Kryptológia – úvod

Peter Gaži

Katedra informatiky
FMFI UK, Bratislava
gazi@dcs.fmph.uniba.sk

Úvod do informačnej bezpečnosti
5/4/2011
(autor slidov: Martin Stanek)

Informačná bezpečnosť a kryptológia

- ukradnutý notebook s osobnými údajmi
  - bol disk šifrovaný? ako?
  - hardvérové šifrovanie disku + RFID kľúč
    - AES-128 – realita: 512B sektory xorované konštantným reťazcom
  - Cold Boot útok na šifrované disky (BitLocker, . . .)
  - Evil maid – útok na šifrovanie disku
- USB kľúč s klasifikovanými dátami zabudnutý vo verejnom počítači
  - FIPS 140-2 certifikované šifrované USB kľúče
    - problém s autentizáciou
- ukradnutý súbor so zahashovanými prístupovými heslami
- software využívajúci MD5
- slabý PRNG v Debiane, Ubuntu

Obsah

Úvod

- kryptológia – jadro informačnej bezpečnosti
- kryptológia = kryptografia + kryptoanalýza
- kryptografia slúži na zabezpečenie:
  - dôvernosti – šifrovanie
  - integrity a autentickosti – podpisy
- ďalšie objekty záujmu:
  - zdieľanie tajomstva
  - výpočty na súkromných dátach
  - e-cash
  - e-voľby
  - . . .

Úvod

- kryptológia – jadro informačnej bezpečnosti
- kryptológia = kryptografia + kryptoanalýza
- kryptografia slúži na zabezpečenie:
  - dôvernosti – šifrovanie
  - integrity a autentickosti – podpisy
- ďalšie objekty záujmu:
  - zdieľanie tajomstva
  - výpočty na súkromných dátach
  - e-cash
  - e-voľby
  - . . .

„Jadro“

- informačná bezpečnosť ⧹ kryptológia = ???
- kvalitná kryptografia je nutná, ale nie postačujúca
- poskytuje (falošný?) pocit bezpečia
  - „šifrujeme“ – ako? mód? správa kľúčov? kontext? . . .
  - „podpisujeme“ – ako? implementácia? správa kľúčov? . . .
- kryptológia
  - matematika
  - detaily sú podstatné
  - idealizované prostredie
  - implementácia a použitie

„Jadro“

- informačná bezpečnosť ⧹ kryptológia = ???
- kvalitná kryptografia je nutná, ale nie postačujúca
- poskytuje (falošný?) pocit bezpečia
  - „šifrujeme“ – ako? mód? správa kľúčov? kontext? . . .
  - „podpisujeme“ – ako? implementácia? správa kľúčov? . . .
- kryptológia
  - matematika
  - detaily sú podstatné
  - idealizované prostredie
  - implementácia a použitie

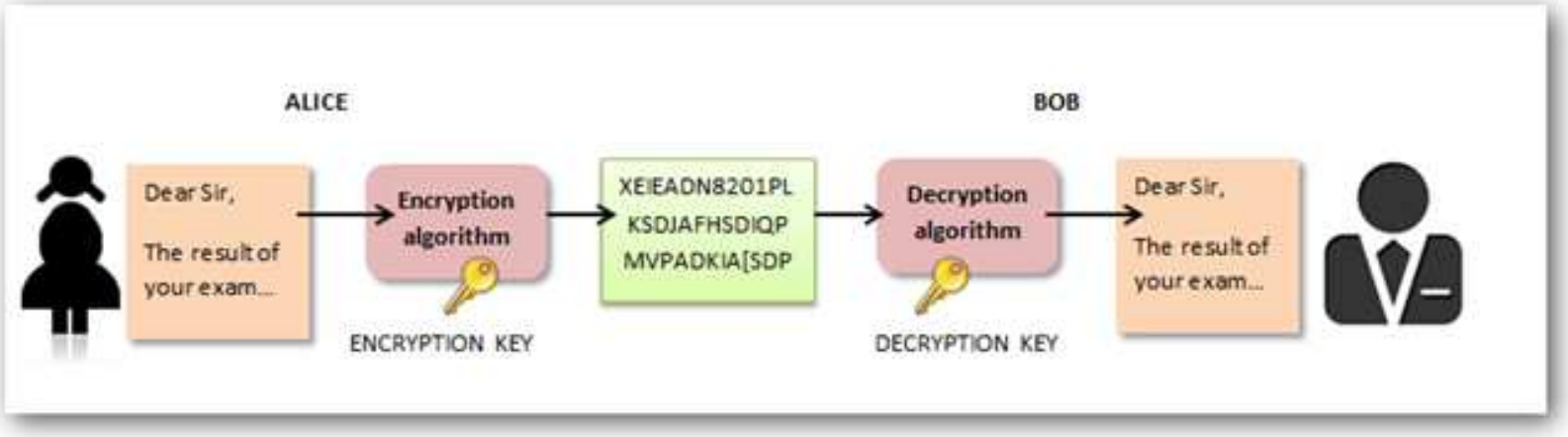
„Jadro“

- informačná bezpečnosť ⧹ kryptológia = ???
- kvalitná kryptografia je nutná, ale nie postačujúca
- poskytuje (falošný?) pocit bezpečia
  - „šifrujeme“ – ako? mód? správa kľúčov? kontext? . . .
  - „podpisujeme“ – ako? implementácia? správa kľúčov? . . .
- kryptológia
  - matematika
  - detaily sú podstatné
  - idealizované prostredie
  - implementácia a použitie

Symetrické šifrovanie – úvod 1

- klasický cieľ kryptografie – dôverný prenos dát
- komunikujúce subjekty zdieľajú tajný kľúč
- kľúč je rovnaký pre odosielateľa aj príjemcu $\Rightarrow$ symetrické šifrovanie
- otvorený text = pôvodná správa, text, dokument, dáta
- šifrový text = zašifrovaný text, výstupné dáta šifrovacieho algoritmu

