Problémy elektronickej archivácie

Prof. RNDr. Otokar Grošek, PhD.
Ing. Vladislav Novák
Mgr. Marek Sýs
Ing. Pavol Zajac
Crypto Group,
Katedra Aplikovanej Informatiky a Výpočtovej Techniky,
FEI STU

Prehľad problematiky

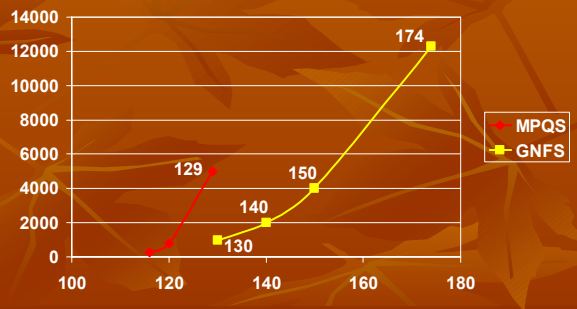
- Problém uchovávania dokumentov:
  - Dostupnosť, Integrita, Nepopierateľnosť.
  - Bezpečnosť (Dôvernosť) x Prístup.
- Prostriedky:
  - Symetrická a asymetrická kryptografia,
  - Elektronický podpis a sústava PKI, časové pečiatky a protokoly,
  - Režimové a organizačné opatrenia, predpisy…

Bezpečnosť algoritmov

Dek. cifier	Dátum	MIPS-roky	Alg.
120	Jún 1993	830	MPQS
129	**Apr. 1994**	**5000**	**MPQS**
130	***Apr. 1996***	***1000***	***GNFS***
140	Feb. 1999	2000	GNFS
155	Aug. 1999	8000	GNFS
174	Dec. 2003	13200	GNFS

MIPS-rok: Doba výpočtu v rokoch na počítači s výkonom 1 MIPS

Vývoj faktorizácie



Odhad bezpečnosti RSA

Posledné známe rekordy

- RSA-576 –December 2003
- DL:
  - GF(p), p – 400 bitové prvočíslo, 2001
  - GF(2^607), 2002.
- ECC:
  - ECCp-109, Nov. 2002
  - ECC2-109, Apríl 2004

Odporúčané dĺžky kľúčov

- Obmedzená životnosť elektronického podpisu.

Rok	RSA/DSA	ECDSA
2004	*1024*	*160*
2014	1536	192
2024	2048	224
2054	4096	256

Hardvér budúcnosti

- TWIRL – špecializovaný HW na faktorizáciu RSA.
- Kvantový počítač:
  - Prehodnotenie algoritmov.

Životnosť médií

- Životnosť nosičov je obmedzená:
  - Morálna životnosť – neustále nové nosiče.
  - Fyzická životnosť – napr. „CD pleseň“ – oxidácia ochrannej vrstvy.
- Problém získať čítacie zariadenie
  - Môžeme mať v centrálnom archíve, ale pre koncového používateľa treba „prekopírovať“.
  - Proprietárne formáty dát.

Uchovávanie dokumentov

- Súkromná sféra:
  - Trezor, firemná LAN/SAN, ...
  - Zodpovedajú sami za svoje dokumenty.
- Polosúkromná (certifikovaná) sféra:
  - Notár, banka, ...
  - Musia sa riadiť predpismi, licenciou.
- Štátna sféra:
  - Štátny archív, matrika, kataster, vojenský archív, ...
  - Organizačne najnáročnejšie,
  - Konflikt verejného záujmu a potreby ochrany.

Podpisovanie a archivácia

- Potrebné stanoviť zodpovednosti za archivovaný dokument.
- Nutnosť časových pečiatok a zabezpečenej evidencie:
  - Je treba evidovať napr. aj CRL.
- Špeciálne formáty a protokoly podpisovania
  - Archívny zaručený elektronický podpis.
  - Zdieľané podpisovanie.

Legislatíva

- Vyhláška NBÚ 542/2002 Zb. o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku,
- §8 - Spracovanie elektronického dokumentu:
  - (1) Orgán verejnej moci alebo orgán verejnej správy po prevzatí elektronického dokumentu s ním zaobchádza obdobným spôsobom ako s písomnosťou.
- Zákon o utajovaných skutočnostiach.
- Príprava novely Zákona o elektronickom podpise.