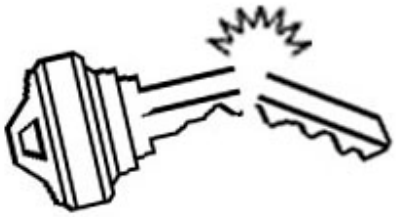
Crypto-World 11/99
Informační sešit GCUCMP

Připravil : Mgr.Pavel Vondruška,
člen IACR, GCUCMP
(35 e-mail výtisků)
Uzávěrka 1.11.99



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. Jak je to s bezpečností eliptických kryptosystémů?

Ing. Jaroslav Pinkava, CSc., AEC Ltd., Brno

Užití eliptických křivek pro návrh kryptosystému s veřejným klíčem poprvé navrhli pánové Victor Miller a Neal Koblitz zhruba uprostřed osmdesátých let. Jedná se v zásadě o analog již existujících systémů s veřejným klíčem; přitom modulární aritmetika je nahrazena aritmetikou budovanou na základě operací s body na eliptické křivce.

Tak jako u jiných kryptosystémů (RSA, systémy na bázi úlohy diskrétního logaritmu) spočívá bezpečnost eliptických kryptosystémů v obtížnosti řešení příslušného matematického problému. Zde se jedná o řešení úlohy diskrétního logaritmu pro eliptické křivky. V současné době je tato úloha podstatně obtížněji řešitelná než je úloha klasického diskrétního logaritmu. V důsledku toho lze konstruovat bezpečné kryptosystémy s výrazně kratší délkou klíče. To vede mimo jiné k implementacím s menšími nároky na paměť, implementacím, které jsou současně i výrazně rychlejší ve srovnání např. s kryptosystémy na bázi diskrétního logaritmu. Teoretická konstrukce přitom umožňuje vytvořit systémy zcela analogické klasickým modelům (šifrování – El Gamal, digitální podpis – DSA a výměna klíčů – Diffie-Hellman). Někteří odborníci hovoří o kryptosystémech na bázi eliptických křivek jako o nové generaci kryptosystémů s veřejným klíčem. Výrazným subjektem podílejícím se jak na teoretickém výzkumu eliptických kryptosystémů tak i na vývoji příslušných realizačních prostředků (hardware i software) je firma Certicom (http://www.certicom.com). V České republice poprvé realizovala eliptické kryptosystémy a do svých produktů implementovala brněnská firma AEC (http://www.aec.cz).

Přitom samozřejmě pro dostatečně malé rozměry klíčů (stejně jako tomu je pro všechny existující kryptosystémy) jsme schopni úlohu diskrétního logaritmu pro eliptické křivky řešit. Základní otázky, které se v této souvislosti nabízí, jsou tedy následující.

Jaké k tomu můžeme použít prostředky (algoritmy) ? Kde leží současné výpočetní meze těchto algoritmů, tj. jaké délky klíčů lze dnes již považovat za bezpečné (a to i s určitým výhledem na perspektivní rozvoj výpočetních možností)? Jaké jsou srovnatelné délky klíčů (při stejné bezpečnosti) pro eliptické křivky a např. pro RSA nebo systémy na bázi diskrétního logaritmu?

Nejprve jedna technická poznámka. Z hlediska implementací systémů na bázi jak klasického diskrétního logaritmu, tak i eliptického diskrétního logaritmu lze zvažovat v zásadě dva druhy těles, ve kterých bude příslušná aritmetika realizována. Jsou to tělesa charakteristiky 2 (tj. tělesa mající 2^n prvků) a prvočíselná tělesa. Pro klasické kryptosystémy na bázi diskrétního logaritmu se ukázala tělesa charakteristiky 2 jako nevhodná varianta – existuje řada technických prostředků k výraznému zvýšení efektivity řešení příslušné matematické úlohy kryptoanalýzy.