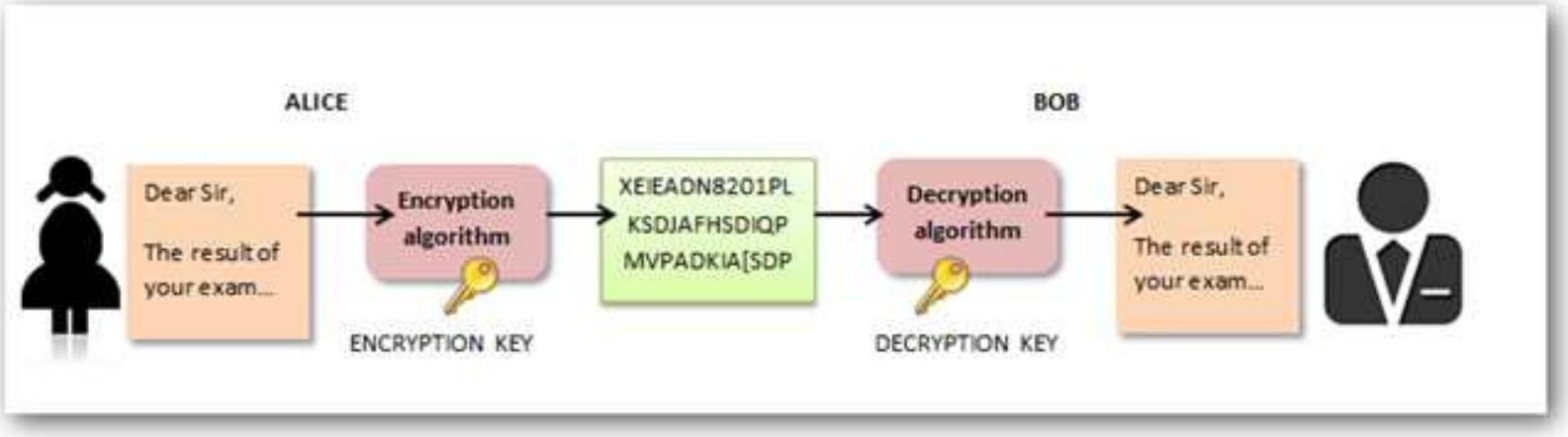
Symetrické šifrovanie – úvod 2



- šifrovanie: $E : P \times K \rightarrow C$
- dešifrovanie: $D : C \times K \rightarrow P$

- čo očakávame od E, D?

Symetrické šifrovanie – úvod 2



- šifrovanie: $E : P \times K \rightarrow C$
- dešifrovanie: $D : C \times K \rightarrow P$

- čo očakávame od E, D?

Symetrické šifrovanie – úvod 3

Očakávame:

- korektnosť:

$$\forall k \in K \ \forall p \in P : \quad D_k(E_k(p)) = p$$

- bezpečnosť: ako definovať?
- Kerckhoffov princíp:

  bezpečnosť šifrovania nezávisí na utajení algoritmu, ale výlučne na utajení kľúča

  (vs. security by obscurity)

Vernamova šifra (one-time pad)

- správa $m = m_1, m_2, \ldots, m_t \in \{0,1\}^t$
- kľúč $k = k_1, k_2, \ldots, k_t \in \{0,1\}^t$
- šifrovanie: $c = m \oplus k \qquad (c_i = m_i \oplus k_i)$
- dešifrovanie: $c \oplus k = (m \oplus k) \oplus k = m$

- výhody:
  - jednoduché (rýchle) šifrovanie a dešifrovanie
  - absolútne bezpečná šifra
- nevýhody:
  - kľúč rovnako dlhý ako otvorený text
  - „jednorazový“ kľúč

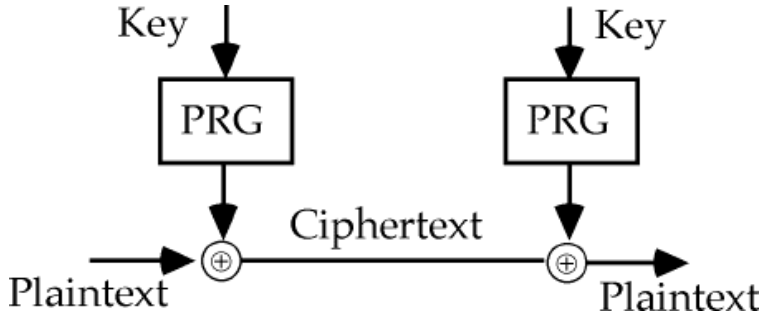
Vernamova šifra (one-time pad)

- správa $m = m_1, m_2, \ldots, m_t \in \{0,1\}^t$
- kľúč $k = k_1, k_2, \ldots, k_t \in \{0,1\}^t$
- šifrovanie: $c = m \oplus k \qquad (c_i = m_i \oplus k_i)$
- dešifrovanie: $c \oplus k = (m \oplus k) \oplus k = m$

- výhody:
  - jednoduché (rýchle) šifrovanie a dešifrovanie
  - absolútne bezpečná šifra
- nevýhody:
  - kľúč rovnako dlhý ako otvorený text
  - „jednorazový“ kľúč

