Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 10, číslo 78/2008 **1. srpna 2008**

78/2008

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1245 registrovaných odběratelů)

Obsah :

Příloha: ---

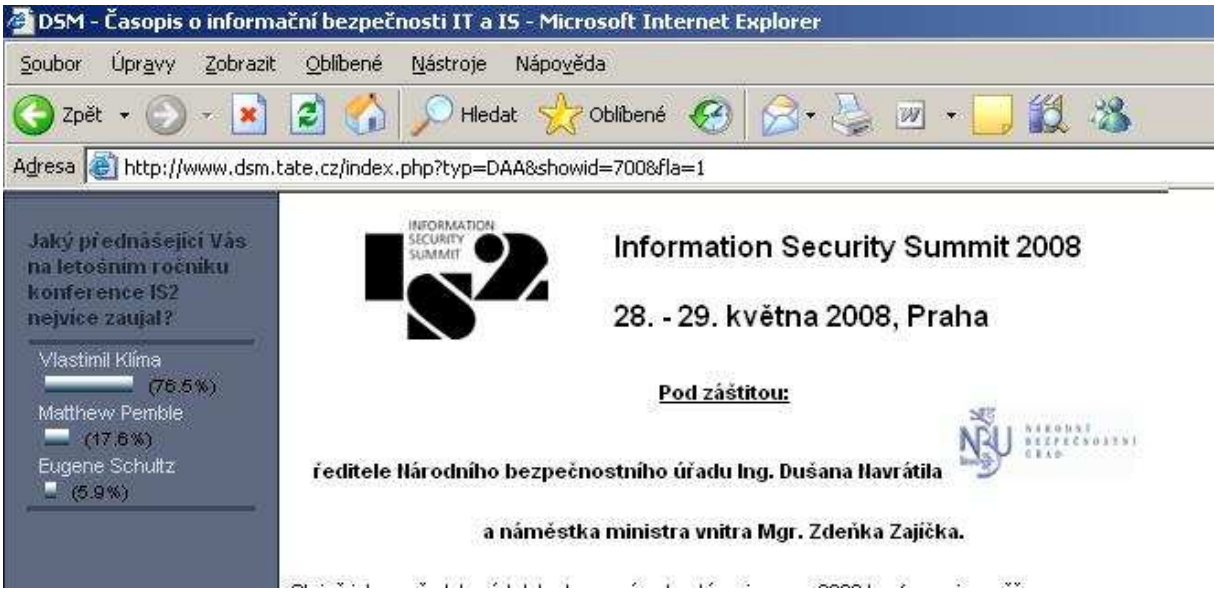
A. Současná kryptologie v praxi

Vlastimil Klíma, kryptolog, v.klima@volny.cz,
http://cryptography.hyperlink.cz

Vážení čtenáři, v tomto čísle zařazujeme (se souhlasem autora) nejlépe hodnocený příspěvek mezinárodní konference IS2 (Information Security Summit 2008). Vystoupení autora bylo vyhodnoceno jako nejzajímavější jak v závěrečné anketě mezi účastníky konference, tak v hlasování na webu pořadatele konference (na obrázku stav hlasování k 16.7.2008).

Prezentaci autora na IS2 naleznete na jeho osobní stránce http://cryptography.hyperlink.cz/ .

Pavel Vondruška



Abstrakt

Tento příspěvek byl zvanou přednáškou na konferenci IS2 2008, která byla určena vyššímu bezpečnostnímu managementu. Uvedl jsem ho tím, že nechci manažerům radit, protože nejsem manažer, ale spíš jim předat zkušenosti a doporučení a docela obyčejně jim říci, jak se na kryptologii dívám po 26 letech praxe.

Klíčová slova: kryptologie, manažeři

1. Úvod

Příspěvek je určen manažerům informačních systémů a bezpečnosti. Jeho cílem je předat jim zkušenosti a doporučení pro jejich činnost, pokud se ve své práci dostanou do kontaktu s aplikovanou kryptologií.

Dnešní kryptologie už není věda o utajování, kterou byla čtyři tisíce let, nyní je to věda o matematických metodách informační bezpečnosti.

