Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 8, číslo 7,8/2006 **15. srpen 2006**

78/2006

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1128 registrovaných odběratelů)

Obsah :

A. Pozvánka k tradiční podzimní soutěži v luštění

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

Vážení čtenáři, 15.9.2006 začne tradiční **podzimní soutěž v luštění jednoduchých šifrových textů o ceny – *Soutěž v luštění 2006***. Obdobné soutěže pořádal náš e-zin v letech 2000 až 2005. V roce 2000 byly úlohy zaměřeny na klasické šifrové systémy. V roce 2001 soutěž pokračovala řešením "moderních“ systémů. Soutěže v roce 2003 až 2005 byly z hlediska předložených úloh zaměřeny na řešení úloh od hříček přes jednoduché šifry až po klasické šifrové systémy (jednoduchá záměna, transpozice, periodické heslo, Fleissnerova otočná mřížka, jedno-dvoumístná záměna a šifry prvé a druhé světové války …).

Pokud se chcete podívat na tyto starší úlohy a jejich řešení, můžete je nalézt na webovské stránce našeho e-zinu v sekci věnované soutěžím:

http://crypto-world.info/souteze.php .

Loni se do soutěže zaregistrovalo přes 150 řešitelů, podmínku pro zařazení do losování o ceny (zisk 15-ti bodů) splnila třetina přihlášených soutěžících (51). Všech 26 předložených úloh vyřešilo 8 soutěžících.

Letošní soutěž bude navazovat právě na ročníky 2003 až 2005, objeví se obdobné šifrové systémy. Celkem bude čtenářům předloženo 30 úloh a několik nápověd, které umožní vyřešit složitější šifrové systémy. V tomto roce budou úlohy celkově obtížnější než v roce 2003, **ale výrazně lehčí než v roce minulém**!

Soutěž bude končit v listopadu a to dnem, kdy bude dána do prodeje moje kniha **Kryptologie, šifrování a tajná písma**. V této knize jsou totiž v závěrečné příloze uvedeny úlohy, které budou použity v naší soutěži, včetně jejich řešení. Kniha vyjde v nakladatelství Albatros v edici OKO (400 stran). Tato knížka bude také určena jako jedna z cen pro prvé tři řešitele a pro další tři vylosované řešitele, kteří splní stanovený bodový limit.

Přesná pravidla soutěže, přehled cen a všechny úlohy najdete v příštím čísle našeho e-zinu Crypto-World 9/2006, který vyjde kolem 15.9.2006. Všechny informace budou dostupné i na našem webu v sekci věnované soutěžím http://crypto-world.info/souteze.php.

Soutěž je určena pouze registrovaným čtenářům našeho e-zinu, do soutěže bude nutné (tak jako v minulých ročnících) se zaregistrovat. Heslo k registraci bude rozesláno společně s kódy ke stažení e-zinu 9/2006.

Na závěr této pozvánky k připravované Soutěži v luštění 2006 předkládám poslední ze soutěžních úloh (úlohu číslo 30).

X D G F X F A F D F X A D F A F D G X A D X D G A A A X A D
A X A D A A G D F G D D D D A D G G D D D D A D G G A F A X
A X X G A D A D X G F G F D G D D D D D G G D X A D G G X A
D D X D X F D F F D G A X F F D G F A A G X X D A G G X A F
A F D D X X A F A F G G D X F F F A F F D G A A F A F F X G
D A F F D A D G X A G D X A D D X D

Pokud se luštěním zabýváte, tak asi poznáte, že se jedná o typickou německou polní šifru ADFGX z konce první světové války, která používá dva klíče (permutační a substituční klíč). Luštění speciálních případů těchto systémů (se znalostí části otevřeného textu (Known-plaintext attack)) nalezl v roce 1918 francouzský důstojník kryptoanalytik Georges–Jean Painvin. Na obecné řešení těchto šifer přišel až roku 1933 známý americký kryptolog ruského původu William Friedman.

