Crypto-World

Informační sešit GCUCMP
ISSN 1801-2140

Ročník 12, číslo 12/2010 **19. prosinec 2010**

12/2010

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1366 registrovaných odběratelů)

Obsah: str.

A. Finále SHA-3 - překvapení a zklamání

Vlastimil Klíma, kryptolog, KNZ, s.r.o., Praha
(http://cryptography.hyperlink.cz, vlastimil.klima@knzsro.cz)

Ve čtvrtek 9. prosince se zpožděním tří měsíců NIST vyhlásil pět algoritmů, které ze 14 kandidátů postoupily do třetího závěrečného kola soutěže SHA-3. Finalisty se staly algortitmy **BLAKE, Grostl, JH, Keccak a Skein**. NIST k tomu vydal krátkou zprávu v oficiálním emailu, kterou si zde můžeme přeložit. Vynecháme ovšem oficiality. Takže máme toto zdůvodnění:

- Bezpečnost byla naše nejdůležitější starost.
- Avšak bezpečnost bez rychlosti nemá smysl, proto NIST chtěl vysoce bezpečné algoritmy, které měly dobrý výkon.
- Preferovali jsme konzervativismus v bezpečnosti, a tak jsme v některých případech nevybrali algoritmy s výjimečnou výkonností, zejména z důvodu, že jsme u nich byli z něčeho nervózní, i když jsme neznali žádný skutečný útok na ně.
- Výkon je mnoharozměrný a žádný z algoritmů nevynikal na všech platformách. Byly větší rozdíly na omezených platformách a v hardwéru, kde plocha je stejně důležitá jako rychlost.
- Nemohl postoupit žádný z algoritmů, který neměl jasnou rundovní strukturu, která by mohla být jednoduše přizpůsobena, aby mohla vyvažovat vztah mezi bezpečností a rychlostí.
- NIST vyloučil několik algoritmů z důvodu šíře jejich změn při postupu do druhého kola.
- NIST také uvažoval rozmanitost finalistů.
- NIST bude publikovat zprávu o výběru finalistů.

http://csrc.nist.gov/groups/ST/hash/sha-3/Round3/submissions_rnd3.html

	Narrow-Pipe	MD	Wide-Pipe	MD	Sponge	Sponge-Like
Bitsliced	*Hamsi*		*JH*		*Keccak*	*Luffa*
AES	*Shavite3*		*Echo*	*Grostl*		*Fugue*
ARX	*Skein*	BLAKE	*BMW*		*Cube*	
Logical/ ARX			*SIMD*	*Shabal*		

Výběr NISTu je překvapující, na tom se shodnou skoro všichni. Překvapením ovšem nemilým pro trojici silných kandidátů Shabal, SIMD a (omluvte moji ješitnost) také BMW. Jejich místo nahradili Grostl, JH a Keccak. Proč, to je záhadou, kterou jistě vysvětlí podrobná zpráva o výběru, která má brzy následovat.

Protože náš kandidát byl také vyřazen, dovolím si malou poznámku. Pro BLAKE a Skein by jakýkoliv z algoritmů Shabal, SIMD a BMW byl lepším soupeřem než jakýkoliv z trojice Grostl, JH a Keccak. Ovšem v článku v předchozím čísle Crypto-worldu jsme uvedli důvody NISTu, které zvažuje pro výběr finalistů. A tam nikde není kritérium vybrat pět "nejlepších", ale množinu algoritmů s nějakými vlastnostmi. Vlastností, kterou má množina algoritmů splňovat, je více, a jak je vidět, zde je velmi zřetelně dvakrát naplněno kritérium antimonokultury: "z každého odlišného strukturálního návrhu vybrat jednoho kandidáta" a "vybrat zástupce různých použitých operací".