Dříve bylo jejím obsahem navrhování šifer a jejich luštění. Dnes je jejím předmětem návrh nejrozmanitějších matematických metod informační bezpečnosti (kryptografie) a na druhé straně odhalování jejich slabin (kryptoanalýza). Výstupem kryptografie nemusí být jen šifra, ale třeba algoritmus prokazující zachování integrity, nepopiratelnosti odeslání digitálního dokumentu elektronickou poštou, protokol prokázání identity nebo protokol výměny klíčů. Výsledkem kryptoanalýzy může sice být odhalený šifrovací klíč nebo rozluštěný otevřený text jako dříve, ale dnes to spíše bude digitální dokument s falšovaným elektronickým podpisem, ale i důkaz toho, že nějaká kryptografická technika má větší riziko prolomení, než bylo o ní předpokládáno v době jejího nasazení. Z různých hledisek se kryptologie může zdát výjimečná, a *proto by kryptologové rádi viděli, aby jejich dítě bylo něco zvláštního.* Z manažerského hlediska však při podrobnějším zkoumání žádné velké rozdíly od ostatních metod informační bezpečnosti nenajdeme. Například jsme si vyvrátili postupně argumenty, že:

- kryptologii se na světě věnuje velmi málo lidí (skutečným *teoretickým matematickým metodám* antivirů, antispamů apod. se věnuje možná ještě méně lidí než kryptologii),
- kryptologie je více založena na matematických základech (kryptologie používá velmi mohutně *heuristické metody*, možná ještě více než antiviry; používané metody jsou sice matematické, ale matematika až na jednu nebo dvě výjimky stejně nezajišťuje jejich absolutní neprolomitelnost),
- důsledky nesprávného použití nebo chyby nebo výběru špatné kryptografické techniky mohou mít větší následky než u jiných metod (*těžko říci, co způsobí větší škodu*, jestli špatně nastavený antispam, který zahodí poptávkový mail, jež mohl půl roku živit firmu, nebo ztráta notebooku s nešifrovanými daty).

*Odtud činíme **první manažerský závěr**:*

Kryptologie je jedna z metod informační bezpečnosti, není nutné se jí věnovat více než ostatním metodám, jako třeba antivirům, antispamům nebo firewallům .

Jediný rozdíl, na který jsme přišli, je, že má bohatší historii a dokonce už zasáhla i do chodu dějin. To však ostatní metody informační bezpečnosti v nejbližších čtyřech tisíciletích mohou ukázat také. Přesto stále platí, že:

Kryptologie je pro nás užitečná a někdy přímo nepostradatelná, umožňuje zajistit potřebné a důležité základní služby informační bezpečnosti, na nichž jsou sestaveny miriády dalších služeb.

Jsou to:

- **utajení,**
- **autentizace,**
- **integrita,**
- **nepopiratelnost.**

Tyto služby kryptografie dosahuje různými technikami, algoritmy, protokoly, nástroji. Mezi základní patří

- **Symetrické šifry - proudové, blokové,**
- **Autentizační kódy zpráv (MAC),**
- **Hašovací funkce,**

- **Klíčové hašovací autentizační kódy zpráv (HMAC),**
- **Generátory náhodných znaků a pseudonáhodné generátory,**
- **Asymetrická schémata digitálního podpisu,**
- **Asymetrická schémata pro šifrování,**
- **Asymetrická schémata dohody na klíči,**
- **Kryptografické protokoly,**
- **a další.**

V každé z uvedených oblastí existuje vždy mnoho *algoritmů* a většinou i několik uznávaných *mezinárodních norem a standardů*, které mají různé *parametry* a *vlastnosti*, vhodné pro různé *druhy použití*. Konkrétních *technik* (*šifer, protokolů, modů, parametrů*) stále přibývá, místo aby ubývalo. Vzniká mnoho *norem*, které říkají, jak se mají tyto algoritmy *implementovat, nastavovat, kombinovat a používat.* Tyto normy je důležité *přesně dodržovat*. Mnohokrát bylo ukázáno, že *„lidová tvořivost" ve vlastním výkladu norem je většinou fatální*. I když kryptografických norem jsou tisíce, pro daný konkrétní případ se jejich množina velmi zužuje. *Normy jsou většinou vyjádřením zkušeností řady odborníků v oboru, jejich aktuálnost a bezpečnost bývá sledována, a proto by měly být velmi dobrým pomocníkem pro aplikování kryptografických metod, pokud pro danou oblast existují.*

Dnes není nedostatek kryptografických technik, ale **chybí vrstva kryptoinženýrů a kryptoinformatiků**, kteří by je uměli správně *kombinovat a implementovat.*

Každá norma musí být konfrontována se současným stavem kryptologie, neboť jsme ukázali, že kryptologie je velmi živá a přináší nové útoky a s nimi i nová protiopatření, která se musí průběžně a co nejrychleji zapracovávat jako v ostatních metodách informační bezpečnosti.