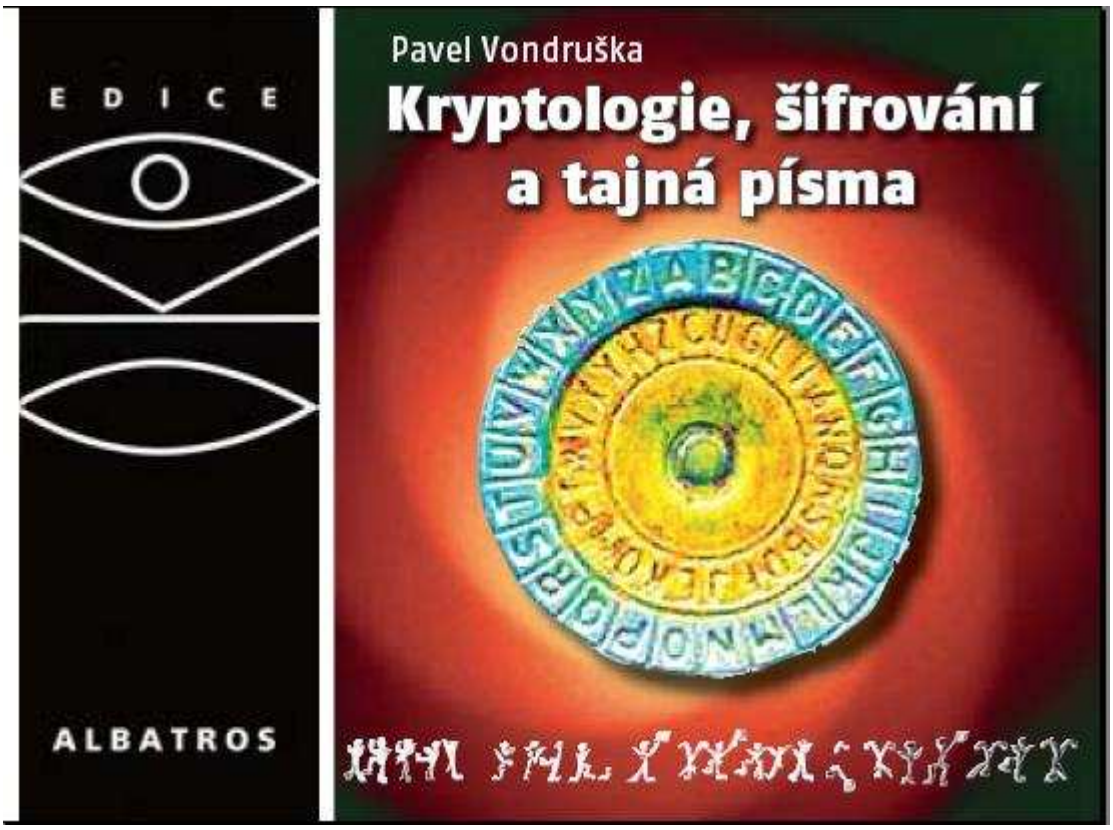
K řešení této úlohy však budete potřebovat méně úsilí než uvedení luštitelé; pomůže vám vyřešení předchozí úlohy a sledování nápovědy, která bude v průběhu soutěže uvedena v Crypto-NEWS na naší stránce.

B. Lektorský posudek na knihu *Kryptologie, šifrování a tajná písma*

Vlastimil Klíma, nezávislý kryptolog, (v.klima@volny.cz)

V minulém článku jsme se zmínili, že v listopadu tohoto roku vyjde v nakladatelství Albatros v edici OKO kniha *Pavel Vondruška: Kryptologie, šifrování a tajná písma.*

S laskavým svolením redakce a lektora vám můžeme již dnes poskytnout posudek, který vypracoval odborný lektor, známý kryptolog Dr. Vlastimil Klíma.



Lektorský posudek na knihu

Lektor: Vlastimil Klíma

Posudek:

Tato kniha obsahuje velmi hodnotné informace o nepříliš známém oboru, který se zabývá utajováním zpráv, šifrováním a "tajným písmem". Poutavým způsobem seznamuje čtenáře s

vývojem šifrovacích a utajovacích systémů a až encyklopedicky tuto oblast postihuje. Kniha je určena především mládeži, ale poutavý jazyk a fascinující historie této vědy vtáhne do děje i mnoho dospělých čtenářů.

