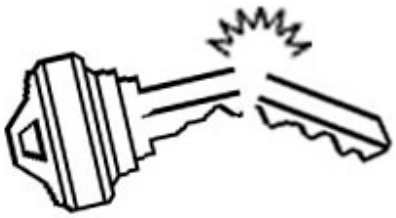
Crypto-World 12/99
Informační sešit GCUCMP

Připravil : Mgr.Pavel Vondruška,
člen IACR, GCUCMP
(47 e-mail výtisků)
Uzávěrka 5.12.99



Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (internet, noviny) nebo se jedná o původní články podepsané autory. Oficiální informační sešit je primárně určený pro členy "Kryptologické sekce Jednoty matematicko-fyzikální " (GCUCMP). Pokud má někdo zájem o tyto informace, stačí se zaregistrovat e-mailem na adrese hruby@gcucmp.cz (subject : Crypto-World). Informační sešit je bezplatně rozesílán v elektronické podobě e-mailem.
Případné chyby a nepřesnosti jsou dílem P.Vondrušky a GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

OBSAH : **Str.**

A. Microsoft nás zbavil další iluze !

Mgr. Pavel Vondruška, NBÚ ČR

Také svým zákazníkům, kolegům a vůbec svému okolí pracně vysvětlujete, že virus se dá chytit jen tak a tak a např. že pouhým přečtením e-mailu jej nemohou získat ? Virus se přece šíří pouze v příloze a my jej sami aktivujeme tím, že přílohu spustíme. Takže se nebojte, pouhým čtením e-mailu se virus šířit nemůže … Jenže ono to už neplatí !!!
Kdosi (zpravidla se říká, že student, nějaký recesista nebo majitel antivirové firmy) napsal nový "chytrý" virus (spíše červa), který využívá skripty vložené do HTML kódu. Účinky a možnosti těchto skriptů jsou velice omezeny, přesto se podařilo najít bezpečnostní trhlinku a na jejím základě virus napsat. Virus byl napsán pro VB Script (ne pro JavaScript nebo Jscript). Ohroženi jsou tedy potenciálně pouze ti, kteří nějaký mailer interpretující HTML a podporující VB Scripty využívá. VB Script je podporován pouze v produktech Microsoftu. Speciálně jsou tedy ohroženi uživatelé rozšířených mailerů Outlook a Outlook Express. Virus se šíří e-mailem s nadpisem "BubbleBoy is back!" Ten si po odklepnutí zapíše svůj kód na disk (to skripty v zásadě dělat nemají), kód je pak automaticky inicializován při restartu počítače. Červ se dále automaticky rozešle na všechny adresy, které najde v uživatelově adresáři (proto červ), smaže existující e-maily (proto virus). Jeho název je zvolen podle subjectu, který používá, tedy BubbleBoy. Microsoft tentokráte reagoval na bezpečnostní chybu rychle a na svém webu umístil bezpečnostní patch (záplatu). Tento patch lze stáhnout z adresy http://www.microsoft.com/security/Bulletins/ms99-032.asp .
Samotný viruso-červ není ani tak nebezpečný, je lehce odhalitelný, jeho význam je především v tom, že pomohl odhalit bezpečnostní nedostatek v produktech Microsoftu a hlavně v tom, že padl další mýtus a to, že "přečtením e-mailu nelze získat virus".

Další doplňující informace lze zjistit na :
http://www.wired.com/news/story/0,1240,32434,00.html
http://www.wired.com/news/technology/0,1282,32529,00.html
http://www.europe.datafellows.com/v-descs/bubb-boy.htm

Mimochodem, když už jsme u těch záplat - patchů - stáhli jste si již záplatu pro problém Y2K (přechod na rok 2000) ve Windows? Na serveru http://www.microsoft.com/year2000 jsou k dispozici všechny patche pro jednotlivé verze Windows.