Prúdové šifry

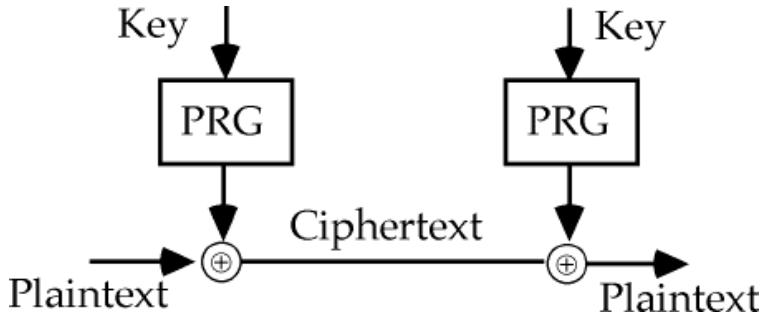
- krátky kľúč použitý na (deterministické) generovanie bežiaceho kľúča
- zväčša používané – (aditívne) synchrónne prúdové šifry
- najznámejšie prúdové šifry: RC4 (softvér), A5 (GSM), E0 (Bluetooth)



- zvyčajné výhody (oproti blokovým šifrám):
  - vhodné pre prúd OT, jednoduchší algoritmus, rýchlejšie šifrovanie/dešifrovanie
- zvyčajné nevýhody:
  - vyžadujú synchronizáciu, bez akejkoľvek integrity

Prúdové šifry

- krátky kľúč použitý na (deterministické) generovanie bežiaceho kľúča
- zväčša používané – (aditívne) synchrónne prúdové šifry
- najznámejšie prúdové šifry: RC4 (softvér), A5 (GSM), E0 (Bluetooth)



- zvyčajné výhody (oproti blokovým šifrám):
  - vhodné pre prúd OT, jednoduchší algoritmus, rýchlejšie šifrovanie/dešifrovanie
- zvyčajné nevýhody:
  - vyžadujú synchronizáciu, bez akejkoľvek integrity

Blokové šifry

- šifrovanie/dešifrovanie blokov dát: $E_k, D_k : \{0,1\}^n \rightarrow \{0,1\}^n$
- E_k a D_k sú inverzné bijekcie
- mód – spôsob šifrovania dlhých OT, napr.
  - ECB (Electronic Code Book)
  - CBC (Cipher Block Chaining)
  - CTR (Counter)
- najznámejšie blokové šifry: AES, (3)DES, RC5/6, IDEA, Blowfish, Twofish

Typy útokov na šifrovacie algoritmy

- základné útoky:
  - (COA) len so znalosťou šifrového textu
  - (KPA) so znalosťou otvoreného textu
  - (CPA) s možnosťou voľby otvoreného textu
  - (CCA) s možnosťou voľby šifrového textu
- ciele útokov:
  - získať kľúč
  - dešifrovať neznámy ŠT
  - zašifrovať nový OT
  - identifikovať, ktorému z dvoch OT zodpovedá daný ŠT
  - . . .

Typy útokov na šifrovacie algoritmy

- základné útoky:
  - (COA) len so znalosťou šifrového textu
  - (KPA) so znalosťou otvoreného textu
  - (CPA) s možnosťou voľby otvoreného textu
  - (CCA) s možnosťou voľby šifrového textu
- ciele útokov:
  - získať kľúč
  - dešifrovať neznámy ŠT
  - zašifrovať nový OT
  - identifikovať, ktorému z dvoch OT zodpovedá daný ŠT
  - . . .

Štandardy (blokové šifry)

- DES/3DES
  - predchádzajúci štandard, 70-te roky 20. storočia
  - bloková šifra, 64 bitov dlhý blok (málo!)
  - DES: dĺžka kľúča 56 bitov (málo!)
  - 3DES: dĺžka kľúča 168 (resp. 112) bitov
- AES (Advanced Encryption Standard)
  - algoritmus Rijndael
  - verejný výber štandardu (NIST, 1997-2001)
  - štandard: FIPS PUB 197, 2001
  - bloková šifra, 128 bitov dlhý blok
  - variabilná dĺžka kľúča: 128, 192, 256 bitov

Štandardy (blokové šifry)

- DES/3DES
  - predchádzajúci štandard, 70-te roky 20. storočia
  - bloková šifra, 64 bitov dlhý blok (málo!)
  - DES: dĺžka kľúča 56 bitov (málo!)
  - 3DES: dĺžka kľúča 168 (resp. 112) bitov
- AES (Advanced Encryption Standard)
  - algoritmus Rijndael
  - verejný výber štandardu (NIST, 1997-2001)
  - štandard: FIPS PUB 197, 2001
  - bloková šifra, 128 bitov dlhý blok
  - variabilná dĺžka kľúča: 128, 192, 256 bitov