Obsahem knihy je přehled šifrových systémů a metod a historický přehled událostí v této oblasti vědy (kryptologii). K popisu používá autor srozumitelný jazyk, kterým vysvětluje odborné termíny a dostatečně je ilustruje. Dociluje čtivosti a pochopitelnosti textu. Autor popsal velké množství šifrovacích a utajovacích systémů, jejichž souhrn v tomto rozsahu nevyšel v češtině a slovenštině vůbec, a lektor si je téměř jist, že pravděpodobně ani v žádném jiném jazyce. Encyklopedický charakter knihy pochopitelně končí zmínkami o moderních šifrovacích systémech, které nelze jednoduše popsat na malém prostoru bez použití algebry a složitějších matematických vztahů. Vývoj v této oblasti je ale podchycen v historickém přehledu kryptologických událostí. Tam jsou zachyceny důležité události několika posledních desetiletí a končí rokem 2006.

Autor používá poutavý popis, doplněný mnoha fakty, jednoduchý a dobře srozumitelný jazyk, a přesto se nedopouští neodborných zjednodušení.

Knihu doplňuje velice vhodně řada úloh. Je to velmi šikovný nápad, neboť z vlastní zkušenosti vím, že jakmile se čtenář pustí do řešení nějaké úlohy, je definitivně pohlcen tímto vzrušujícím tématem. Neplatí to zdaleka jen pro dětské čtenáře, ale minimálně stejným dílem i pro dospělé.

Je zde soustředěno velké množství zajímavých, encyklopedických informací. Některé šifrovací systémy neznal ani lektor, neboť byly jednotlivě roztroušeny v různých dílech. Autor je velmi dobře znalý problematiky, když se mu téměř jako sběrateli podařilo vytvořit takovou kolekci šifrových systémů. Jako příklad zmíním šifru Mistra Jana Husa, o níž jsem neměl ani tušení.

Z faktografického hlediska myslím, že kniha přesahuje obzor "dětské kryptologie" a bude zajímavou i pro dospělého čtenáře a z výše uvedeného důvodu dokonce i pro odborníky v tomto oboru.

Autor, milovník historie, proložil na řadě míst text i historickými poznámkami. Jako čtenář je vítám, protože jsou zajímavé, jako lektor jsem je označil pro případ, kdy bude nutné z tiskařského hlediska text krátit. Tyto pasáže je pak možno vypustit. Pokud to však z hlediska rozsahu bude možné, v knize bych je rozhodně ponechal.

Z odborného hlediska jsem v textu zaznamenal opravdu jen pár velmi drobných nepřesností, které jsem v textu opravil. To jen dokládá autorovu vysokou odbornost a vysokou odbornou hodnotu této knihy. Knihy, původně určené pro mládež, která však určitě zaujme mnoho dospělých čtenářů.

Autor navržené opravy přijal a předkládá text již opravený. Lektor svůj posudek uspíšil, aby případné úpravy textu a jeho eventuelní krácení po doplnění obrázků již mohly probíhat na textu, který je již po všech jazykových, autorských i lektorských úpravách.

Lektor doporučuje vydavatelství zvážit překlad a vydání i v jiných jazycích.

V Praze, dne 19.2.2006
RNDr. Vlastimil Klíma, nezávislý kryptolog

C. Ukázky z knihy Kryptologie, šifrování a tajná písma

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

Se svolením redakce Albatros otiskujeme tři krátké ukázky z knihy *Pavla Vondrušky: Kryptologie, šifrování a tajná písma*. Tato kniha vyjde v edici OKO v listopadu 2006.