A ještě jedna poznámka, zajímali jste se již někdy, kolik těch záplat v produktech Microsoftu už asi je ? Bruce Schneier odhadl, že jen bezpečnostních záplat a dodatečných nastavení je pro Windows NT asi 300 … V polemice, kterou tento jeho odhad vyvolal, pak odborníci vyslovili různé odhady a to od padesáti do tří tisíc … (viz Crypto-World 10/99).

B. Matematické principy informační bezpečnosti

RNDr. Jiří Souček, DrSc., MÚ ČSAV

Identifikace: MAT069
Konání: každé úterý 17:20 seminární místnost KSI (Malá Strana)

Každé úterý se koná dvouhodinová přednáška (seminář) v seminární místnosti KSI MFF UK na Malé straně (druhé poschodí, katedra systémového inženýrství). Seminář vychází z praktických úloh, na semináři přednáší přední odborníci v dané oblasti. Seminář je vhodný pro studenty a bude probírána daná problematika od počátku. Na seminář je volný přístup pro členy GCUCMP a další zájemce o konkrétní témata.

Přehled již uskutečněných přednášek:

12.10. Ondřej Pangrác: Diferenční kryptoanalýza I. (DES 4,6 rund)
19.10. Ondřej Pangrác: Diferenční kryptoanalýza II. (DES 16 rund)
26.10. Ondřej Pangrác: Lineární kryptoanalýza
2.11. Tonda Beneš : Faktorizační metody I.
9.11. Tonda Beneš : Faktorizační metody II.*
16.11. Jaroslav Hrubý: Kvanová kryptolgie
23.11. Pavel Vondruška: TWINKLE**
30.11. Pavel Kaňkovský: Informační toky

Zbývající přednášky:

7.12. Jaroslav Pinkava: Softwarové pseudogenerátory
14.12. Jaroslav Hrubý: Kvantové počítání
21.12. Jiří Souček: Závěrečný seminář

(Případné změny v přednáškách budou domluveny na semináři 7.12.99)

* Na vyžádání lze zaslat elektronickou verzi přílohy k semináři (Faktorizace)
** Na vyžádání lze zaslat elektronickou verzi přednášky (TWINKLE)

C. Pod stromeček nové síťové karty

Mgr. Pavel Vondruška, NBÚ ČR

Pokud Vaše společnost plánuje "přezbrojení" na nový operační systém Windows 2000, musíte do finanční kalkulace rovnou zahrnout i nákup nových síťových karet od firmy 3Com. Firma 3Com totiž uzavřela s firmou Microsoft strategickou dohodu na vývoj rozhraní umožňující hardwarové zrychlení klíčových operací mezi síťovou kartou a jádrem Windows 2000 týkajících se TCP/IP protokolu a síťové bezpečnosti. Toto rozhraní významně odlehčí zatížení CPU na hostitelském počítači, čímž se zvýší propustnost sítě a rychlost vlastního PC.

Nová rodina karet 3COM-3XP je osazena speciálním čipovým obvodem (ASIC), který obsahuje integrovaný procesor 3XP. Právě tento procesor umožňuje vylepšený výkon a snižuje zatížení při využití klíčových síťových úkolů pod Windows 2000. Karta se bude vyrábět ve verzi 10/100 PCI.
http://www.3com.com

D. Konec filatelie

Ing. Jiří Němejc CSc., GESTO Communications

Od července 1999 je možné frankovat zásilky americké pošty USPS (US Postal Service) elektronicky. Známky se tisknou jako 2-dimensionální čárový kód, který obsahuje údaje potřebné pro účtování a sledování procesu doručení, přičemž tato data jsou digitálně podepsána. Aplikace IBIP (Information Based Indicia Program) je založena na využití certifikátů a digitálního podpisu. Celou rozsáhlou bezpečnostní infrastrukturu pro USPS vybudovala a komponenty pro ni dodala americká firma Cylink. PKI je implementována na systému clusterů serverů Sun Enterprise a produktu CryptoServer. Architektura je distribuovaná se zajištěným zálohováním, transakčním zpracováním, vysokou dostupností a výkonem. Obsahuje certifikační autority, registrační servery a je dimenzována pro řádově stovky milionů certifikátů (aby byla dostupná všem uživatelům USPS nejen v USA). Infrastruktura je určena i pro další aplikace.