Příklad:

- Nejpoužívanější norma pro aplikaci nejpoužívanějšího asymetrického kryptosystému, PKCS#1, prošla dvěma zásadními změnami.

  (První útok na ni ukázal Bleichenbacher v roce 1998 [2], v roce 2003 byl útok ještě prohlouben, viz Klíma-Rosa-Pokorný [3]. V obou případech byly přijaty záplaty v nejdůležitějších aplikacích, například protokolu SSL, ihned po vydání zprávy).

- IP šifrátory.

  (Šifrují protokol IP a byly konstruovány podle platných, prověřených a vyzrálých standardů IPSec. Tato zařízení se předřadí lokálním sítím nebo jednotlivým počítačům v síti a zajišťují, že veškerý provoz mezi nimi je šifrován. Proto tato zařízení mohou být propojena prostřednictvím jakékoliv veřejné sítě, třeba internetu. Tyto drahé „železné krabice" se obvykle jednou nastaví, a pak léta pracují a spolehlivě chrání přenášená data, aniž bychom se o ně museli nějak zvlášť starat. Použití nejnovějších kryptoanalytických metod (tzv. postranních kanálů, viz dále) však ukázalo, že komunikaci lze poměrně snadno dešifrovat! Proto tato zařízení bylo nutné okamžitě překonfigurovat, jinak by se staly zbytečnými kusy železa, vhodnými jen do šrotu [1, díl 51 a 52].)

2. Novinky

Na téma „poslední vývoj v kryptologii“ hovořil zde na konferenci IS2 naposledy známý světový kryptolog Aarjen Lenstra v roce 2001. Od té doby se toho dosti událo. Připomeňme některé události:

- V celosvětové veřejné soutěži byl přijat nový šifrovací standard AES, USA jej dokonce poté schválily pro ochranu utajovaných informací stupně TOP SECRET
- Byly nalezeny slabiny v konstrukci téměř všech moderních hašovacích funkcí, včetně nejpoužívanější SHA-1, která za dva roky již nebude podporovaným standardem a měla by být do té doby nahrazena,
- připravuje se standard SHA-3 v celosvětové veřejné soutěži jako AES,
- Byly nalezeny kolize hašovací funkce MD5 a jejich generování je otázkou vteřin na notebooku,
- Byla ukázána možnost rozšifrování protokolu SSL,
- Byla ukázána možnost získání privátního podpisového klíče PGP,
- Byla objevena revoluční metoda kryptoanalýzy, tzv. postranní kanály. Jejich aplikace přinesla snové výsledky a jedná se o bezprecedentně nejúčinnější metodu kryptoanalýzy,
- Kryptologie a aplikovaná kryptologie se začala vyučovat na mnoha vysokých školách a univerzitách v Česku, na Karlově Univerzitě byl k tomu založen nový studijní obor.

3. Interpretace a vyhodnocování kryptologických zpráv (novinek)

Pro manažera bezpečnosti je vyhodnocování novinek z oblasti virů, záplat operačních systémů nebo programů běžnou věcí, kterou je dávno zautomatizována a přenechána pověřeným pracovníkům. Avšak vyhodnocování novinek z oblasti kryptologie je většinou ponecháno na bedrech manažerů a při absenci „podnikového kryptologa“ je přenecháno lidové tvořivosti pracovníků IT. Odtud činíme ***druhý manažerský závěr***:

Kryptologie není nic zvláštního, je to jedna z metod informační bezpečnosti, je však nutné se jí věnovat alespoň tak jako ostatním metodám, jako třeba antivirům, antispamům nebo firewallům.

Interpretace kryptologických novinek je dosud nejslabší stránkou aplikované kryptologie, a to i v kryptologicky vyspělých zemích, kde je vrstva kryptoinženýrů a kryptoinformatiků vychovávána o 10 - 15 let déle než u nás.

4. Současný stav

Kryptologie nám v současné době neposkytuje příliš mnoho jistoty. Možná máme obavy, že je tak trochu sopkou, u níž nevíme, jestli nezačne bouřit.