Podívejme se na tabulku, s níž jsme si minule hráli a na skutečný výběr. Z každého sloupce je vybrán jen jeden kandidát. Z každého řádku, kromě posledního, je také vybrán alespoň jeden kandidát. Pokud bychom ovšem hráli s NISTem tuhle křížovku, museli bychom místo JH vybrat SIMD. Kvalita a rychlost SIMD je podle našeho mínění lepší než JH, ale to už je věcí NISTu.

	Narrow-Pipe	MD	Wide-Pipe	MD	Sponge	Sponge-Like
Bitsliced	*Hamsi*		*JH*		*Keccak*	*Luffa*
AES	*Shavite3*		*Echo*	*Grostl*		*Fugue*
ARX	*Skein*	BLAKE	*BMW*		*Cube*	
Logical/ ARX			*SIMD*	*Shabal*		

Řada lidí z kryptokomunity je tímto výběrem diplomaticky řečeno, hm ... *překvapena*. Proč? Myslíme si, že algoritmy Grostl, JH a Keccak nemají oproti Skein a BLAKE žádnou šanci.

Tým BMW byl také překvapen a pochopitelně i zklamán, neboť náš miláček v soutěži tímto končí. Ovšem kryptografické hřbitovy jsou plné "nadějných" i "bezpečných" algoritmů, budiž tedy i BMW země lehká. Finalistům jsem osobně blahopřál, neboť jak praví klasik: Show must go on!

B. Finále SHA-3 – jak to vidím já

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Když 10.12.2010 zveřejnil v NEWS na našem webu V.Klíma informaci, že do finále SHA-3 postupuje **BLAKE, Grostl, JH, Keccak a Skein**, byl jsem opravdu velmi překvapen.

(http://crypto-world.info/news/index.php?prispevek=13806&sekce=c).
Byl jsem přesvědčen, že **BMW** – nejrychlejší algoritmus z kandidátů druhého kola, do kterého se dostaly již pouze algoritmy bez známých bezpečnostních problémů, bude vzhledem k této výhodě jasným postupujícím.

Ještě týden předtím 3.12 na mezinárodní konferenci MKB v Praze (http://mkb.buslab.org/) další z tvůrců algoritmu BMW Danilo Gligoroski také na přímý dotaz, které algoritmy mají šanci postoupit do třetího kola, dal najevo, že očekává, že mezi nimi BMW bude.

Začal jsem tedy hledat na internetu důvody proč tomu tak není. Jenže oblíbený Google mi odpovědět nedal. Celé tři dny se totiž dokonce nedaly na Internetu najít skoro vůbec žádné komentáře k tomuto výběru. Prakticky bylo jen opakováno to, co napsal NIST a upřímně řečeno, NIST toho mnoho nenapsal.

Co mně zaujalo je, že NIST nikde nedeklaroval, že kritérium je vybrat pět "nejlepších", ale je z jeho komentářů jasné, že se snažil vybrat množinu algoritmů s nějakými vlastnostmi. Vlastností, kterou má množina algoritmů splňovat, je více, a jak je vidět, zde je velmi zřetelně naplněno kritérium antimonokultury, tj. "z každého odlišného strukturálního návrhu vybrat jednoho kandidáta" a "vybrat zástupce různých použitých operací".

Já však vidím výběr i tak trochu „politicky“. Mnohokulturnost výběru pokryla totiž i všechny světadíly. K americkému (tedy alespoň formálně) algoritmu Skein a třem vybraným evropským algoritmům BLAKE, Keccak and Grøstl byl „přidán“ asijský JH (Singapore).
Vlasta ve svém článku poukazuje na to, že by si uměl představit místo JH např. SIMD, ale to je opět evropský kandidát… ostatně BMW je také evropský kandidát…

Když již píši o „politice“, pak si dovolím zákulisní drb. Stejně se očekává, že vítěz bude Bruce Schneier, pardon algoritmus **Skein**. V soutěži, kde žádný z algoritmů nemá zjevné bezpečnostní vady, již hrají i jiné faktory. PR má Bruce Schneier již tradičně nejlepší a chvála na Skein je tak zaručena.