Druhým společným projektem Cylink a USPS ve spolupráci s IPC (International Postal Corporation) je "PostECS" (Electronic Courier Service). Jde o elektronickou obdobu kurýrní pošty, která je však digitálně podepsaná a šifrovaná (event. s dalšími přidanými službami). Privátní klíče jsou zpracovávány v kryptografických smart kartách (PrivateCard). Garantem z hlediska certifikátu a údajů o odeslání je opět příslušná pošta. Pilotní projekt probíhá s účastí tří pošt: USPS, Canada Post Corporation, La Post (Francie).

http://56.0.78.92/html/ibimain.html
http://www.usps.gov/news/press/99/99066new.htm
http://www.cylink.com/news/press/pressrels/80999.htm
http://www.usps.gov/dtf/1dtfelectronic.html
http://www.usps.gov/dtf/28short11.htm
http://www.usps.gov/postecs/
http://www.postescanada.ca/CPC2/eps/postecs/eleccour.html
http://pcworld.com/pcwtoday/article/0%2C1510%2C7655%2C00.html

E. Y2K (Problém roku 2000)

Mgr. Pavel Vondruška, NBÚ ČR

O tomto problému již bylo napsáno tolik, že napsat něco nového a chytrého teď , necelý měsíc před prověrkou, zda jsme my a naše okolí připraveni, snad ani nejde. Přesto v tomto čísle o tomto problému něco musí být napsáno (jak by náš sešit vypadal …), a tak snad jen pár historicko-právních poznámek..

Na úrovni státních orgánů se tímto problémem v USA začali oficiálně zabývat již v roce 1995. Následovala Velká Británie (1996) a potom v rychlém sledu další státy např. 1997 Mexiko, Tunis atd. Rok 1998 byl ve vývoji zlomový. V tomto roce se problémem již zabývala většina států celého světa a vznikala první koordinační a krizová centra. V USA byl přijat 14.6.1998 zákon o "Y2K", který platí po dobu 3 let. Zajímavý aspekt je doktrína, která říká, že soukromé podniky musí v této oblasti bezpodmínečně poslouchat stát, a dále doktrína, která říká, že žádný subjekt se nesmí spoléhat na jiný subjekt a musí se postarat sám o sebe . Smysl druhé doktríny je v zabránění možných dlouhodobých následných právních sporů o náhradách škody. Koncem roku - 11.12.1998 na půdě OSN zaznělo, že státy sdružené v OSN musí ve své legislativě zakotvit nebo alespoň deklarovat, že se nezbavují odpovědnosti za možné dopady na obyvatelstvo (především za energetiku, dodávky vody, tepla apod.) a to i v oblastech, které nejsou ve vlastnictví státu, ale v soukromých rukou. Současně byl náš stát koncem roku 1998 ambasádou USA požádán, aby celý problém začal urychleně na úrovni státu také řešit.

Dne 1.2.1999 bylo konečně zřízeno Národní koordinační centrum i v České republice. Pro dotazy občanů a firem byla zřízena zelená linka 0800 11 2000 , kde je možné zdarma získat všechny základní informace. Stát se zavázal koncem roku vystupňovat mediální kampaň, která informuje občany o možných dopadech problému Y2K na domácnosti. Do 15.12.99 bychom pak měli všichni najít ve svých schránkách letáček s informacemi, jak se máme připravit na překonání možných problémů.

31.12.1999 ve 23.59 pohlaďme své počítače, mikrovlnky, automatické pračky a popřejme jim do nového roku vše nejlepší. Ty chytřejší se nám za to určitě v roce 2000 odvděčí.