Prvním velkým rozporem v kryptologii je, že většina jejích metod je založena na nedokazatelné bezpečnosti, o níž hovořil A. Lenstra zde v roce 2001 [4]. To má praktické důsledky v tom, že musíme pracovat s rizikem prolomení těchto metod. Pokud tato rizika

pouze ignorujeme, může pro nás mít zásadní objev fatální důsledky. Vždyť co jiného by znamenalo objevení metody faktorizace velkých čísel pro světové internetové bankovnictví nebo pro světový internetový obchod? Co všechno pečlivě zašifrované v minulosti by bylo odhaleno? Co by znamenalo, kdyby zásadní pokrok v použití kvantových počítačů umožnil dešifrovat všechny symetrické šifry?

Druhým velkým rozporem kryptologické současnosti je rozpor mezi teorií a praxí.

Na jedné straně existují metody šifrování, které nerozluští ani nejmocnější luštitelské služby světa, a přitom je může používat obyčejný občan. Na druhé straně jsou na exponovaných místech používány šifry nebo jiné kryptografické metody tak špatně, že jejich význam je degradován. Na jedné straně masově používaný operační systém obsahuje silné nástroje šifrování, na druhé straně je málokdo používá z důvodu složitosti, obavy o ztrátu dat nebo nedůvěry z existence zadních vrátek. Na jedné straně existují volně dostupné zdrojové kódy PGP a dalších programů, na druhé straně jsou tak složité, že za bezpečnost celého produktu dá ruku do ohně jen málokdo.

Moderní kryptoanalýza dokáže proměnit šifrovací zařízení v samotné vykonavatele útočníkových výpočtů. To je důsledek revolučního rozvoje kryptoanalýzy. Takové možnosti kryptoanalytikové nikdy předtím v historii neměli. Tímto způsobem byla v roce 2003 dešifrována i komunikace chráněná protokolem SSL [3].

Kryptologie je ve fázi exponenciálního rozmachu do šířky, hloubky i významu nových věcí, které přináší, v kladném i záporném směru. To vede k řadě problémů v praxi, která nestačí vstřebávat nové výsledky a zapracovávat existující know-how do kryptografických produktů a systémů. Kryptologie přináší nové úžasné možnosti obráncům, ale také útočníkům. A chybí odborníci, kteří by byli schopni sledovat tento vývoj a v praxi aplikovat odpovídající obranná opatření. ***Setkáváme se proto s celou škálou aplikací, prostředků a systémů, které patří k absolutní špičce, i se školáckými chybami na všech úrovních***, včetně velmi citlivých z hlediska možného dopadu. I v celosvětově rozšířených bezpečnostních produktech nalezneme hrubé chyby, které tyto produkty otevírají útočníkům. Příčinou je ohromný tlak konkurence a trhu. Bezpečnost je až v druhé řadě za funkčností. U produktu se v napjatých termínech často stihne vývoj tak, že je částečně splněna funkčnost, bezpečnost se doplňuje na poslední chvíli nebo „až pak“. ***Místo kryptologů a kryptoinženýrů kryptologii nakonec často „dolepují“ aplikační programátoři.*** Jenže bezpečnost nelze dolepovat, musí být od začátku zahrnuta v architektuře a někdy bohužel znamená i uživatelský diskomfort. Odtud činíme tuto ***manažerskou poznámku***:

V oblasti aplikované kryptologie se obecně vzato neuvědoměle příliš riskuje.