Se zájmem jsem proto očekával, co Bruce Schneier ve svém CRYPTO-GRAMMU o výběru postupujících napíše (mimochodem CRYPTO-GRAMM má již 125 000 čtenářů).
V prosincovém čísle (15.12) je pouze velmi stručný komentář, ze kterého plyne, že výběrem JH byl také překvapen. Tvrdí zde, že výběr ostatních čtyř kandidátů očekával.

Ani on se však nepouští do úvah, PROČ byli jednotliví kandidáti vybráni či vyřazeni, a proto skončím tak jako on:

NIST will publish a report that explains its rationale for selecting the five it did.
NIST zveřejní zprávu, která vysvětluje jeho důvody pro výběr těchto pěti kandidátů.

Osobně jsem na zprávu velmi zvědavý. Zajímá mne, která kritéria „převálcovala“ původně jasně stanovený cíl najít bezpečný algoritmu, který je rychlejší než SHA-2.

C. Novela rozhodnutí Komise 2009/767/ES

Pavel Vondruška (pavel.vondruska@crypto-world.info)

1999

Povinnost uznávat kvalifikované certifikáty vydané poskytovateli certifikačních služeb usazenými v jiných státech EU je zakotvena již v čl. 3 odst. 7 **Směrnice č. 1999/93/ES**, a to zejména v jeho poslední větě. Cesta ke skutečnému naplnění této povinnosti byla však dlouhá a vůbec ne přímočará.

2006

Rozhodnutí Rady 2006/123/ES o službách na vnitřním trhu (dále jen „Rozhodnutí“) uložilo členským státům povinnost uvést do provozu nástroj umožňující vzájemné uznávání kvalifikovaných certifikátů, na kterých jsou založeny zaručené elektronické podpisy. Tímto nástrojem se staly „důvěryhodné seznamy“ (dále jen TSL - Trusted Services Lists), které obsahují údaje o poskytovatelích certifikačních služeb, kteří vydávají kvalifikované certifikáty pro veřejnost v daném státu a kteří jsou zároveň akreditováni, resp. jsou pod dohledem (dozorem) orgánu, který je v daném státu k tomu určen.

Každý stát má podle tohoto rozhodnutí povinnost vytvářet vlastní TSL, který bude k dispozici uživatelům ze všech členských států. Pomocí tohoto TSL bude možné ověřit, zda je certifikát kvalifikovaný ve smyslu směrnice 1999/93/ES.

2009

Teprve však **Rozhodnutí 2009/767/ES** lze považovat za akt, kterým Komise Evropských společenství odstranila překážky pro faktickou realizaci vzájemného uznávání kvalifikovaných certifikátů. Povinnost uznávat kvalifikované certifikáty vydané poskytovateli certifikačních služeb usazenými v jiných státech EU nastala dne 28. 12. 2009 nejen pro jednotná kontaktní místa, ale i pro orgány veřejné moci.