1499

Významným představitelem evropské kryptografie byl Němec Johannes Trithemius (někdy psán jako Tritheim) (1462-1516). Byl opatem benediktinského kláštera ve Spanheimu a od roku 1506 v klášteře Sv. Jakuba ve Würzburgu. Napsal řadu významných knih o historii, životopisný slovník slavných Němců, biografii o slavných benediktinech. Dopisoval si s řadou učenců své doby. Je však znám také tím, že se zasloužil o rozkvět vysoké magie v době renesance. Známé jsou jeho spisy *Antipalus maleficiorum* (Varování před černokněžnictvím, 1508) a *Steganographia* (1499). Ač byl označován za mága a kouzelníka, zachoval si kritický úsudek a sám před podvodníky a šarlatány varuje. Šarlatánem nazval např. i proslulého doktora Johannesa Fausta (1480 nebo1485 –1530?). Jeho okultní spisy jsou ovlivněny jeho obrovským zájmem a vírou ve skryté a tajemné síly. Např. roztřídil čarodějnice do 4 přesně definovaných kategorií, zabýval se tříděním andělů atd. Mezi tyto spisy lze zařadit knihu *Steganographia* (Tajné písmo), která se však částečně věnuje i kryptografii. V prvních dvou svazcích popsal elementární substituce (samohláska / souhláska) a utajení textu, kdy se čtou jen určitá písmena na určitých místech a ostatní písmena nedávají žádný smysl. Například lze pro získání otevřeného textu číst pouze druhá písmena z každého druhého slova. Věta : „Takže p**o**dle popisu u**k**áži jak t**o** fungovalo“ - je skrytý zápis slova OKO v popsaném systému.

Pro Trithemia sloužily tyto systémy především ke krytí a zamaskování magických operací, které jsou popsány ve třetí knize, která není věnována kryptografii. Pokud do kryptografie nebudeme počítat tu část, kde Trithemius popisuje, jak na dálku přenášet skrytě a bezpečně text.

Podle něj k tomu stačilo pouze říct zprávu modle nebo obrazu planetárního anděla v okamžik stanovený na základě složitých astrologických výpočtů, zahalit modlu, říci příslušnou formuli a zpráva došla na místo určení bez jakýchkoliv slov nebo šifrovaného textu nebo použití posla.

Jeho pověst a popularita, pokud jde o znalosti tajemných sil, natolik vzrostla, že jeho dílo *Steganographia* se šířilo v rukopisu po stovky let, mnoho lidí si je opisovalo a hledalo v knize tajemství, která tato kniha měla obsahovat. Jeden z opisů knihy vlastnil např. Giordano Bruno. Právě toto dílo způsobilo, že se v následujících letech kryptologie spojovala v obecném povědomí většiny lidí s alchymií a okultními vědami.

1508

V roce 1508 se pustil Johannes Trithemius (1452-1516) do psaní šestidílné knihy výhradně zaměřené na kryptologii. Tuto knihu nazval *Polygraphia*, a to vzhledem k rozmanitosti možných metod psaní, které se v knize vyskytují. Knihu (rukopis) věnoval 24. dubna 1508 císaři Maxmiliánovi I. Dva roky po jeho smrti byla kniha roku 1518 vytištěna, a stala se tak vůbec první tištěnou knihou pojednávající o kryptologii. Její celý název je *Šest knih o polygrafii od Johanna Trithemia, opata z Würzburgu, dříve ze Spanheimu věnované císaři Maxmiliánovi*. Kniha má 540 stran, je tištěna černým a červeným písmem.

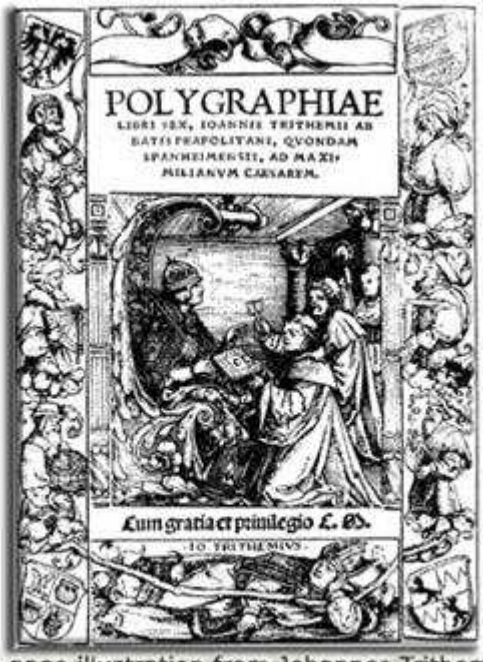
V knize je představen jím navržený šifrový systém nazývaný Ave Maria. Šifra spočívá v tom, že jednotlivým písmenům jsou přiřazena celá slova. Seznam slov volí autor tak, aby dávala smysluplný text – jakousi nevinnou modlitbu. Tak třeba slovo abbot (opat) se zašifruje jako DEUS CLEMENTISSIMUS REGNES AEVUM INFINIVET, kde DEUS = A, CLEMENTISSIMUS = B, REGNES = B atd.