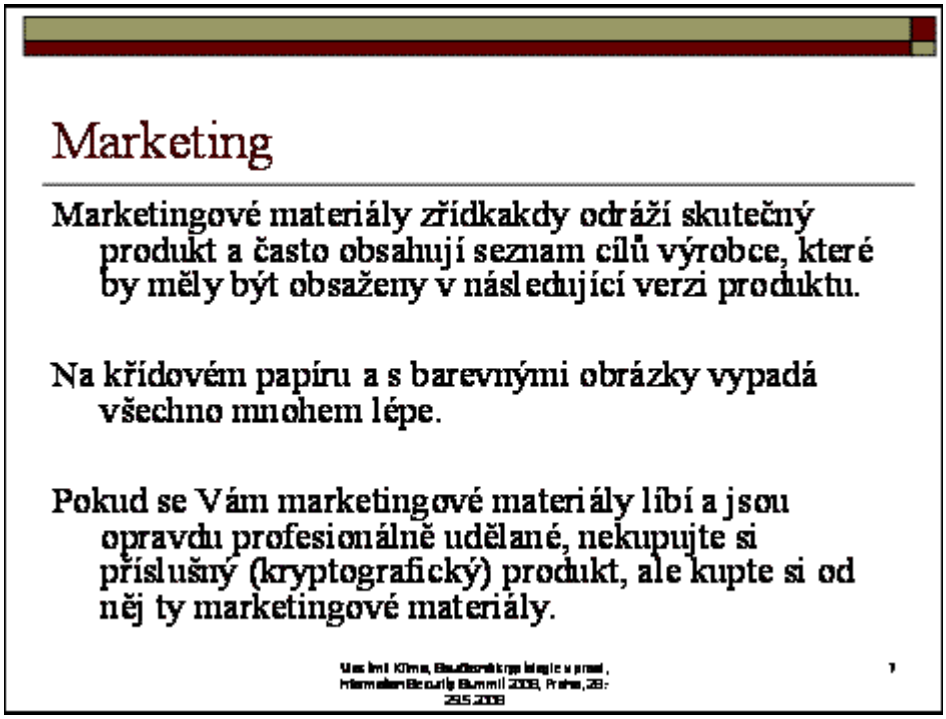
5. Interpretace marketingových materiálů

Z výše uvedeného vyplývá, že *je nutné velmi pečlivě ověřovat pravdivost informací, uváděných o kryptografických produktech.*

Typické chyby marketingových materiálů: nedostatečná specifikace technik, použití nekvalitního RNG, aplikace staré normy, použití nevhodného modu šifrování nebo nevhodné techniky, nedokonalá autentizace, nedomyšlené zálohování a obnova klíčů, nekvalitní generování klíčů, nezajištěná ochrana klíčů po celou dobu jejich životnosti (včetně dokonalého mazání), nedomyšlená obnova dat, nemožnost kryptografické konfigurace a aktualizace.

Mezi základní rady, jak hodnotit marketingový materiál, patří také:

- ověření a ochota dodavatele umožnit ověření, že produkt realizuje danou techniku tak, jak tvrdí,
- vyzkoušení praktického chování produktu ve zkušebním provozu,
- posouzení vlastností nezávislým subjektem,
- ověření, že výrobek má certifikáty, které deklaruje (často tento certifikát mají jiné verze daného produktu).



6. Základní teze

Základní teze tohoto příspěvku je:

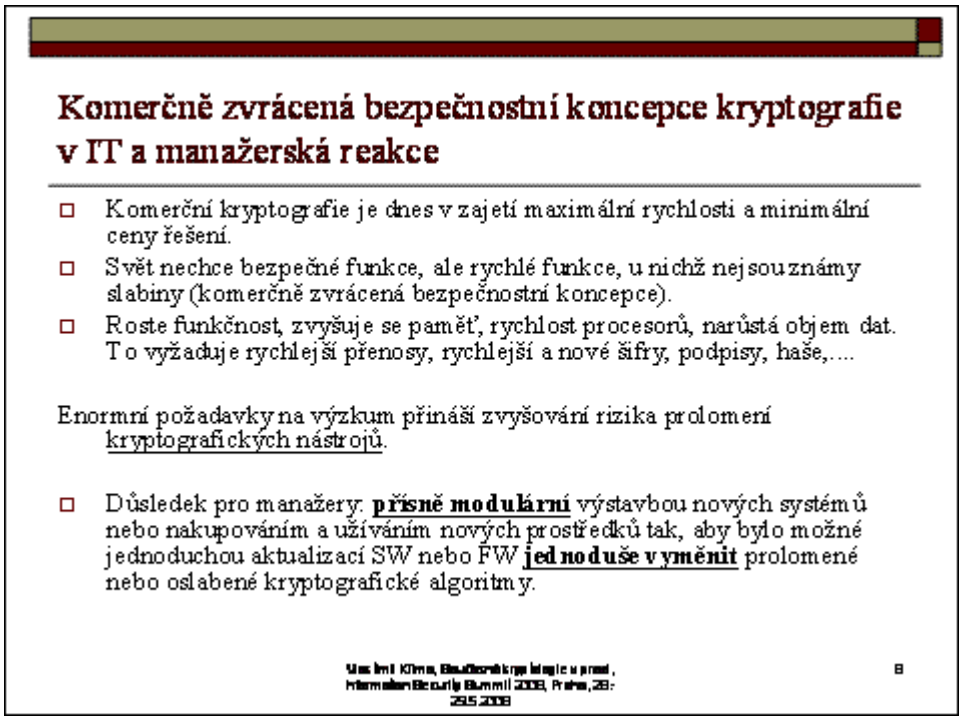
Kryptologie není nic zvláštního, je to jedna z metod informační bezpečnosti, chovejte se k ní úplně stejně jako k ostatním metodám, třeba jako k antivirům, antispamům, bezpečnostním záplatám operačních systémů a aplikací nebo personální, procesní či fyzické bezpečnosti.