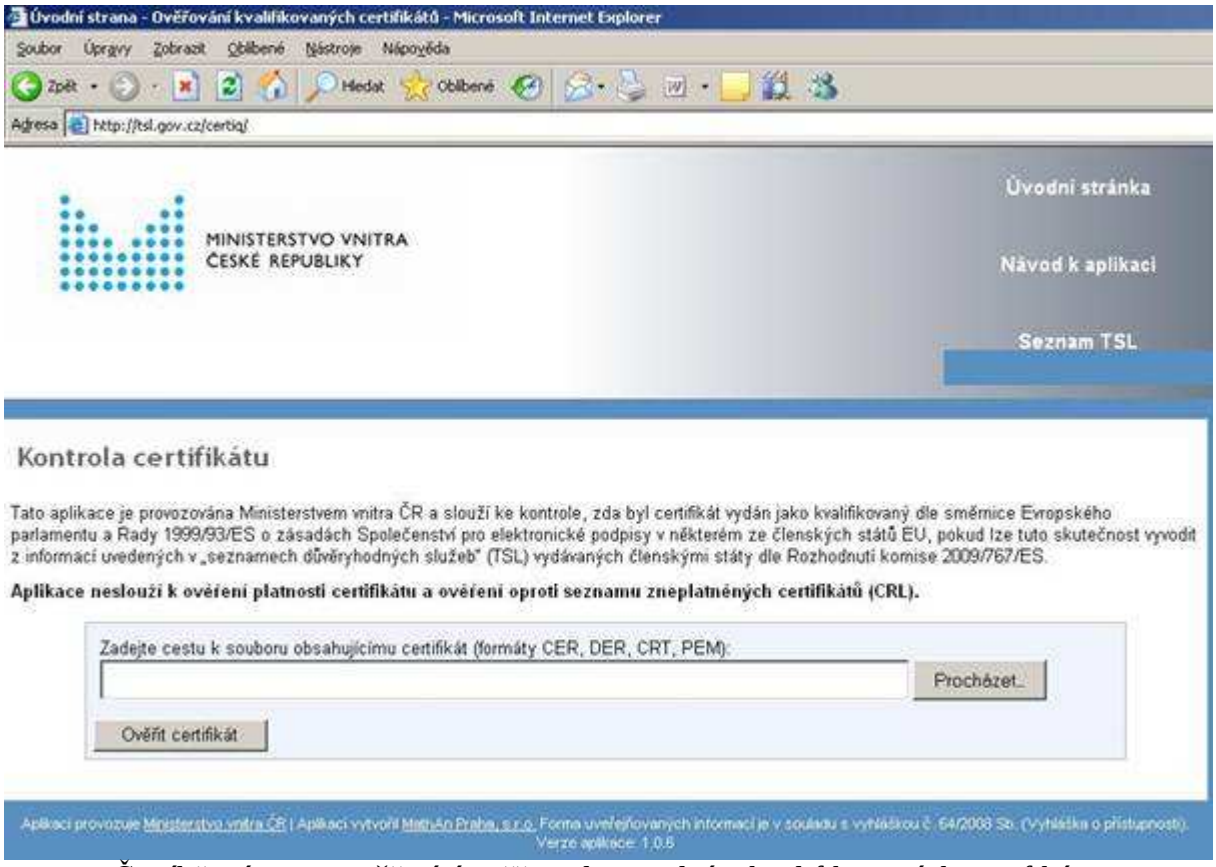
Předpokladem funkčnosti je, že stát, ve kterém byl certifikát vydán, zveřejní TSL. Seznam adres všech publikovaných TSL členských států je pak zveřejněn Evropskou komisí v LOTL (List of the Lists - „seznamu TSL“). Ten je dostupný v lidsky čitelné podobě (human readable form) na adrese https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf a ve strojově zpracovatelné formě (machine processable form) na adrese https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml.

Prosinec 2009

Pro usnadnění ověřování certifikátů z jiných členských států nechalo Ministerstvo vnitra ČR připravit webovou aplikaci, která po vložení souboru s certifikátem vyhodnotí, na základě informací publikovaných v TSL jednotlivých členských států, zda byl tento certifikát vydán jako kvalifikovaný. Aplikace je volně dostupná všem zájemcům na adrese http://tsl.gov.cz/certiq/.

O povinnosti vydávat a zveřejňovat TSL seznamy a o nástroji umožňující vzájemné uznávání kvalifikovaných certifikátů – web aplikaci „čertík“ (certiq) jsme psali letos v březnovém

ezinu a to konkrétně v článku *Aktuální situace v oblasti uznávání zahraničních kvalifikovaných certifikátů*, Crypto-World 3/2010.



„Čertík", nástroj umožňující ověřit, zde se jedná o kvalifikovaných certifikát.

