, uprednostnite RSA-OAEP pre šifrovanie a RSA-PSS pre podpisovanie
- ✓ Použite hašovaciu funkciu s dvojnásobnou dĺžkou odtlačku ako je dĺžka symetrického kľúča
- ✓ Heslá ukladajte a overujte vhodným spôsobom (algoritmus, soľ, počítadlo)
- ✓ Analyzujte činnosť aplikácie, ak kryptografické služby (napr. pre overenie platnosti certifikátu) nebudú k dispozícii
- ✓ V praxi často krát požiadavky na funkčnosť a pohodlie víťazia nad bezpečnosťou – dbajte, aby to nebolo K.O.

Varovania

- Kryptografia nie je miesto na kreativitu a ad-hoc riešenia
- Dlhodobo nezmenené kľúče považujte za prezradené
- Šifrovanie nezabezpečuje integritu ani autentickosť údajov
- Autentizačné kódy ani digitálne podpisy nezabezpečujú dôvernosť
- Obvykle je heslo najslabším „kľúčom“ v systéme
- Samopodpísaný certifikát nehovorí nič o autentickosti verejného kľúča
- Certifikácia nie je náhradou bezpečného používania
- Kryptografia nenahradí iné organizačné a technické bezpečnostné opatrenia

Ďakujem za pozornosť