Pravděpodobně nenajdeme manažera, který by v rámci své funkce zkoumal logické algoritmy antivirů, antispamů nebo nastavoval firewall. Proč by se tedy manažeři měli orientovat v kryptologických metodách? A přesto po nich často někdo chce rozhodnout, jak dlouhý klíč mají mít certifikáty nebo jestli k šifrování firemní sítě zakoupit ten či onen šifrovací prostředek nebo co pro firmu znamená zpráva z médií, že elektronický podpis je ohrožen. Příčinou je, že v průmyslu IT chybí vrstva kryptoinženýrů a kryptoinformatiků, kteří by manažerům měli připravit podklady k rozhodnutí. Rozhodování bez dostatečných informací dnes v oblasti kryptologie na svých bedrech odnáší manažeři. A proto další rada je:

Pěstujte si svého kryptologa

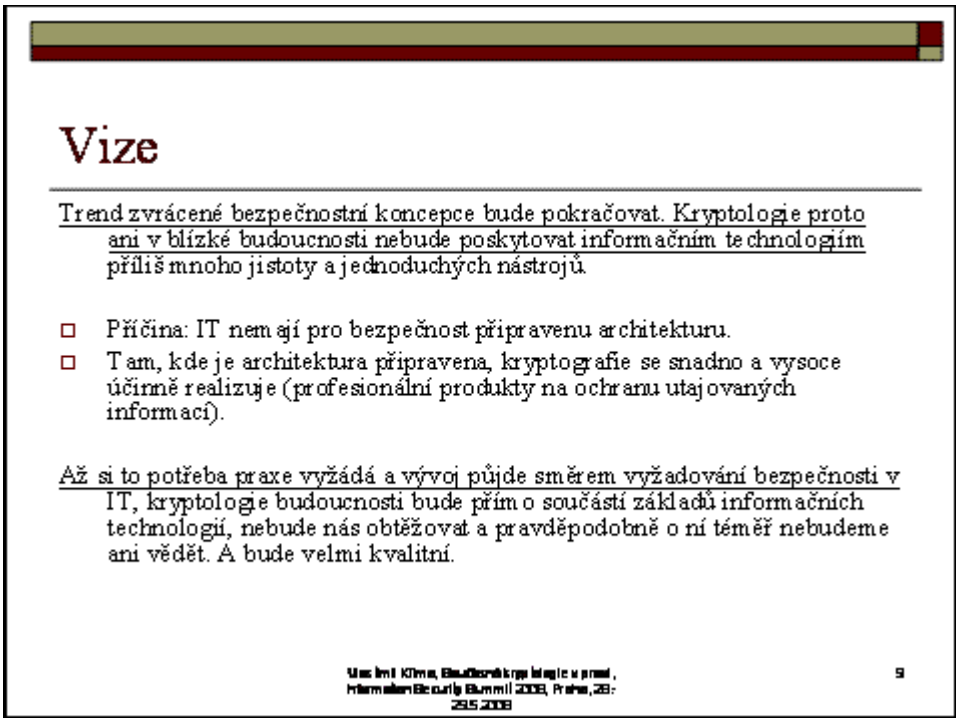
Pěstujte si svého odborníka, který bude mít kryptologii na starosti a bude sledovat novinky, vzdělávat se, informovat vás a připravovat podklady pro vaše rozhodnutí. Protože samostatného kryptologa si většina firem a institucí nebude chtít nebo moci dovolit, je možné zadat tuto problematiku někomu třeba jako poloviční pracovní náplň. Ideální, pokud to nebude člověk z IT, abyste měli dva úhly pohledu. Současný stav, kdy manažeři musí na různých školeních také vstřebávat technické problémy kryptologie (často podávané tak populárně, že je to stejně málo efektivní) je dlouhodobě špatný.