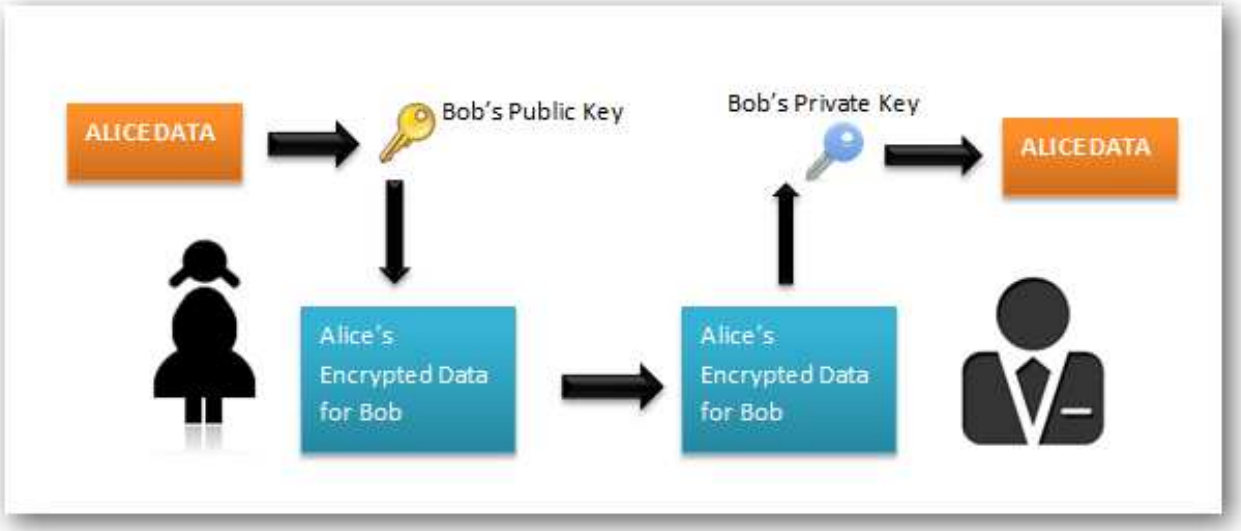
Výkon – softvérové implementácie

- knižnica Crypto++ v.5.6.0, (Windows Vista)
- hardvér: Intel Core 2, 1.83 GHz

alg.	**MB/s**
AES-128	109
AES-192	92
AES-256	82
3DES	13

- špecializovaný HW: AES-128 $\sim$ 21 Gbit/s

Asymetrické šifrovanie



- dvojica rôznych kľúčov:
  - verejný – šifrovanie $\Rightarrow$ ktokoľvek vie šifrovať
  - súkromný – dešifrovanie $\Rightarrow$ len vlastník vie dešifrovať
- jednoduchšia správa kľúčov
- bezpečnosť:
  - CPA útok je vždy možný
  - verejný kľúč $\not\rightarrow$ algoritmus na dešifrovanie
- najznámejšie systémy: RSA, ElGamal

RSA

- (1978) Rivest, Shamir, Adleman
- bezpečnosť súvisí s problémom faktorizácie veľkých čísel
- konštrukcia:
  - $n = p \cdot q$, p, q sú veľké prvočísla
  - $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$
  - verejný kľúč: (e, n)
  - súkromný kľúč: d
- šifrovanie ($E : Z_n \to Z_n$): $E(m) = m^e \bmod n$
- dešifrovanie ($D : Z_n \to Z_n$): $D(c) = c^d \bmod n$
- RSA je bijekcia
- RSA je deterministické (fuj!) $\Rightarrow$ v praxi sa znáhodňuje

RSA – štandardy

- RSA PKCS #1 v1.5
  - žiadny dôkaz bezpečnosti
  - verí sa, že je CPA-bezpečné
  - známy CCA útok
- RSA PKCS #1 v2.1 – RSA-OAEP
  - znáhodnený padding (zarovnanie)
  - „dôkaz“ bezpečnosti (v modeli s náhodným orákulom)

RSA – štandardy

- RSA PKCS #1 v1.5
  - žiadny dôkaz bezpečnosti
  - verí sa, že je CPA-bezpečné
  - známy CCA útok
- RSA PKCS #1 v2.1 – RSA-OAEP
  - znáhodnený padding (zarovnanie)
  - „dôkaz“ bezpečnosti (v modeli s náhodným orákulom)

Výkon – softvérové implementácie

- knižnica Crypto++ v.5.6.0, (Windows Vista)
- hardvér: Intel Core 2, 1.83 GHz

alg.	**MB/s**
AES-128	109
AES-192	92
AES-256	82
3DES	13

alg.	**ms/oper.**
RSA-1024 šifr.	0.08
RSA-1024 dešifr.	1.46
RSA-2048 šifr.	0.16
RSA-2048 dešifr.	6.08

Hybridné šifrovanie

- asymetrické šifry sú pomalé (v porovnaní so symetrickými)
- čo s prenosom objemných dát?
- riešenie:
  - šifrujme symetricky s náhodným kľúčom k
  - kľúč k zašifrujeme asymetricky pre adresáta

$$\langle AES_k(m), E_A^{\mathrm{RSA}}(k)\rangle$$

- v praxi špeciálne schémy (KEM – Key Encapsulation Method), napr. RSA-KEM (ISO/IEC 18033-2)