2010

Přestože výše uvedené rozhodnutí Komise 2009/767/ES uložilo členským státům povinnost od 28. 12. 2009 zveřejňovat a spravovat „důvěryhodné seznamy" TSL, v praxi se ukázala plnění tohoto rozhodnutí jako nedostatečné.

Jako problematické se v praxi ukázalo zejména toto:

- Členské státy však mají za povinnost zveřejňovat pouze lidsky čitelnou podobu TSL (human-readable, neboli dokument ve formátu PDF/A), která neumožňuje automatizované ověřování certifikátů. Rozhodnutí ovšem současně definuje i druhou formu a to strojově zpracovatelnou (machine-processable), kterou je dobře definovaný soubor ve formátu XML, ale vydávání TSL v tomto formátu není povinné.
- Důvěryhodnost vydaných TSL není zajištěna. Publikování zabezpečeným kanálem nebo podpis TSL souboru toto Rozhodnutí pouze doporučuje.
- Nejsou zajištěny vhodné podmínky pro ověření podepsaných TSL, protože Evropská komise dosud nezajistila důvěryhodnou distribuci certifikátů potřebných k ověření těchto podpisů.

Snahou odstranit tyto překážky je novela Rozhodnutí, která byla přijata dne 28. 7. 2010 jako rozhodnutí **Evropské komise 2010/425/EU.** Tato novela nabyla účinnosti právě v těchto dnech a to konkrétně **1. 12. 2010.**

Novela jako reakce na výše uvedené problémy ukládá členským státům EU tyto nové povinnosti:

- publikovat jak lidsky čitelnou, tak strojově zpracovatelnou podobu TSL,
- strojově zpracovatelná podoba musí být opatřena elektronickým podpisem,
- lidsky čitelná podoba TSL musí být publikovaná bezpečným způsobem (tj. buď zabezpečeným kanálem, nebo musí být opatřena elektronickým podpisem),
- členské státy jsou povinny předat Evropské komisi certifikáty s veřejnými klíči, potřebné k ověření podpisů TSL. Evropská komise následně zajistí jejich důvěryhodnou distribuci přes LOTL (centrální seznam TSL).

Plné znění rozhodnutí Komise 2010/425/EU je dostupné na následujících webových adresách:

v angličtině:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:199:0030:0035:EN:PDF

v češtině:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:199:0030:0035:CS:PDF
Bohužel tento oficiální překlad do češtiny nepoužívá terminologii vycházející z českého zákona o elektronickém podpisu 227/2000 Sb. a je proto těžko čitelný a může být zavádějící.

18. 12. 2010

Na závěr se podívejme, jak jednotlivé státy EU tuto povinnost začaly plnit. Následuje seznam TSL členských států EU, který byl načten **18. 12. 2010** z oficiální k tomu určené adresy internetové adresy **https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml**

Stát	URL strojově zpracovatelného TSL	URL lidsky čitelného TSL
Belgie (BE)	http://tsl.belgium.be/tsl-be.xml Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	http://tsl.belgium.be/tsl-be.pdf
Bulharsko (BG)	Není k dispozici	http://www.crc.bg/section.php?lang=en&id=31
Česká republika (CZ)	http://tsl.gov.cz/publ/TSL_CZ.xtsl	http://tsl.gov.cz/publ/TSL_CZ.pdf