Ve druhé knize je připraveno 284 takovýchto abeced.

Obdobně v knize tři a čtyři jsou připraveny další abecedy, které však již tak nevinně nevypadají. V knize tři jsou použita běžná slova a v knize čtyři dokonce slova umělá.

V pátém díle, který je z kryptologického hlediska nejvýznamnější, je uvedena šifrovací tabulka, tzv. "tabula recta", která je základem pro polyalfabetické šifry.

abcdefghijklmnopqrstuvwxyz
bcdefghijklmnopqrstuvwxyza
cdefghijklmnopqrstuvwxyzab
defghijklmnopqrstuvwxyzabc
efghijklmnopqrstuvwxyzabcd
...
zabcdefghijklmnopqrstuvwxy



The title page illustration from Johannes Trithemius' 1518 "Poiygraphiae libri sex" shows the author wearing his Benedictine habit and kneeling to present his book to the Holy Roman Emperor Maximilian.

Trithemius používal této tabulky k polyalfabetickému šifrování velmi prostě a jednoduše. První písmeno otevřeného textu zašifroval pomocí první abecedy, druhé písmeno pomocí druhé abecedy atd. Slovo OKO by se zašifrovalo touto metodou jako OLQ (otevřené písmeno vyhledejte v prvním řádku a šifrový ekvivalent najdete pod ním v abecedě, která odpovídá pořadí písmene ve zprávě).

Bezpečnostním zlepšením proti polyalfabetickému systému Albertiho je, že se abeceda mění po každém písmenu.

Trithemius měl obrovský vliv na kryptologii. Bylo to jednak proto, že se těšil mimořádné pověsti a věhlasu a jednak proto, že jeho kniha o kryptologii, která byla první tištěnou knihou o tomto tématu, se stala pro zájemce relativně snadno dostupná.

1552-1557

Girolamo Cardano (1501-1576), milánský fyzik, astronom a matematik trpěl až chorobnou touhou získat popularitu. Za svého života napsal neuvěřitelné množství knih (131 vyšlo a dalších 111 zůstalo v rukopise). O kryptologii nenapsal samostatnou knihu, ale své poznatky uložil do dvou spisů věnovaných popularizaci vědy. První se nazýval *De Subtiliate* (1550) a druhý *De Rerum Varietate Libri XVII* (1557). Obě knihy si veřejnost oblíbila pro jejich jasný popis, využití zajímavých až anekdotických příběhů a bohaté ilustrace. Obsahovaly nejmodernější učení fyziky tehdejší doby a byly napsány velmi pokrokovým způsobem. Obě knihy byly překládány a vydávány po celé tehdejší Evropě.

Pokud jde o vývoj kryptologie, přidal Cardano další významnou myšlenku pro zvýšení bezpečnosti polyalfabetické šifry. Pochopil, že změna klíče, který se využívá k určení abecedy pro zašifrování dalšího znaku zprávy, má významný vliv na bezpečnost. Je jasné, že změna hesla před každou zprávou je z hlediska bezpečnosti výhodnější než používat jeden klíč na

šifrování všech zpráv. Kompromitace (prozrazení) hesla v prvním případě vede k rozluštění jen jedné zprávy, ve druhém případě ke kompromitaci celé korespondence. Jak však zajistit, aby mohl být klíč pro výběr abecedy pokaždé jiný? Cardano navrhuje použití autoklíče. Bohužel tuto novou nádhernou myšlenku formuluje nedokonale. Jím popsaný způsob dovoluje určitou nejednoznačnost šifrování, navrhuje opětovné použití klíče vždy na začátku otevřeného slova a nestanoví předání začátečního hesla autoklíče – tj. příjemce i luštitel jsou ve stejném postavení. Proto se jím uvedený systém nepoužíval. Kdyby jej byl dotáhl k dokonalosti, získal by mezi kryptology nesmrtelnou slávu, po které tolik toužil.