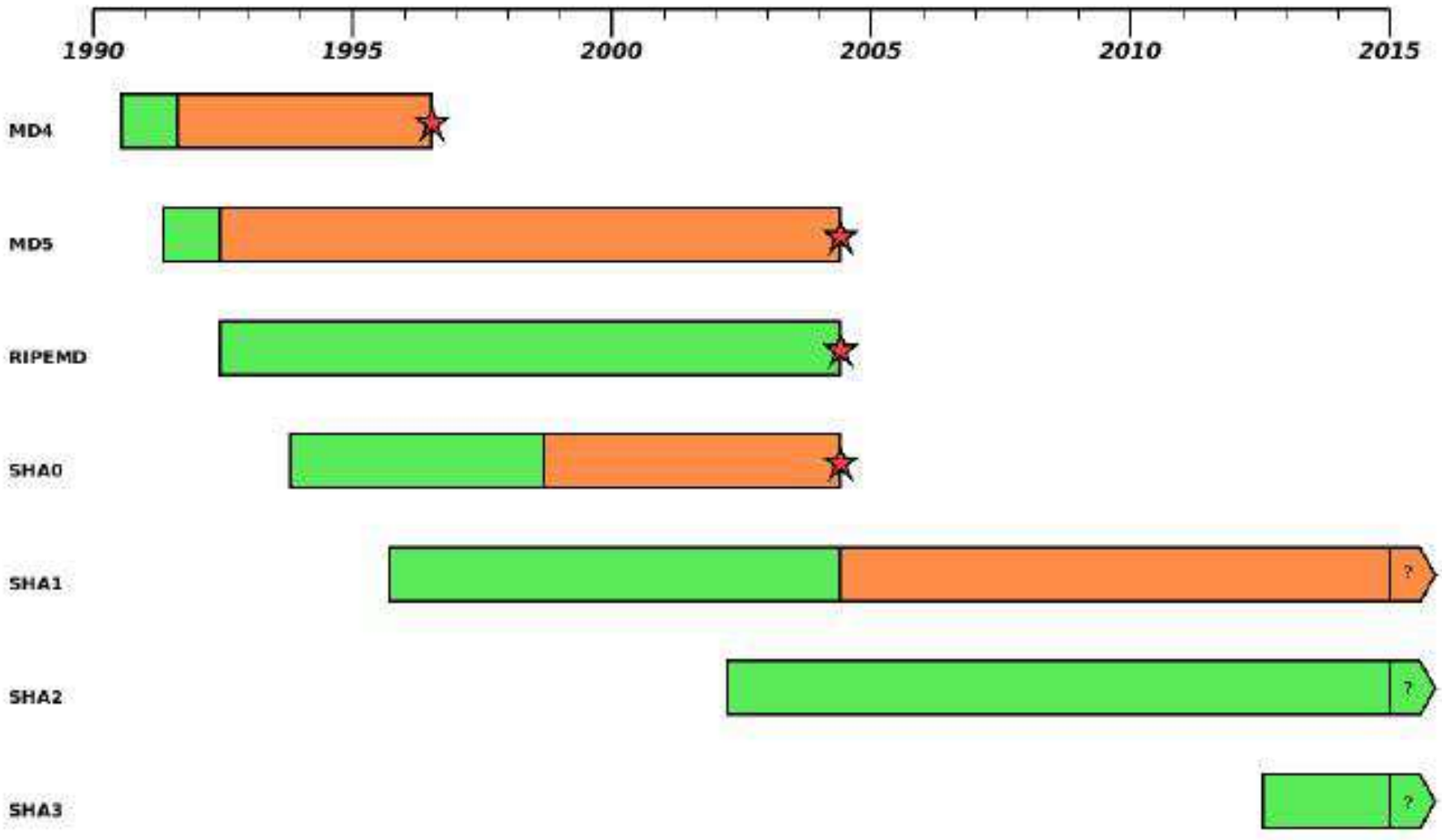
Hašovacie funkcie

- funkcia $h : \{0,1\}^* \rightarrow \{0,1\}^n$
- „odtlačok“ správy, dokumentu
- kontrola integrity, digitálne podpisy
- kryptografické vlastnosti:
  - jednosmernosť: pre dané y nájsť x: $h(x) = y$
  - odolnosť voči kolízám: nájsť $x \neq x'$: $h(x) = h(x')$
- najznámejšie hašovacie funkcie: MD5, SHA1, SHA-(224,256,384,512)

Bezpečnosť hašovacích funkcií

- generický útok – narodeninový útok
  - hľadanie kolízií
  - využíva tzv. „narodeninový“ paradox
  - zložitosť útoku $O(2^{n/2})$
- nedávne výsledky:
  - kolízie v MD5 (2005), kolízie v certifikátoch (!)
  - SHA-1 (160 bitov) kolízie $\sim 2^{69}$

Útoky na rodinu MD/SHA



Zdroj: Thomas Peyrin, CCRG NTU, 2010

Výkon – softvérové implementácie

- knižnica Crypto++ v.5.6.0, (Windows Vista)
- hardvér: Intel Core 2, 1.83 GHz

alg.	**MB/s**
AES-128	109
AES-192	92
AES-256	82
3DES	13

alg.	**ms/oper.**
RSA-1024 šifr.	0.08
RSA-1024 dešifr.	1.46
RSA-2048 šifr.	0.16
RSA-2048 dešifr.	6.08

alg.	**MB/s**
SHA-1	153
SHA-256	111
SHA-512	99
Whirlpool	57

Autentizačné kódy správ (MAC)

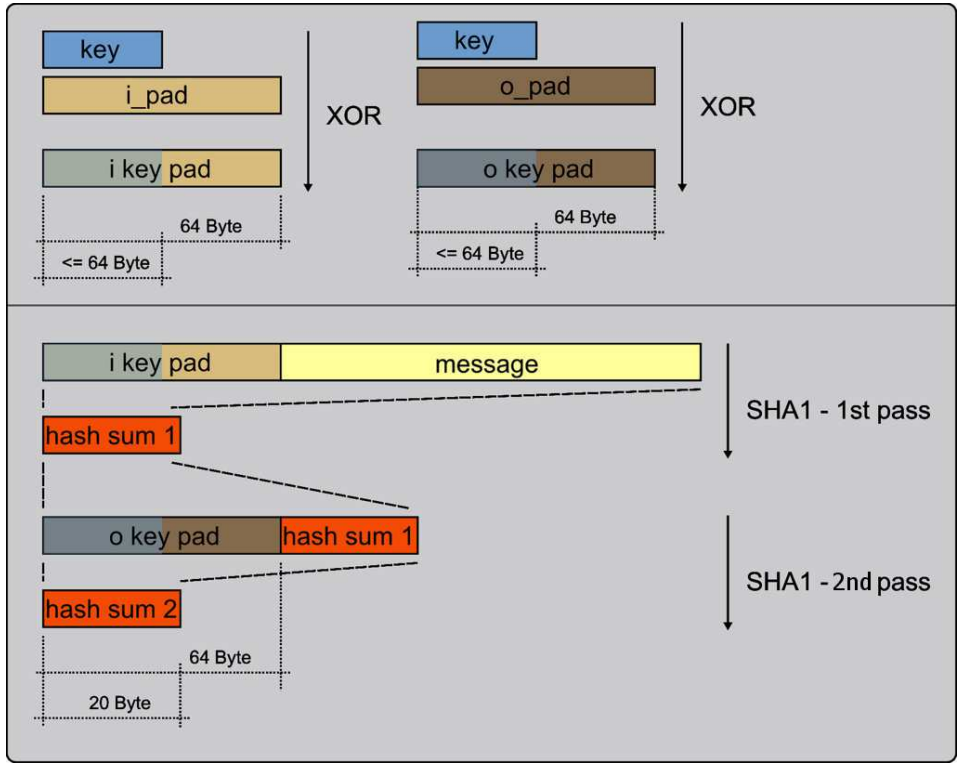
- hašovacie funkcie s kľúčom (symetrické)
- zabezpečenie autentickosti správ (bez nepopierateľnosti !)
- rýchle (oproti digitálnym podpisom)
- použitie napr. SSL/TLS, IPSec