7. Honba za rychlostí

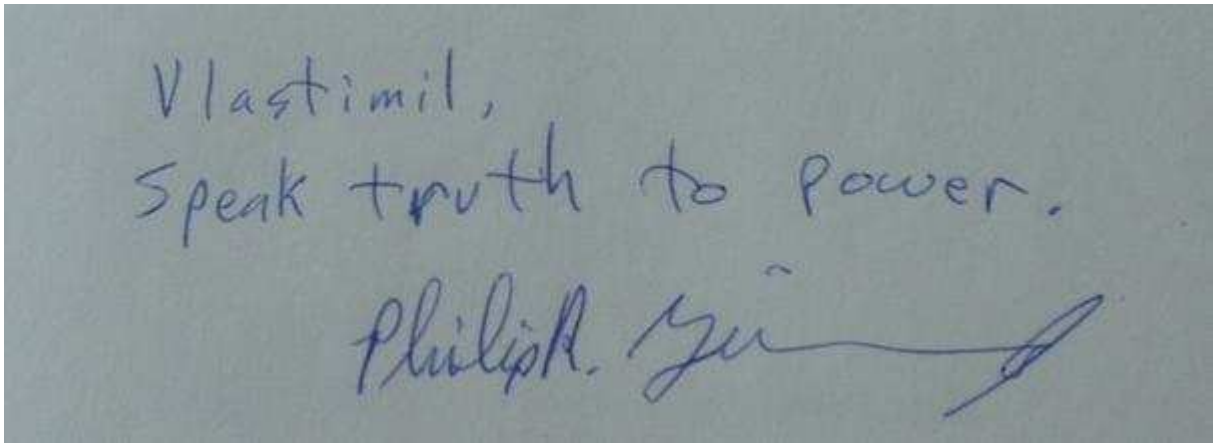


Komerční kryptografie je dnes v zajetí maximální rychlosti a minimální ceny řešení.
Svět nechce bezpečné funkce, ale rychlé funkce, u nichž nejsou známy slabiny.
Toto je důsledek tržní ekonomiky, která na první místo staví funkčnost. Elektronika se zrychluje, zvyšuje se paměť, rychlost procesorů, narůstá objem dat. To vyžaduje rychlé přenosy. Důsledkem jsou nové požadavky na rychlé proudové šifry, rychlé blokové šifry, rychlé hašovací funkce, rychlé asymetrické kryptosystémy. Například nový světový hašovací standard SHA-3 bude muset být pravděpodobně nejen bezpečnější než starý, ale také rychlejší. Tyto požadavky jsou však klasicky v přímém rozporu, nicméně praxe je taková. To klade na výzkum enormní požadavky a vede to ke *zvyšování* rizika prolomení takových kryptografických nástrojů (podtrhujeme slovo zvyšování, protože uvedené riziko existuje i tak, vzhledem k nedokazatelnosti bezpečnosti většiny kryptografických nástrojů). Protože uvedený trend bude pokračovat, manažeři na to musí reagovat ***přísně modulární výstavbou nových systémů nebo nakupováním a užíváním nových prostředků tak, aby bylo možné jednoduchou aktualizací SW nebo FW jednoduše nahradit prolomené nebo oslabené kryptografické algoritmy***.