Na rozdíl od toho pro úlohu eliptického diskrétního logaritmu žádné postupy vedoucí k efektivnějšímu řešení pro tělesa charakteristiky dvě známa nejsou a jsou proto používány souběžně oba typy implementací, každý z těchto typů má výhody pro určitý typ realizací. Obvykle se uvádí, že eliptické křivky v prvočíselných tělesech jsou vhodnější pro softwarové realizace, zatímco eliptické křivky v tělesech charakteristiky dvě jsou vhodnější pro hardwarové realizace.

Nyní k matematické úloze řešení úlohy eliptického diskrétního logaritmu. Zde existuje několik algoritmů, jejichž výpočetní složitost lze popsat ve tvaru druhé odmocniny z N, kde N je počet bodů příslušné eliptické křivky. Jsou to zejména Pollardova ρ-metoda a Pollardova λ-metoda. Složitost z nich nejefektivnější Pollardovy ρ-metody je daná výrazem $(\pi N/4)^{1/2}$.

Obecně pro řešení úlohy eliptického diskrétního logaritmu není znám žádný algoritmus mající subexponenciální výpočetní složitost jako je tomu pro řešení úlohy faktorizace (RSA) nebo řešení úlohy klasického diskrétního logaritmu. Existují však určité speciální případy (speciální typy eliptických křivek), kde takovéto postupy existují. Např. v roce 1991 pánové Alfred Menezes, Tatsuaki Okamoto, a Scott Vanstone přišli se subexponenciálním algoritmem pro tzv. supersingulární eliptické křivky (MOV útok) a v roce 1997 byl nalezen algoritmus s lineární (!) výpočetní složitostí pro eliptické křivky s tzv. stopou-1 (trace-1). Podobné útoky jsou stále předmětem úvah odborníků, jsou však obvykle orientovány na speciální případy eliptických křivek.

Z tohoto důvodu je také v současnosti doporučováno používat eliptické křivky s náhodně generovanými parametry, kde pravděpodobnost existence podobných útoků je minimální. Zejména atraktivním postupem je možnost generovat parametry eliptické křivky tzv. prokazatelně náhodně. Konstruktér eliptické křivky se takto může vyhnout potenciálním obviněním ze strany uživatele, že vložil do hodnot parametrů určitá zadní vrátka, která mu umožňuji proniknout snadněji za bezpečnostní hranice systému. Pro konstrukci eliptických křivek je nezbytné pro stanovení konkrétních hodnot parametrů mít k dispozici prostředek pro výpočet počtu bodů dané eliptické křivky. Obecně toto řeší tzv. Schoofův algoritmus, který však není tak jednoduché implementovat. Proto také v současnosti jsou již k dispozici určité doporučené množiny parametrů (NIST, SECG – viz dále).

Srovnatelná bezpečnost různých kryptosystémů při různých délkách klíčů:

Blokové šifry	Eliptické křivky	RSA/DL (klasický diskrétní logaritmus)
56	112	512
64	128	768
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Již delší dobu probíhá tzv. RSA Factoring Challenge sponzorovaná RSA Security, Inc. (http.//www.rsasecurity.com) V srpnu 1999 byl v tomto směru získán význačný výsledek, bylo rozbito RSA s délkou klíče 512 bitů (mj. tato délka klíče je stále používána v řadě komerčních systémů, zejména systémů pro elektronický obchod).

Analogický výsledek byl získán francouzským vládním institutem INRIA, kdy při použití 740 počítačů v 20 zemích byl za 40 dnů rozbit 97-bitový eliptický kryptosystém (Certicom Elliptic Challenge). Tento výsledek byl popsán v minulém čísle informačního sešitu (Crypto-World 10/99).

Pokud srovnáme dosažené výsledky s výše uvedenou tabulkou můžeme zcela jednoznačně zhodnotit jejich význam pro bezpečnost příslušných kryptosystémů. Doplníme-li tyto informace o známý výsledek rozbití DES (56-bitová bloková šifra), máme vlastně plnou charakterizaci současných možností.