Dánsko (DK)	http://www.itst.dk/digitale-losninger/digital-signatur/in... TSL není elektronicky podepsaný, jeho obsah má proto jen informační hodnotu, nelze na něj spoléhat.	http://www.itst.dk/digitale-losninger/digital-signatur/in...
Estonsko (EE)	http://sr.riik.ee/tsl/estonian-tsl.xml Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	http://sr.riik.ee/tsl/estonian-tsl.pdf
Finsko (FI)	http://www.ficora.fi/attachments/suomiry/5m5T1qldW/truste... Formát XML souboru není dle specifikace XML.	http://www.ficora.fi/attachments/suomiry/5m5Sl2GEj/truste...
Francie (FR)	http://references.modernisation.gouv.fr/sites/default/fil... TSL není elektronicky podepsaný, jeho obsah má proto jen informační hodnotu, nelze na něj spoléhat.	http://references.modernisation.gouv.fr/sites/default/fil...
Irsko (IE)	Není k dispozici	Není k dispozici
Island (IC)	Není k dispozici	Není k dispozici
Itálie (IT)	https://applicazioni.cnipa.gov.it/TSL/IT_TSL_signed.xml Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	https://applicazioni.cnipa.gov.it/TSl/IT_TSL_HR.pdf
Kypr (CY)	http://www.mcw.gov.cy/mcw/DEC/DEC.nsf/all/9BE02B75459C1ED... Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	http://www.mcw.gov.cy/mcw/DEC/DEC.nsf/all/0F90C75AEE05D35...
Lichtenštejnsko (LI)	Není k dispozici	Není k dispozici
Litva (LT)	https://epp.ivpk.lt/epp/Dokumentai/TSL/LT-TSL.xml	https://epp.ivpk.lt/epp/Dokumentai/TSL/LT-TSL.pdf

	Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	
Lotyšsko (LV)	Není k dispozici	http://www.dvi.gov.lv/edokumenti/TSL_LV.pdf
Lucembursko (LU)	http://www.ilnas.public.lu/tsl-xml Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	http://www.ilnas.public.lu/tsl-pdf
Maďarsko (HU)	http://www.nhh.hu/tl/pub/HU_TL.xml Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	http://www.nhh.hu/tl/pub/HU_TL.pdf
Malta (MT)	http://www.mca.org.mt/tsl/MT_TSL.xml TSL není elektronicky podepsaný, jeho obsah má proto jen informační hodnotu, nelze na něj spoléhat.	http://www.mca.org.mt/tsl/MT_TSL.pdf
Německo (DE)	http://www.nrca-ds.de/st/TSL_DE.XML.tsr.zip Formát XML souboru není dle specifikace XML.	http://www.nrca-ds.de/st/TSL_DE.PDF.tsr.zip
Nizozemsko (NL)	Není k dispozici	https://www.opta.nl/download/bestand/current-tsl.pdf
Norsko (NO)	http://www.npt.no/TSL/NO_TSL.xml Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	http://www.npt.no/TSL/NO_TSL.pdf
Polsko (PL)	https://www.nccert.pl/tsl/PL_TSL.xml Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	https://www.nccert.pl/tsl/PL_TSL.pdf
Portugalsko (PT)	http://www.gns.gov.pt/NR/rdonlyres/AE2B69CF-4869-4CDC-820... Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen infor-	http://www.gns.gov.pt/NR/rdonlyres/ED525381-8A44-4704-9F0...

	mační hodnotu, nelze na něj spoléhat.	
Rakousko (AT)	**http://www.signatur.rtr.at/currenttsl.xml** Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	**http://www.signatur.rtr.at/currenttsl.pdf**
Rumunsko (RO)	Není k dispozici	Není k dispozici
Řecko (EL)	**https://www.eett.gr/tsl/EL-TSL.xml** TSL není elektronicky podepsaný, jeho obsah má proto jen informační hodnotu, nelze na něj spoléhat.	**https://www.eett.gr/tsl/EL-TSL.pdf**
Slovensko (SK)	**http://ep.nbusr.sk/kca/tsl/tsl.xml**	**http://ep.nbusr.sk/kca/tsl/tsl_hrf.zip**
Slovinsko (SI)	**http://www.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/...** Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	**http://www.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/...**
Španělsko (ES)	**https://sede.mityc.gob.es/prestadores/tsl/tsl.xml** Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	**https://sede.mityc.gob.es/prestadores/tsl/tsl.pdf**
Švédsko (SE)	**http://www.pts.se/upload/Ovrigt/Internet/Branschinformati...** Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	**http://www.pts.se/upload/Ovrigt/Internet/Branschinformati...**
Velká Británie (UK)	Není k dispozici	Není k dispozici

2011

???