F. PATÁLIE SE SYSTÉMEM MICKEYSOFT FRITÉZA

CyberSpace.cz - the future of M.A.T.R.I.X)
(Silvestrovské čtení)

Píše se rok 2000, rok vítězného tažení operačního systému Mickeysoft Windows CE do našich obýváků, kuchyní i ložnic a už i my máme doma několik zařízení nové generace. Po cestě z práce domů jsem dostal chuť na hranolky a koupil si jich pytlík, těšíc se na dobrou večeři. Příprava měla být snadná a jednoduchá - naše fritéza je vybavená poslední verzí operačního systému, pochopitelně včetně pěti nejdůležitějších softwarových záplat. Osud tomu však chtěl jinak.

Položil jsem pytlík s hranolkami na linku, zapnul přístroj pomocí tlačítka "Zažehnout" a už po necelých třech minutách (můj osobní rekord, měl jsem skutečně hlad) a dvou resetech (znáte to, klasický trojhmat Ctrl+Alt+Hranolek) jsem z menu vydoloval program fritování. A kruciš, v tom spěchu jsem zapomněl odpojit friťák z lokálního Mickeysoft Kitchenetu. Ta mrcha to stihla, spojila se s ledničkou a zahlásila: "Jste si jist, že chcete fritovat hranolky, když v lednici žádné nemáte?" a nabídla mi tlačítka "Ne" a "Storno". S odevzdaných povzdechem vkládám hranolky do ledničky, zavírám dveře, čekám pět vteřin až blikne zelená kontrolka, signalizující aktualizaci databáze potravin v Kitchenetu a vytahuji pochoutku zpět.

Po dalším startu už fritéza neprotestovala a na jejím displeji konečně naskočil známý "Průvodce fritováním". Pravda, těsně po záruce přestala fungovat vestavěná váha a hned po ní se odebral do věčných lovišť i scanner, takže mne navíc čekaly kroky "Nakreslete typický tvar hranolku", "Zadejte počet hranolků" či "Určete délku nejdelšího a nejkratšího hranolku", ale na to už jsem byl připravený - odhad mám skvělý a navíc jako jediný z rodiny celkem obstojně kreslím, takže napůl syrové a napůl spálené hranolky jsme měli zatím pouze dvakrát.

Mnohem větší obavy jsem měl z neblaze proslulé databáze olejů. Svoji drahou ženu jsem už sice naučil kupovat na její vkus poněkud předražené flašky s logem "Mickeysoft Kitchen 2000 compatible", ale jeden nikdy neví, zrovna včera jsem ve špajzu zahlédl novou láhev Lukany a nebyl jem si jist, zda se nejednalo o nějakou levnější noname verzi… Bohužel mé tušení bylo správné a na displeji se proto vynořila obávaná hláška "Neočekávaná chyba při detekci oleje, aktualizujte prosím seznam ovladačů a spusťte průvodce fritováním znovu."

Ještě že olej byl v novém balení, které mívá ve špuntu mikročip s ovladačem. Špunt, proboha kde je ten špunt ?! Určitě bude v šuplíku. V šuplíku bylo mnoho špuntů, máme moderní domácnost… Po deseti minutách, kdy jsem na snímač fritézy přiložil dva tucty mikročipů ve vršcích ze sirupů, moštů, piv a minerálek jsem propadl totální beznaději. Pravda, jeden z moštů označil Mickeysoft Fritéza CE za kompatibilní s obecným rostlinným olejem, ale po loňské zkušenosti s kuřecími prsíčky na octu už má důvěra v odhady fritézy značně poklesla.

Vypnul jsem proto strojek jak jinak než pomocí tlačítka "Zažehnout" a hladově si namazal osvědčený chleba se sádlem. Domácí sádlo bez identifikačního čipu máme od rodičů a starý nemoderní nůž jsme naštěstí ještě nevyhodili. I když, při vytahování sklenice se sádlem z ledničky se mi na její dvířka promítla za zvuků rolniček reklama na nový kráječ na chleba kompatibilní se sadou Mickeysoft Kitchen 2000. Prý mimo krájení umí navíc vyřezávat betlémy z překližky…

(převzato ze serveru www.tombo.cz bez redakční úpravy)

G. Letem "šifrovým světem"

1. Zákon o elektronickém podpisu, jehož znění inicioval SPIS (Sdružení pro informační společnost) inicioval a jehož autory jsou doc. Smejkal a doc. Mates , je vystaven na internetových adresách, mj.
   http://www.spis.cz/ , http://www.apek.cz/digitpodpis.html
   Na adrese "spisu" je dále k dispozici rozsáhlá a velice zajímavá diskuse k předloze tohoto zákona. Diskuse byla uzavřena 15.10.99 v 16.30 hod. Reakce na podněty a připomínky měly být vyvěšeny během 44 týdne , dnes (49 týden) ještě stále nejsou k dispozici.