Věhlas mu však přinesla jiná zde publikovaná metoda, která se zabývá utajením textu, tedy steganografická metoda. Metoda nese na jeho počest jeho jméno. Metoda byla velmi jednoduchá a i proto se stala velmi oblíbenou. V obdélníkové nebo čtvercové mřížce se vystřihla určitá pole, vzniklá šablona se položila na papír a do děr se zapsalo tajné sdělení. Šablona se zvedla a doplnil se zbytek písmen tak, aby text vypadal jako obyčejná nezávadná zpráva. Šlo tedy o jednoduché skrytí otevřeného textu do těla jiné zprávy, která vypadala jako zcela nezávadná. Cardano navrhoval, aby zpráva byla takto opsána za sebou dokonce 3x, aby se odstranily jakékoli případné problémy při dešifrování. Dešifrování bylo velmi prosté, příjemce přiložil mřížku a text v okénkách jednoduše přečetl.

Cardano proslul také svými důkazy o nemožnosti rozluštit jednoduchou substituci metodou, která byla později popsána jako útok hrubou silou (*Bruttal Force Attack*). Tato metoda je založena na vyzkoušení všech možných klíčů na šifrovaný text. Ukázal, že všech možností jak vytvořit klíč z abecedy čítající N znaků, je N! (N! se čte N faktoriál a je to symbol pro součin všech čísel od 1 do N). Pokud abeceda obsahuje 26 znaků, pak je klíčový prostor tak obrovské číslo, že šifru nelze v průběhu luštitelova života tímto způsobem prolomit. Vzhledem k tomu, že k vyluštění monoalfabetické šifry stačí kryptologovi zpravidla jen několik minut, je toto současně poučným příkladem, že kvalita šifry nezávisí jen na počtu všech možných klíčů. Nicméně i dnes se stává, že firmy zabývající se implementací některého šifrového algoritmu (zvláště méně známého) argumentují obdobně a na počtu klíčů a zdánlivé složitosti dokazují zákazníkovi, že systém je zcela bezpečný a že jej nelze v reálném čase prolomit.

D. Chcete si zaluštit?

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

Pro nedočkavé účastníky naší luštitelské soutěže, ale samozřejmě i pro další zájemce, tu mám malou lahůdku. Můžete se pocvičit na luštění opravdového záchytu. Skutečné šifrové zprávy, která byla zaslána příjemci pomocí SMS.

Šifrový text (včetně mezer resp. „chybějících“ mezer):

Bomkehmayh qyrmpce LAMKAYINI Kihiji Seygal!Sejake gamkeyame.Memkiyigqejaq

Lze předpokládat, že zpráva byla psána tak, aby ji mohl příjemce rozluštit.

Co by Vám mohlo v luštění pomoci:

Autorem této zašifrované SMS je 24 letá česká žena jménem Anežka. Obsahem je buď nějaké sdělení, týkající se vztahu s mužem jménem Pavel nebo je to nesmyslná zpráva, mající za cíl ho pozlobit. Anežka je umělecky zaměřená, ale schopná si i šifrovanou zprávu připravit před napsáním do mobilu. Text může být v českém jazyce, ale pisatel umí i anglicky (možná i další řeči).

Příjemce se marně pokoušel text dešifrovat / rozluštit. Protože se z určitých důvodů již nemůže odesílatelky na obsah SMS dotázat, prosí touto cestou o pomoc ….

Pokud budete úspěšní, prosím o zaslání textu na moji e-mailovou adresu. Zprávu obratem předám.

E. NIST (National Institute of Standards and Technology - USA) a kryptografie.
Recommendation on Key Management – část 3.

Jaroslav Pinkava, CA Czechia, (Jaroslav.Pinkava@zoner.cz)

1. Úvod

Obsahem dnešní informace jsou další dvě kapitoly materiálu [1] - 6. Protection Requirements for Cryptograpic Information + 7. Key States and Transitions.