Proto také doporučované hodnoty délek příslušných klíčů se dnes pohybují (tabulka) od třetího řádku níže. Přitom v tabulce první řádek vlastně charakterizuje již dosažené výsledky (s výjimkou eliptických křivek, kde realizace příslušných kryptoanalytických metod je asi přeci jen ještě obtížnější než dávají odhady v tabulce). Druhý řádek charakterizuje již mez, která sice zatím v praxi dosažena ještě nebyla, avšak lze předpokládat, že např. v dalších

dvaceti či možná deseti letech dosažena bude. Ani jedny z těchto hodnot parametrů nejsou tudíž doporučovány pro praktické použití.

Samozřejmě v budoucnu lze předpokládat, že budou v tomto směru dosaženy další výsledky dokumentující postup výpočetních možností lidské společnosti. Pokud však nebudou získány zásadní matematické výsledky umožňující zcela nový pohled na úlohu elitptického diskrétního logaritmu (nebo nebude např. zrealizován kvantový počítač), lze tyto výpočetní možnosti určitým způsobem predikovat. Odsud lze potom také odvodit doporučení pro bezpečné délky klíčů. To je také cílem výše zmíněných „výzev“ (challenge) organizovaných firmami RSA a Certicom.

V současné době již existuje řada plnohodnotných norem pro vytváření kryptosystémů na bázi eliptických křivek. Jedná se především o materiály vytvořené skupinou IEEE P1363, které jsou zpracovány s velkou důkladností a vytváří základní východiska pro budování konkrétních kryptosystémů. Dále jsou to normy vytvořené pro finanční sféru (ANSI X9.62 a ANSI X9.63), které dále konkretizují postupy při vytváření digitálních podpisů a definují postupy pro výměnu a přenos klíčů. Konkrétní volbou parametrů pro eliptické kryptosystémy se zabývají materiály skupiny SECG (Certicom, http://www.secg.org) a v květnu 1999 vydaná příslušná doporučení amerického vládního úřadu NIST.

V materiálech SECG lze nalézt řadu dalších hodnotných informací ve vztahu k různým bezpečnostním problémům při realizacích eliptických kryptosystémů.

B. Známý problém přístupu k zabezpečeným serverům pomocí protokolu https s aplikací Internet Explorer 5 v systému Windows NT 4.0 s aktualizací SP4

Přístup k zabezpečeným serverům pomocí protokolu https (tj. bezpečný SSL protokol) může s aplikací Internet Explorer 5 nainstalovanou v systému Windows NT 4.0 s aktualizací Service Pack 4 nefungovat.

Jestliže nainstalujete systém Windows NT 4.0 a dále aktualizaci Service Pack 4 a poté aplikaci Internet Explorer 5.0, nebude pravděpodobně možné získat přístup k zabezpečeným serverům. To je způsobeno souborem s názvem schannel.dll. Česká verze aktualizace Service Pack 4 instaluje nesprávnou verzi tohoto souboru, která nepracuje správně s aplikací Internet Explorer 5. Tento problém lze vyřešit zkopírováním správné verze daného souboru do systému Windows NT.

Soubor schannel.dll je umístěn v adresáři \winnt\system32. Existuje několik způsobů řešení tohoto problému:

1) Instalace aplikace Internet Explorer 4.0 Problém lze vyřešit tak, že nejprve nainstalujete aplikaci Internet Explorer 4.0, a poté provedete aktualizaci na verzi Internet Explorer 5. Aplikace Internet Explorer 4.0 zkopíruje do systému správný soubor, a verze Internet Explorer 5 jej zachová.

2) Instalace aplikace Internet Explorer 5 do systému Windows NT s aktualizací Service Pack 3. Pokud aplikaci Internet Explorer 5 nainstalujete do systému Windows NT 4.0 s aktualizací Service Pack 3, aplikace Internet Explorer 5 do systému zkopíruje správný

soubor. Jestliže později provedete aktualizaci na Service Pack 4, správný soubor bude v systému zachován.

3) Zkopírování souboru schannel.dll do adresáře \winnt\system32 Problém lze vyřešit ručním zkopírováním správné verze souboru schannel.dll do adresáře \winnt\system32. Správnou verzi daného souboru (jedná se o soubor s číslem verze rovným nebo vyšším než 1877.1) můžete získat z anglické verze aktualizace Service Pack 4 systému Windows NT 4.0 nebo z jiného PC, kde již je nainstalován správný soubor např. pomocí metody 1 nebo 2.