HMAC

- najznámejšia konštrukcia: HMAC (RFC 2104)

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

- pre HMAC-MD5/SHA1 je opad = $(0x5C)^{64}$, ipad = $(0x36)^{64}$



Zdroj: Wikipedia

Digitálne podpisy

- autentickosť, integrita, nepopierateľnosť pôvodu . . .
- ekvivalent „vlastnoručného“ podpisu v elektronickom prostredí
- asymetrická schéma:
  - súkromný kľúč – podpisovanie $\Rightarrow$ len vlastník vie podpísať
  - verejný kľúč – overovanie $\Rightarrow$ ktokoľvek vie overiť
- podpis musí závisieť na podpisovanom dokumente/správe
- podpisuje sa odtlačok dokumentu ($H(m)$):
  - výkonové dôvody
  - bezpečnostné dôvody (falšovanie náhodnej správy)

RSA podpisy

- „prehodíme“ transformácie z klasického RSA:
  - podpisovanie: $s = H(m)^d \bmod n$
  - overovanie podpisu: platí $s^e \bmod n = H(m)$?
- (len tu!) bijektívnosť je zriedkavá vlastnosť asym. systémov
- v štandardoch zvyčajne so znáhodneným zarovnaním, napr. RSA-PSS (Probabilistic Signature Scheme) v RFC 3447, resp. v PKCS #1 v2.1

DSA

- DSA – Digital Signature Algorithm
- súčasť štandardu DSS (FIPS 186-2, draft 186-3)
- bezpečnosť súvisí s problémom diskrétneho logaritmu
- parametre:
  - p, q – 1024, resp. 160 bitové prvočísla, $q \mid (p-1)$
  - g – vypočítame $g = h^{(p-1)/q} \bmod p > 1$, kde $h \in_R \{2, 3, \ldots, p-2\}$
  - súkromný (podpisový) kľúč: $x \in_R Z_q^*$
  - verejný (overovací) kľúč: $y = g^x \bmod p$ a parametre p, q, g

DSA (pokračovanie)

- podpisovanie:
  1. $k \in_R \{1, \ldots q-1\}$
  2. $r = (g^k \bmod p) \bmod q$
  3. $s = k^{-1}(H(m) + xr) \bmod q$
- overovanie:
  1. $u_1 = H(m) \cdot s^{-1} \bmod q$
  2. $u_2 = r \cdot s^{-1} \bmod q$
  3. platí $(g^{u_1} \cdot y^{u_2} \bmod p) \bmod q = r$?
- nový štandard DSS (draft FIPS 186-3): predĺženie parametrov až na 3072/256 bitov

PKCS

- Public-Key Cryptography Standards
- implementačné štandardy (RSA Laboratories), napr.:

PKCS #1: RSA Cryptography Standard
PKCS #3: Diffie-Hellman Key Agreement Standard
PKCS #5: Password-Based Cryptography Standard
PKCS #7: Cryptographic Message Syntax Standard
PKCS #8: Private-Key Information Syntax Standard
PKCS #10: Certification Request Syntax Standard
PKCS #11: Cryptographic Token Interface Standard
PKCS #12: Personal Information Exchange Syntax Standard
PKCS #13: Elliptic Curve Cryptography Standard
PKCS #15: Cryptographic Token Information Format Standard

Bezpečnosť – dĺžka kľúča

- generický útok – úplné preberanie množiny K
- dostatočná veľkosť $|K|$ (dĺžka kľúča)
  - nutná, ale
  - nie postačujúca podmienka bezpečnosti
- aká dĺžka kľúča je dostatočná?
  - *Deep Crack – DES, 1998, $250k,* 1 *kľúč* $\sim$ 4 *dni*
  - *COPACOBANA – DES, 2007, $12 000,* 1 *kľúč* $\sim$ 6 *dni*
  - *odhady:* 80 *bitový kľúč* $\sim$ 1 *rok, $8M, 2006*
  - *odhady:* 80 *bitový kľúč* $\sim$ 1 *mesiac, $33M, 2010*
  - Von Neumann-Landauer limit: 128 bitov je dosť proti BF

  - ako dlho má šifra (ŠT) odolať („cena“ dát)?
  - aký progres v kryptoanalýze predpokladáme?
  - aký bude progres v technológii (Mooreov zákon)?
  - aký silný (ekonomicky) je/bude útočník?

Bezpečnosť – dĺžka kľúča

- generický útok – úplné preberanie množiny K
- dostatočná veľkosť $|K|$ (dĺžka kľúča)
  - nutná, ale
  - nie postačujúca podmienka bezpečnosti
- aká dĺžka kľúča je dostatočná?
  - *Deep Crack – DES, 1998, $250k,* 1 *kľúč* $\sim$ 4 *dni*
  - *COPACOBANA – DES, 2007, $12 000,* 1 *kľúč* $\sim$ 6 *dni*
  - *odhady:* 80 *bitový kľúč* $\sim$ 1 *rok, $8M, 2006*
  - *odhady:* 80 *bitový kľúč* $\sim$ 1 *mesiac, $33M, 2010*
  - Von Neumann-Landauer limit: 128 bitov je dosť proti BF

- ako dlho má šifra (ŠT) odolať („cena“ dát)?
- aký progres v kryptoanalýze predpokladáme?
- aký bude progres v technológii (Mooreov zákon)?
- aký silný (ekonomicky) je/bude útočník?