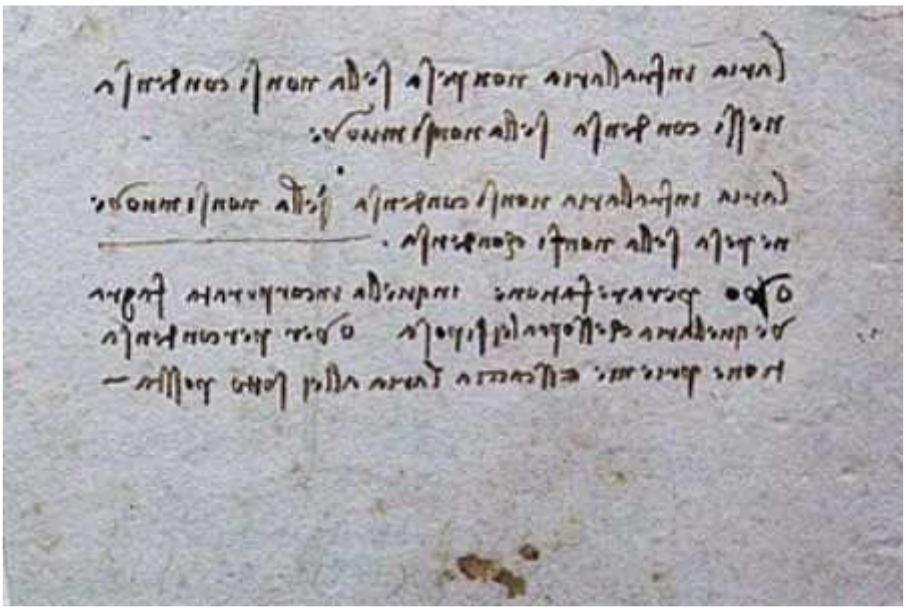
D. Šifra mistra Leonarda ☺

Koncem roku proběhla v médiích zajímavá zpráva, která se týká nálezu šifrovaného rukopisu známého renesančního umělce Leonarda da Vinciho (1452 -1519). Zatím se ho nepodařilo rozluštit.

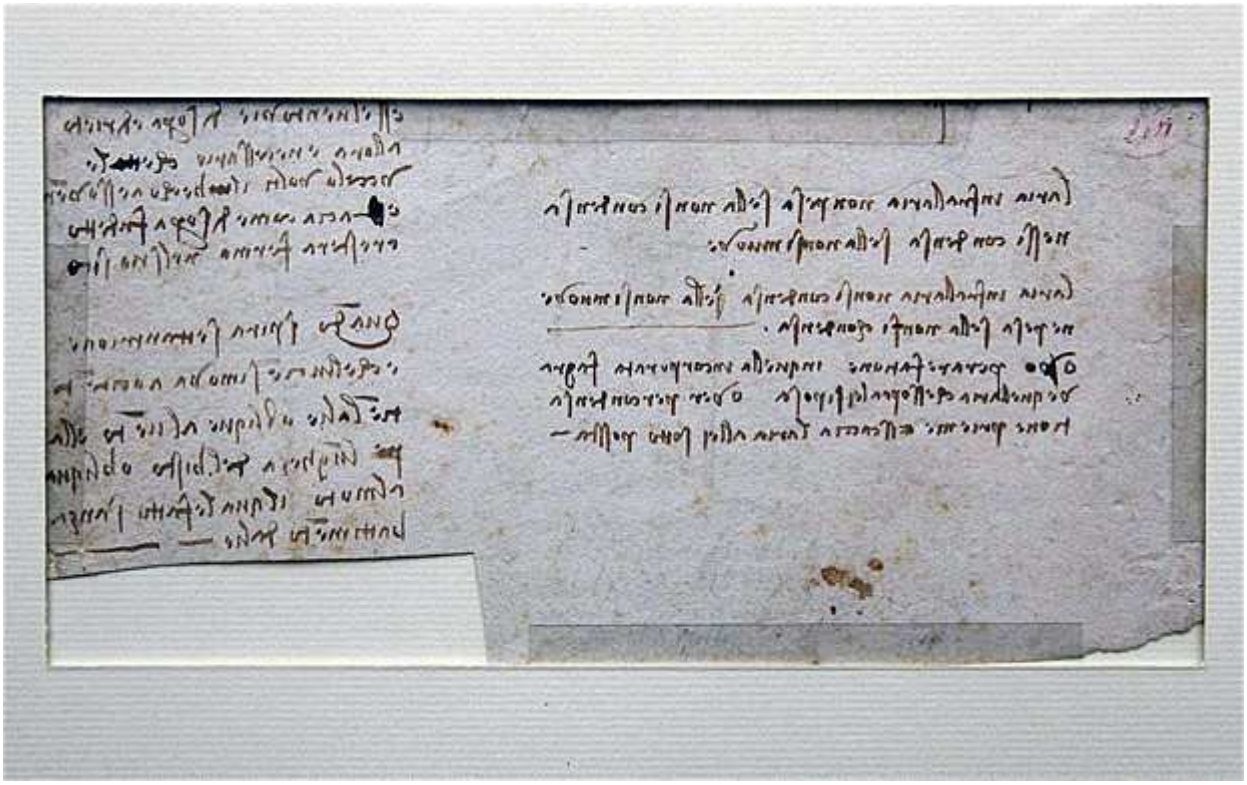
Vzácný manuskript byl nalezen v knihovně francouzského města Nantes. Zde byl uložen od roku 1872, kdy jej knihovna získala s více jak pěti tisíci rukopisy, které ji věnoval bohatý sběratel Pierre-Antoine Labouchere.