C. Y2Kcount.exe - Trojský kůň v počítačích

Společnost Microsoft varuje své zákazníky, že zatím neznámý pachatel zneužil její e-mailovou adresu a distribuuje elektronickou poštu s virem typu trojského koně (Y2Kcount.exe).

Ve středu 15. září byla společnost Microsoft Corporation upozorněna, že jejím zákazníkům někdo distribuuje elektronickou poštu vydávající se za časomíru poskytovanou společností Microsoft, která má odpočítávat čas, jenž zbývá do roku 2000.
Tuto elektronickou poštu neposílala společnost Microsoft a distribuovaná příloha není program pro odpočítávání času zbývajícího do roku 2000, ale vir typu trojského koně, nazvaný Y2Kcount.exe. Odesílatel pošty zneužil e-mailovou adresu společnosti Microsoft: Support@Microsoft.com

Společnost Microsoft má pro uživatele několik užitečných informací: zásadně nedistribuuje software elektronickou poštou, updaty související s rokem 2000 lze nalézt pouze na jejích webových stránkách (http://www.microsoft.com/y2k/) nebo fyzicky na CD ROM nosiči jako je např. Microsoft Year 2000 Resource CD. Upgrady distribuuje přes Internet. Při tomto způsobu distribuce je software dostupný na webových stránkách společnosti Microsoft na adrese http://www.microsoft.com/ nebo na FTP serveru na adrese ftp://ftp.microsoft.com.

Microsoft příležitostně zasílá zákazníkům elektronickou poštu, aby je informoval o dostupnosti upgradů. V elektronické poště jsou však uvedeny pouze odkazy na místa, odkud si je možné tento software stáhnout. Tyto odkazy se vždy týkají webových stránek nebo FTP serveru, nikdy ne serverů třetích stran. K digitálnímu podpisu produktů společnosti Microsoft vždy používá autentický kód. Zákazníci tak mají jistotu, že produkty nebyly poškozeny. Pokud obdržíte e-mail, ve kterém se bude uvádět, že obsahuje software společnosti Microsoft, zásadně neotevírejte přílohu. Nejjistější věc, kterou můžete udělat, je tuto zprávu kompletně vymazat.

E-mailová zpráva, kterou v žádném případě nedistribuuje společnost Microsoft, vypadá takto:

From: support@microsoft.com
Sender: support@microsoft.com
Subject: Microsoft Announcement
Date: Wed, 15 Sep 1999 00:49:57 +0200

Další informace (mimo tohoto oficiálního prohlášení firmy Microsoft) můžete najít na:
http://www.wired.com/news/print_version/technology/story/21823.html?wnpg=all
http://www.zdnet.com/zdnn/stories/news/0,4586,1017257,00.html

D. Matematické principy informační bezpečnosti

RNDr. Jiří Souček, DrSc., MÚ ČSAV

Pozvání pro členy GCUCMP a další zájemce o problematiku informační bezpečnosti. Každé úterý se koná dvouhodinová přednáška (seminář) v seminární místnosti KSI MFF UK na Malé straně (druhé poschodí, katedra systémového inženýrství). Seminář bude věnován matematickým analytickým principům, bude definována a analyzována matematická podstata zabezpečení informací. Seminář bude vycházet z praktických úloh, na semináři budou přednášet přední odborníci v dané oblasti. Seminář je vhodný pro studenty a bude probírat danou problematiku od počátku. Na seminář je volný přístup pro členy GCUCMP a další zájemce o konkrétní témata.

Identifikace: MAT069
Zajišťuje: MUKU
Vyučující: Jiří Souček, Tonda Beneš
Rozsah: 0/2 Z, 0/2 Z
Konání: každé úterý 17:20 seminární místnost KSI (Malá Strana)

Konkrétní témata přednášek budou vyhlašovány v průběhu semestru.