Bezpečnosť – dĺžka kľúča

- generický útok – úplné preberanie množiny K
- dostatočná veľkosť $|K|$ (dĺžka kľúča)
  - nutná, ale
  - nie postačujúca podmienka bezpečnosti
- aká dĺžka kľúča je dostatočná?
  - *Deep Crack – DES, 1998, $250k,* 1 *kľúč* $\sim$ 4 *dni*
  - *COPACOBANA – DES, 2007, $12 000,* 1 *kľúč* $\sim$ 6 *dni*
  - *odhady:* 80 *bitový kľúč* $\sim$ 1 *rok, $8M, 2006*
  - *odhady:* 80 *bitový kľúč* $\sim$ 1 *mesiac, $33M, 2010*
  - Von Neumann-Landauer limit: 128 bitov je dosť proti BF

  - ako dlho má šifra (ŠT) odolať („cena“ dát)?
  - aký progres v kryptoanalýze predpokladáme?
  - aký bude progres v technológii (Mooreov zákon)?
  - aký silný (ekonomicky) je/bude útočník?

Bezpečnosť – dĺžka kľúča 2

- rôzne doporučenia, rôzne metodiky výpočtu
- NSA Suite B Cryptography (2005)
- ECRYPT Report (2008)
- NIST Recommendations (2006)
- ...a ďalšie (`www.keylength.com`)

NSA Suite B Cryptography (2005)

- pre komerčne dodávané systémy
- (Suite A – neverejné algoritmy, neznáme dĺžky kľúčov)
- algoritmy:
  - šifrovanie: AES (FIPS 197)
  - podpisy: ECDSA (FIPS 186-2)
  - hašovanie: SHA-2 (FIPS 180-2)
  - výmena kľúčov: ECDH

	sym. šifr.	EC (GF(p))	EC (GF(2^n))	hašovanie
Secret	128/256	256	283	256
Top Secret	256	384	409	384

ECRYPT Report (2010)

- ECRYPT – európska sieť excelencie v kryptológii
- rôzne aktivity
- každoročný report o doporučených dĺžkach kľúčov
- level 1-8
  - level 4 – najmenšia všeobecná ochrana (do 4 rokov)
    „veľmi krátkodobá ochrana voči agentúram“
  - level 7 – dlhodobá ochrana (cca. 30 rokov)
  - level 8 – „prevídateľná budúcnosť“

	sym. šifr.	RSA	EC	hašovanie
level 4	80	1 248	160	160
level 7	128	3 248	256	256
level 8	256	15 424	512	512

Protokoly

- rôzne typy protokolov (účel):
  - výmena (distribúcia/dohoda) kľúča
  - autentizácia subjektu
  - slepé podpisy, voľby, peniaze, . . .
- bezpečnosť závisí na schopnosti útočníka:
  - odpočúvať / modifikovať ľubovoľné správy
  - legitímny subjekt prostredia / mimo
- (zvyčajne) chceme protokol odolný voči najsilnejšiemu útočníkovi

Diffieho-Hellmanov protokol

- protokol na dohodnutie kľúča
- súvisí s problémom diskrétneho logaritmu (DH problém)

$$A \to B: \quad X = g^x$$
$$B \to A: \quad Y = g^y$$
výsledný kľúč: $K = X^y = Y^x = g^{xy}$

- man-in-the-middle útok (len pre aktívneho útočníka)
- schopnosť overiť autentickosť dát (napr. dig. podpismi) znemožní MITM útok

SSL/TLS 1

- SSL – Secure Socket Layer (pôvodne Netscape)
- TLS – Transport Layer Security (v súčasnosti TLS 1.2, označovaný tiež SSL v3.3, spätne kompatibilný s SSL v3)

- protokol nad transportnou vrstvou (hlavne TCP, aj UDP, ...)
- zabezpečuje intergitu (sym. šifra) a dôvernosť (MAC)
- nad SSL protokol aplikačnej vrstvy (FTP, SMTP,. . .)
  - najčastejšie: HTTP/SSL (https)

SSL/TLS 2

TLS protokoly:

- Record Protocol – spodná vrstva (šifrovanie, MAC, kompresia[1])
- Handshake Protocol – autentizácia (jednostranná – len server, alebo vzájomná) dohoda o kryptografických algoritmoch, dohoda o šifrovacom kľúči a MAC kľúči
- Alert Protocol – oznamovanie chybových hlášok (napr. `certificate_expired`)
- Change Cipher Spec Protocol – „prepnutie“ algoritmov

Formát názvu cipher suite: `_KeyExchange_WITH_Cipher_MAC`

- napr.: `SSL_DHE_DSS_WITH_DES_CBC_SHA`
  `TLS_RSA_WITH_AES_256_CBC_SHA`

[1] ktorú nikto nepoužíva

SSL/TLS 2

TLS protokoly:

- Record Protocol – spodná vrstva (šifrovanie, MAC, kompresia[1])
- Handshake Protocol – autentizácia (jednostranná – len server, alebo vzájomná) dohoda o kryptografických algoritmoch, dohoda o šifrovacom kľúči a MAC kľúči
- Alert Protocol – oznamovanie chybových hlášok (napr. `certificate_expired`)
- Change Cipher Spec Protocol – „prepnutie“ algoritmov

Formát názvu cipher suite: `_KeyExchange_WITH_Cipher_MAC`

- napr.: `SSL_DHE_DSS_WITH_DES_CBC_SHA`
  `TLS_RSA_WITH_AES_256_CBC_SHA`

[1] ktorú nikto nepoužíva

IPSec

- bezpečnostný „doplnok“ k IP vrstve, pôvodne pre IPv6
- oblasti pôsobnosti: dôvernosť, autentickosť, správa kľúčov
- výhody „nízkoúrovňového“ protokolu:
  - zabezpečená celá komunikácia nad IP
  - transparentné pre aplikácie
  - možnosť vytvoriť VPN
  - integrácia do sieťových zariadení (smerovače a pod.)
- nevýhody:
  - SW implementácia (v operačnom systéme) zaťažuje server
  - identita zariadania, nie používateľa/aplikácie