Knihovna tuto rozsáhlou kolekci přijala, zaevidovala a uschovala k dalšímu výzkumu. Postupně byla tato rozsáhlá sbírka s delšími přestávkami zpracovávána. Před dvěma lety se mezi těmito exponáty například podařilo objevit noty psané Wolfgangem Amadeem Mozartem

Nyní byl ohlášen ve stejné kolekci nález rukopisu Leonarda da Vinciho. Jedná se o útržek papíru s hnědými klikyháky. Je psán zprava doleva, a to zrcadlovým písmem, které Leonarda používal i ve svých jiných záznamech. V tomto případě se však jedná o zašifrovaný text.
Text se zatím nepodařilo dešifrovat.
Dle ředitelky knihovny Agnes Marcetteauová je text nejspíše psán v italštině patnáctého století, kterou Leonardu ve svých zápisech běžně používal, ale nelze ani vyloučit že v tomto konkrétním případě použil některý jiný jazyk, který ovládal.



http://www.presstv.ir/detail/154963.html



http://i.telegraph.co.uk/telegraph/multimedia/archive/01779/davinci_1779391b.jpg

http://www.uniritter.edu.br/biblioteca/blog/page/2/

E. O čem jsme psali v prosinci 2000 – 2009

Crypto-World 12/1999

Crypto-World 12/2000

Příloha : teze.zip - zkrácené verze prezentací ÚOOÚ použité při předložení tezí k Zákonu o elektronickém podpisu (§6, §17) dne 4.12.2000 a teze příslušné vyhlášky.

Crypto-World Vánoce/2000

Crypto-World 12/2001

Příloha: uloha7.wav

Crypto-World 12/2002

Crypto-World 12/2003

Crypto-World 12/2004

Crypto-World 12/2005

Crypto-World 12/2006

Crypto-World 12/2007

Crypto-World 12/2008

Crypto-World 12/2009

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí e-ziny, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály: http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Vlastimil Klíma
	Pavel Vondruška
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS (výběr příspěvků, komentáře a vkládání na web)	Jaroslav Pinkava Vlastimil Klíma Pavel Vondruška Tomáš Rosa
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info