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

E. Letem "šifrovým" světem

1. Sešit GCUCMP dosáhl svého rekordního nákladu 35 registrovaných e-mail odběratelů.

2. Na internetu je asi od poloviny tohoto měsíce k dispozici nově přepracovaná stránka NBÚ (Národní bezpečnostní úřad). Obsahuje přehled příslušných zákonů, vyhlášek a nařízení, strukturu úřadu, náplň práce jednotlivých odborů, kontaktní adresy, seznam akreditovaných psychologických pracovišť, akreditovaných zdravotnických pracovišť, certifikované technické prostředky apod. Celkově lze říci, že stránka obsahuje všechny základní veřejné informace o úřadu a i grafická úroveň je dobrá. Stránka obsahuje překlepy (techické, Ptaha, Csc., v anglické verzi číslování prázdných odstavců … , atd.), ale snad budou tyto chyby brzy odstraněny.
   http://www.nbu.cz/

3. Organizátoři nejvýznamnější kryptologické konference v Evropě - EUROCRYPT 2000 - oznámili konečný termín a místo konání . Konference se bude konat od 14.5 do 18.5.2000 v Bruggách v Belgii. Informace o konferenci lze najít na následující stránce : http://www.esat.kuleuven.ac.be/cosic/eurocrypt2000/ . Současně organizátoři upozorňují, že 3.11.1999 končí termín k odevzdání příspěvků na konferenci.

4. Ve dnech 29.9 až 1.10.1999 se konal ve Švédsku v Royal Institute of Technology (KTH, Stockholm) PKCS WORKSHOP '99. V seznamu účastníků bohužel chybí zástupci z České republiky. Jednotlivé přednášky a další dokumenty jsou k dispozici na adrese :
   http://www.rsasecurity.com/rsalabs/pkcs/

5. Tento měsíc se uskutečnila konference "International Association for Counterterrorism and Security Professionals". Na téma počítačová kriminalita zde zaznělo hodně odstrašujících případů a historek z celého světa. Pokud máte o tyto informace zájem, naleznete je na adresách :
   http://www.iacsp.com/
   http://www.wired.com/news/news/politics/story/22146.html

6. Firma AMD vyvinula novou technologii, kterou nazvala "Magic Packet", pomocí které lze po síti "vzbudit" nebo "uspat" procesor - PC nebo dokonce vypnout PC (ATX board). V této technologii se vůbec neuvažuje o zabezpečení tohoto procesu. Takže jistě již někde hackeři vyvíjí program, kterým budou moci tato PC v síti vypínat …
   http://www.amd.com/products/npd/overview/20212.html

7. 18.10.99 oficiálně odstartoval v USA- Kalifornii projekt , jenž si klade za cíl využívat pro bezpečnou komunikaci digitální podpis. Digitální podpis zde má již ze zákona stejnou váhu jako podpis "manuální". V tomto projektu se jedná především o komunikaci mezi státními orgány a občany a o zavedení celé nové oblasti elektronických služeb. Jako certifikační autorita byla vybrána známá firma Verisign Inc. Jako zajímavost uveďme, že se stát dokonce zajímá i o možnost použít digitální podpis k zabezpečení voleb přes internet. Ředitel firmy Verisign - pan Sclavos - prozradil, že firma spolupracuje na podobném projektu (využití digitálního podpisu) také v dalších státech Oregonu, New Jersey, Utahu a Washingtonu.
   http://cnn.com/TECH/computing/9910/19/california.digital.idg/index.html

8. Než začnete používat (a důvěřovat) různým "anonym serverům", přečtěte si informaci od Richarda Smithe, která je uvedena na přiložených www adresách. "Anonym servery" jsou servery poskytující službu, která umožňuje se přes ně připojit na jinou www adresu a poskytovaná služba má dále zajistit, že informace o vašem připojení (především Vaše IP adresa) se vymaskuje a na cílovém serveru nelze informace o Vás získat (dostupné mají být pouze informace o "anonymním" serveru, přes který jste se přihlásili). Jistě nejznámější (a to i mezi naší studentskou populací) je server Anonymizer , další významné servery, které poskytují tyto služby, jsou Bell Labs, Naval RL, Aixs.