2. Při spolupráci Windows NT se zařízeními řízenými pomocí Windows CE (viz bod F "silvestrovské čtení") Microsoft zašifrová vaše heslo. To je jistě chvályhodné, ale je zarážející, že k tomu zvolil následující algoritmus (toto již není silvestrovské čtení!) :
   XOR vašeho hesla s "susageP" . Tedy se slovem Pegasus napsaným obráceně (Pegasus je pracovní název Windows CE ….).
   http://www.cegadgets.com/artsusageP.htm

3. Na internetu se objevil nový elektronický časopis "Skytale". Časopis se zabývá obecně informační bezpečností. Právě vyšlo prvé číslo. Texty je možné stáhnout z webu nebo si je nechat elektronicky zasílat na uvedenou e-mail adresu. Texty jsou uvedeny ve formátu TXT, HTML nebo PDF.
   Více informací, prvé číslo časopisu, registraci apod. lze najít na adrese :
   http://www.isrc.qut.edu.au/skytale

4. (Jaroslav Pinkava) Čerstvé informace k chystaným úpravám v americkém zákonodárství
   -nedochází k plnému uvolnění amerického vývozu
   -neomezeně lze vyvážet produkty obsahující symetrické šifry s maximální délkou klíče 64 bitů a asymetrické šifry s maximální délkou klíče 1024 bitů
   -dochází k určité liberalizaci formulace komu lze dovážet produkty s neomezenou délkou klíče (dříve to např. v České republice byly pouze finanční a příbuzné instituce).
   http://cryptome.org/ear-crypto.htm
   http://www.usatoday.com
   http://www.cdt.org/crypto/regs112399.shtml

5. (Jiří Němejc) Daňové přiznání v elektronické formě, kryptograficky zabezpečené lze podat v Brazílii a Izraeli přes Internet. Aplikace byla vytvořena pro brazilskou vládu firmou Cylink (Algorithmic Research). Základní bezpečnostní komponentou je standardní produkt "Private Wire". Daňové přiznání podalo elektronicky v roce 1997 (pilot) 500 000 brazilských poplatníků, v roce 1998 2,5 milionu a letos se očekává 7,5 milionu on-line podaných přiznání. (A jako minulý rok bude zřejmě jejich většina podána v průběhu posledních 2 dnů lhůty).
   http://www.cylink.com/news/press/pressrels/81899.htm

6. (METRO 29.11.1999) - "Prvá vlašťovka" problému Y2K přiletěla do americké Filadelfie, kde 500 občanů dostalo 26.11.99 upozornění, že budou povoláni jako členové soudních porot v příštím roce - 1900. Městský komisař pro soudní poroty M. McAllister oznámil, že byla provedena příslušná opatření, aby se již tento problém nevyskytl.

7. (DSM 5/99) Společnost SGI oznámila instalaci prvního 128 procesorového serveru pracujícího pod operačním systémem Linux. Předinstalovaným softwarem je SGI Linux Enviroment s Red Hat Linux 6.0. Počítač je umístěn v Ohio Supercomputer Centru ve městě Columbus.

8. Jste připraveni i na 29.2.2000 ? A bude vůbec tento den v příštím kalendářním roce ? Odpovězte tedy rychle na otázku : "Je rok 2000 přestupný nebo ne ? " .
   Řešení : Platí pravidlo, že rok je přestupný tehdy, je-li dělitelný 4. Výjimkou jsou roky dělitelné 100, pokud nejsou dělitelné 400. Rok 2000 je tedy výjimkou z výjimky (rok 1900 přestupný nebyl, rok 2000 tedy je přestupný).