IPSec 2

- základné protokoly – AH, EPS
- AH (Authentication Header) – len autentickosť/integrita
- ESP (Encapsulating Security Payload) – šifrovanie a voliteľne autentickosť/integrita
- transportný mód (spracúvajú sa vybrané časti IP paketu) a tunelovací mód (zabalenie celého IP paketu do nového)
- algoritmy: HMAC-MD5/SHA-1 (96), 3DES, Blowfish, . . .
- správa kľúčov: manuálna, automatizovaná

Kryptológia v kontexte

- aká dôveryhodná je implementácia?
- akým spôsobom sú spravované kľúče:
  - generovanie?
  - distribúcia?
  - backup?
  - riadenie prístupu?
  - ničenie?
- postranné kanály (čas, spotreba zdrojov, hyperthreading, chybové hlášky, . . .)?

. . . je ľahké urobiť chybu.

Kryptológia v kontexte

- aká dôveryhodná je implementácia?
- akým spôsobom sú spravované kľúče:
  - generovanie?
  - distribúcia?
  - backup?
  - riadenie prístupu?
  - ničenie?
- postranné kanály (čas, spotreba zdrojov, hyperthreading, chybové hlášky, . . .)?

. . . je ľahké urobiť chybu.

Kryptológia v kontexte 2

- kryptografia je obvykle použitá v niečom „väčšom“
- operačný systém, čipové karty, databázový systém, mail, webová aplikácia, e-commerce, sieťové protokoly, . . .

ISO/IEC 27002 (BS 7799)

- Code of practice for information security management

1. Risk assessment
2. Security policy
3. Organization of information security
4. Asset management
5. Human resources security
6. Physical and environmental security
7. Communications and operations management
8. Access control
9. Information systems acquisition, development and maintenance
10. Information security incident management
11. Business continuity management
12. Compliance

ISO/IEC 27002 (BS 7799) – hlbšie

- 8.3 Cryptographic controls

  8.3.1 Policy on the use of cryptographic controls
  8.3.2 Encryption
  8.3.3 Digital signatures
  8.3.4 Non-repudiation services
  8.3.5 Key management

ISO/IEC 27002 (BS 7799) – ešte hlbšie

- 8.3.5 Key management
- Existujú štandardy, procedúry a metódy pre:

1. Generating keys for different cryptographic systems
2. Generating and obtaining public key certificates
3. Distributing keys to intended users
4. Storing keys and how to obtain access to keys
5. Changing or updating keys
6. Dealing with compromised keys
7. Revoking and deactivating keys
8. Recovering keys that are lost or corrupted as part of BCM
9. Archiving keys
10. Destroying keys
11. Logging and auditing key management activities

Common Criteria

- ISO/IEC 15408 – Evaluation criteria for IT security
- použitie: jednotný jazyk pre
  - používatelov: špecifikujú požiadavky
  - výrobcov: popíšu vlastnosti produktov
  - nezávislé testovanie: vyhodnotí
- časti:
  - Part 1: Introduction and general model
  - Part 2: Security functional requirements
  - Part 3: Security assurance requirements
- EAL: evaluation assurance level

- flexibilné – hodnotenie veľkých systémov (napr. operačné systémy), aj malých (napr. čipové karty, aplikácie)

Common Criteria 2

- CC a kryptografické algoritmy:

  The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in ISO/IEC 15408. Should independent assessment of mathematical properties of cryptography embedded in a TOE be required, the evaluation scheme under which ISO/IEC 15408 is applied must make provision for such assessments.

Common Criteria 3

- požiadavky na bezpečnostné funkcie
- trieda FCS (Cryptographic support):
  - Správa kryptografických kľúčov
    - generovanie kľúčov
    - distribúcia kľúčov
    - prístup ku kľúčom
    - deštrukcia kľúčov
  - Kryptografická činnosť
- pre jednotlivé komponenty sa vyžaduje súlad s definovanými algoritmami, metódami, dĺžkami kľúčov, štandardmi.

FIPS 140-2

- Security Requirements for Cryptographic Modules
- požiadavky na kryptografické moduly (SW aj HW)
- 4 úrovne bezpečnosti:
  Level 1: najnižšia úroveň
  Level 2: + detekcia fyzickej manipulácie, . . .
  Level 3: + odolnosť voči fyzickej manipulácii, . . .
  Level 4: + . . .
- Level 1,2 – najčastejšie úrovne
  - (za rok 2008) 83 certifikátov L1, 91 L2, 19 L3, 2 L4
- FIPS 140-2 $\rightsquigarrow$ ISO/IEC 19790:2006 Security requirements for cryptographic modules
- existuje už draft FIPS 140-3

FIPS 140-2 (oblasti)

1. Špecifikácia (dokumentácia) modulu
2. Časti modulu a rozhrania (vrátane segregácia)
3. Role, služby a autentizácia
4. Konečnostavový model
5. Fyzická bezpečnosť
6. Operačné prostredie (operačný systém)
7. EMI/EMC
8. Správa kryptografických kľúčov
9. Samotestovanie
10. Záruky pre kvalitu návrhu a implementácie
11. Ochrana pred útokmi

Záver

- bez kryptológie je ťažké (nemožné?) dosiahnuť bezpečnosť IS

- niekedy sú použité kryptografické konštrukcie zlé
- niekedy sú kryptografické konštrukcie použité zle

. . . ale občas sa to (náhodou?) podarí.