2. Požadavky na ochranu kryptografických informací

Kryptografický klíčový materiál – to jsou kryptografické klíče a další související informace, které jsou nezbytné pro použití klíčů. Tato specifické informace závisí samozřejmě na typu klíče. Kryptografický klíčový materiál musí být samozřejmě chráněn a to tak, aby příslušná bezpečnostní služba byla smysluplná. Řadu takovýchto ochran zajistí kryptografické moduly evaluované dle FIPS 140-2, pokud se však tyto informace vyskytují mimo takovéto moduly, jsou nezbytné další ochranné prostředky.

Klíčový materiál by měl být dostupný (pro kryptografické operace) po celou dobu s ním související kryptografické služby. Klíče mohou být používány prostřednictvím kryptografického modulu (v aktivní fázi) anebo uloženy externě (s využitím vhodných ochranných prostředků). Některé typy klíčů mohou být archivovány i mimo jejich kryptoperiodu (tj. období, kdy jsou aktivně používány).

Na klíčové materiály mohou být vázány následující typy ochran:

- ochrana integrity (ta musí být použita pro jakýkoliv klíčový materiál). Vždy je pak prováděna kontrola zdroje a formátu získaného klíčového materiálu. Ochrana integrity je prováděna prostřednictvím mechanizmů kryptografické integrity (kryptografické kontrolní

součty, kryptografické hashe, MAC a dig. podpisy) nebo prostřednictvím nekryptografických mechanizmů (CRC, parita,…).

- důvěrnost všech symetrických a soukromých klíčů musí být zabezpečena příslušnými ochranami. Veřejné klíče – obecně ochranu (obsahu) nevyžadují. Symetrické a soukromé klíče – uvnitř validovaného modulu mají vhodnou ochranu zabezpečenu. Pokud se nachází mimo takovýto kryptomodul, musí být jejich důvěrnost zajištěna buď šifrováním (zabalením klíče) anebo kontrolou přístupu ke klíči fyzickými prostředky (např. uložením v sejfu, do kterého je omezený přístup).
- ochrana asociace, ta musí být prováděna tak, aby bylo zajištěno, že příslušná kryptografická služba využívá správný kryptografický materiál (pro ní určený) a v souladu se zamýšleným využitím v aplikaci.
- záruky platnosti (validity) doménových parametrů a veřejného klíče.
-záruky vlastnictví soukromého klíče (tj., že majitel veřejného klíče vlastní i odpovídající soukromý klíč.
-období, po které jsou kryptografické klíče, asociované klíčové informace a další kryptografické parametry (např. inicializační vektory) chráněny , závisí na typu klíče, příslušné kryptografické službě a také na časovém období, ve kterém je příslušná kryptografická služba vyžadována (např. jak dlouho mají být příslušné informace utajovány).

V materiálu je pak proveden přehled požadavků v podobě tabulky (tabulka 5) – pro jednotlivé typy klíčů (soukromý podpisový klíč, veřejný klíč pro ověřování podpisů, symetrický autentizační klíč, soukromý autentizační klíč, veřejný autentizační klíč, symetrický klíč pro šifrování/dešifrování, symetrický klíč pro zabalení klíče,….)
a sice ve vztahu k požadovaným bezpečnostním charakteristikám (typ bezpečnostní služby, ochrany, záruky, období ochrany).

Obdobně tabulka 6. uvádí analogický přehled pro související, resp. na kryptografii navazující informace (doménové parametry, inicializační vektory, sdílená tajemství,…).

3. Ochranné mechanizmy

V průběhu životního cyklu kryptografické informace se může tato nacházet "v tranzitu" (například distribuce klíčů elektronickou či jinou cestou oprávněným uživatelům). Volba konkrétního typu ochranného mechanizmu však může být různorodá. Samozřejmě ne všechny ochranné mechanizmy poskytují stejný stupeň ochrany a je proto vždy třeba pečlivě vážit, kterou ochranu v konkrétním případě zvolíme. A to zejména v závislosti na zvážení možných existujících dostupných typů útoků.