9. Na závěr jedna zajímavost: víte o tom, že 21. století nezačíná rokem 2000, ale až rokem 2001?

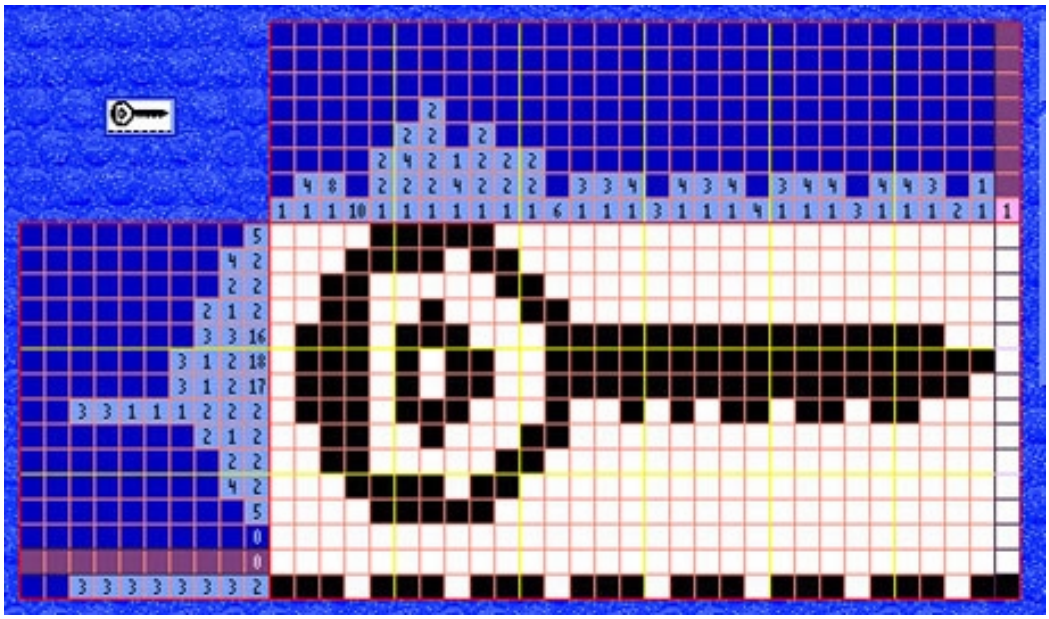
10. A úplně na samý závěr malá statistika vztahující se k našemu sešitu:

Sešit	**výtisků***	**autoři**	**velikost**	**Počet stran**
9/99	25	Vondruška	84992	7
10/99	31	Vondruška,Pinkava	130048	10
11/99	36	Vondruška,Souček,Pinkava	205312	9
12/99	47	Vondruška,Souček,Pinkava,Němejc	337920	9

* počet "výtisků" v době oficiálního rozeslání sešitu

H. Řešení malované křížovky z minulého čísla

Descartes Enigma (malovaná křížovka) je hra, v níž máte odhalit skrytý obrazec pomocí klíčů, které Vám dávají informace o jednotlivých blocích čtverečků v každém řádku a sloupci. Tuto velice zajímavou hru jsme Vám představili v minulém čísle 11/99. Zde uvádíme řešení malované křížovky z minulého čísla :



I. Spojení

hruby@gcucmp.cz (Group of Cryptology Union of Czech Mathematicians and Physicists)
- oficiální adresa kryptologické sekce JČMF
pavel.vondruska@post.cz - osobní poštovní stránka
pavel.vondruska@sms.paegas.cz - jen 160 znaků !
mobil : Mgr.Pavel Vondruška 0603 436 341

S přáním všeho nejlepšího v celém příštím roce ~~**1900**~~ **2000** se s Vámi loučí autoři tohoto sešitu.
(Pokud vše dobře dopadne, tak se těšíme na shledání v příštím miléniu).