Anonymizer	(http://www.anonymizer.com/)
Bell Labs	(http://www.bell-labs.com/project/lpwa)
Naval Research Laboratory	(http://www.onion-router.net)
Aixs	(http://aixs.net/aixs/)

   Pan Smith ve svém článku popisuje, jak během několika hodin se mu podařilo dokázat, že ve službách všech výše uvedených "anonym serverů" je chyba a lze na cílovém serveru Vaši IP adresu získat. Přesné detaily (použitý browser, demo programu, podmínky, popis chyb - na různých serverech jsou chyby a tedy metody získání IP různé) viz. jeho článek.
   http://www.tiac.net/users/smiths/anon/anonprob.htm
   http://www.tiac.net/users/smiths/anon/test.htm

9. Odvolací soud souhlasil s novým slyšením v Bernsteinově procesu. Ten je obviněn za to, že letos v květnu tvrdil, že šifrovací programy jsou jen algoritmy a slouží k vyjádření myšlenek matematickým vzorcem a jako takové je nemůže vláda potlačovat a regulovat.
   http://www.techserver.com/noframes/story/0,2294,500040274-500065347-500103132-0,00.html

10. A tuhle znáte …
    Víte co se stane, když v budově Microsoftu praskne žárovka a na chodbě nastane tma ? Nic, nikdo žárovku nevymění, protože Microsoft prohlásí tmu za standard.

F. e-mailové spojení (aktuální přehled)

hruby@gcucmp.cz (Group of Cryptology Union of Czech Mathematicians and Physicists)
- oficiální adresa kryptologické sekce JČMF

pavel.vondruska@post.cz - osobní stránka

pavel_vondruska@hotmail.com - ZRUŠENA !!!

pavel.vondruska@sms.paegas.cz - jen 160 znaků !

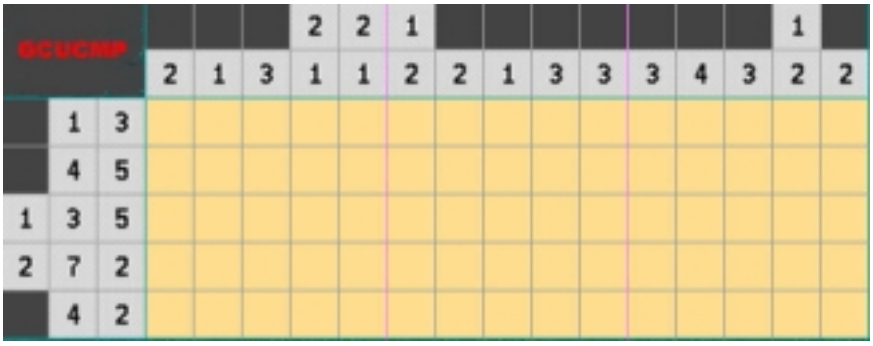
G. Trocha zábavy na závěr (malované křížovky)

Descartes Enigma je hra, v níž máte odhalit skrytý obrazec pomocí klíčů, které Vám dávají informace o jednotlivých blocích čtverečků v každém řádku a sloupci.

Postup:

1. Je potřeba vymalovat takový počet za sebou jdoucích políček, kolik určuje číslo zadané v řádku nebo sloupci.
2. Jestliže je v řádku nebo ve sloupci zadané více jak jedno číslo, je potřeba mezi nimi vynechat vždy nejméně jedno políčko nevyplněné (počet prázdných políček není tedy zadaný)

Tento typ hry byl ve skutečnosti vymyšlen v Japonsku panem Tetsuya Nishio a ve Spojených státech velmi zpopularizován časopisem World of Puzzles. Na Slovensku se prodávají tyto hlavolamy pod jménem malované křížovky a jsou poměrně populární.
Ve volném času si jednu lehkou vyzkoušejte :



A pokud máte zájem, je zde ještě jedna (delší a těžší), výsledkem je obrazec.