Ochranné mechanizmy jsou jiné pro kryptografické metody v tranzitu a jiné pro uložené informace. Pokud se týká informací v tranzitu, materiál uvádí následující nároky na použité ochranné mechanizmy:

- dostupnost (redundantní kanály, opravné kódy,…)
- integrita (jak prevence, tak i detekce modifikací informací)
- důvěrnost
- propojení (asociace) se zamýšleným použitím či aplikací
- propojení s jinými entitami resp. s dalšími souvisejícími informacemi

Pokud se týká ochranných mechanizmů ve vztahu k uloženým informacím (včetně třeba kopií informací, které jsou v tranzitu) jsou uváděny následující nároky:

- dostupnost (v období, kdy existují data chráněná touto informací)
- integrita (ochrana před modifikacemi prostřednictvím fyzických či kryptografických mechanizmů či obou současně)
- důvěrnost, musí být použit jeden z následujících tří mechanizmů
    1. zašifrování schváleným algoritmem v modulu evaluovaném dle FIPS 140-2
    2. fyzická ochrana v FIPS 140-2 kryptografickém modulu (úroveň 2 či vyšší)
    3. bezpečným uložením s kontrolovaným přístupem (trezor, chráněná oblast).
- propojení (asociace) se zamýšleným použitím či aplikací
- propojení s jinými entitami resp. s dalšími souvisejícími informacemi

4. Stavy klíčů a přechody mezi jednotlivými stavy

Klíče mohou procházet v čase (mezi jejich vygenerováním a jejich zničením) různými stavy. V každém z těchto stavů životního cyklu s nimi bude pracováno jiným způsobem. Klasifikaci těchto stavů provádí materiál z hlediska systémového pohledu:

1. Stav před vlastní aktivací (klíč je již vygenerován, ale ještě není autorizován pro příslušné použití). V tomto stavu může být klíč použit pouze pro důkaz vlastnictví klíče nebo pro potvrzení klíče (např. dvěma stranami v průběhu protokolu pro dohodu na klíči).
2. Aktivní stav (použití pro kryptografickou ochranu informací či jiný kryptografický proces)
3. Deaktivovaný stav (kryptoperioda klíče již skončila, ale existence klíče je stále z nějakých důvodů důležitá.
4. Stav "destrukce klíče" (zničený klíč) – některé jeho atributy však stále mohou existovat (jméno, typ,…)-
5, Kompromitovaný stav (k příslušné informaci se dostala neoprávněná entita)
6. Kompromitovaný a zničený klíč (odlišnost od stavu 4 v tom, že kritické informace vlastní neoprávněná entita anebo je podezření, že je vlastní).

Klíče během životního cyklu přechází z jednoho z popsaných stavů do jiného, každý z těchto možných přechodů má odlišnou logiku a smysl. Tyto přechody jsou pochopitelně jednosměrné.

Asymetrické klíče mají některá specifika. Např. soukromý podpisový klíč se nikdy nenachází v deaktivovaném stavu, ale je vždy ničen bezprostředně s ukončením aktivního stavu. Obdobnou vlastnost mají třeba i veřejný a soukromý klíč, které byly použity v protokolu pro dohodu na klíči – okamžitě po ukončení aktivního stavu jsou ničeny.

5. Literatura

[1] NIST Special Publication SP 800-57 Recommendation on Key Management, Part 1 (http://csrc.ncsl.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf)

F. O čem jsme psali v létě 1999 – 2005

Crypto-World 78/2000

Příloha : 10000.txt , soubor obsahuje prvních 10 000 prvočísel (další informace viz závěr článku "Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla" , str.9) .

Crypto-World 78/2001

Příloha : priloha78.zip (dopis pana Sůvy - detailní informace k horké sazbě, viz. článek Záhadná páska z Prahy, Crypto-World 6/2001)

Crypto-World 78/2002

Crypto-World 78/2003

Crypto-World 78/2004

Crypto-World 78/2005

G. 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 P.Vondrušky a 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 sešity GCUCMP, 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:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS (výběr příspěvků, komentáře a vkládání na web)	Vlastimil Klíma Jaroslav Pinkava Tomáš Rosa Pavel Vondruška
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@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.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
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/