8. Jak budeme šifrovat v roce 2100 ?



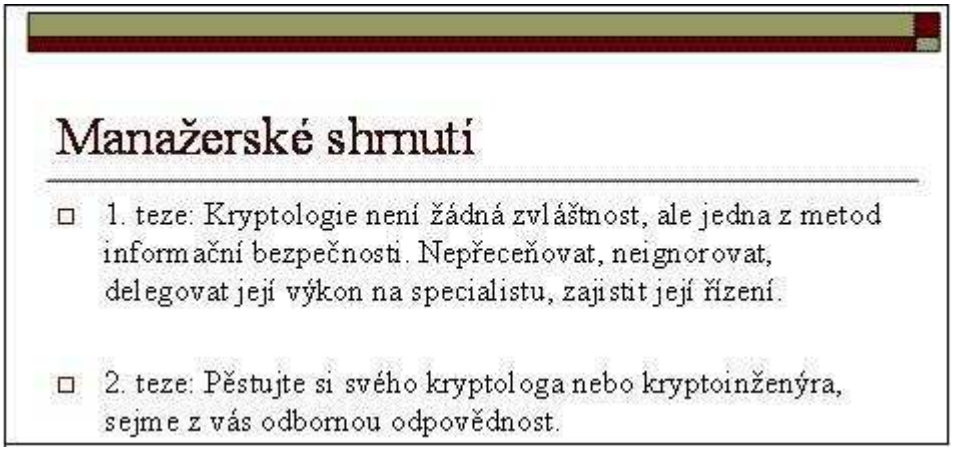
Kryptologie obecně neposkytuje v současné době informačním technologiím příliš mnoho jistoty a jednoduchých nástrojů. Příčinou je, že matematické metody informační bezpečnosti se v současných informačních technologiích nedají jednoduše a účinně použít, protože současné informační technologie nejsou pro účel bezpečnosti konstruovány, nemají pro to připravenu vhodnou architekturu. Až budou informační technologie od základu navrhovány tak, aby mohly být bezpečné nebo aby u nich bezpečnost mohla být bezpečně doplňována, kryptologie jistě přijde s jednoduchými a bezpečnými nástroji. To dokazují profesionální produkty například na ochranu utajovaných informací, kde bezpečnost je od jejich počátku základem jejich architektury. Tam kryptologie již nabízí vysoce účinná řešení. Pokud vývoj půjde směrem vyžadování bezpečnosti, kryptologie budoucnosti bude přímo součástí základů informačních technologií, nebude nás obtěžovat a pravděpodobně o ní téměř nebudeme ani vědět.



Rada otce PGP: „říkej mocným pravdu“

9. Manažerské shrnutí

V příspěvku jsme se snažili popsat současný stav, provést jeho analýzu a vyvodit závěry. Z manažerského hlediska jsme učinili tento závěr: kryptologie není žádná zvláštnost, ale jedna z metod informační bezpečnosti. Z toho také plyne, jak se k ní chovat: neignorovat, nepřeceňovat, delegovat její výkon na specialistu a zajistit pouze její řízení.



10. Poděkování

Rádi bychom poděkovali za velice cenné připomínky zejména Mgr. Pavlu Vondruškovi a doc. Vašku Matyášovi, Ph.D. Druhému jmenovanému patří též velký dík za skvělý překlad článku do angličtiny.

11. O autorovi

RNDr. Vlastimil Klíma je absolventem Matematicko-fyzikální fakulty Univerzity Karlovy v Praze, nyní nezávislý kryptolog. V ČR patří k zakladatelům oboru kryptoanalýzy postranními kanály. Je autorem přes 200 příspěvků a přednášek. Ve světě je znám nejrychlejší metodou hledání kolizí MD5 a odhalením slabin v OpenPGP a SSL/TLS. Navrhl nový koncept hašovacích funkcí SNMAC (HDN) a blokových šifer (DN). Osobní stránky: http://cryptography.hyperlink.cz

Literatura

[1] Vlastimil Klíma, Tomáš Rosa: Archiv (56+...) článků ze seriálu *Kryptologie pro praxi*, publikovaných v časopisu Sdělovací technika, dostupné na stránkách autorů http://cryptography.hyperlink.cz/, http://crypto.hyperlink.cz/

[2] Daniel Bleichenbacher: Chosen Ciphertexts Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1, CRYPTO '98, pp. 1 - 12, Springer - Verlag, 1998,

[3] Vlastimil Klima, Ondrej Pokorny, Tomas Rosa: Attacking RSA-based Sessions in SSL/TLS, CHES 2003, pp. 426 - 440, Springer - Verlag, 2003, http://eprint.iacr.org/2003/052.pdf,

[4] Aarjen Lenstra: Poslední vývoj v kryptografii, Information Security Summit 2001, Praha, 30.-31. května 2001.

B. Zabezpečení souborů v kanceláři

Luděk Caha (xcahal00@stud.feec.vutbr.cz)

Úvod

Článek se zabývá kvalitou kryptografické ochrany souborů, které se běžně používají v kancelářích. Mezi popisované formáty jsou zařazeny ZIP, RAR a 7z. Dále je popsán program pro vytváření šifrovaných disků TrueCrypt a ochrana dokumentů v kancelářských balících Microsoft Office a OpenOffice.org. Součástí článku je i popis ochran formátu PDF.

Základem je heslo

Před popisem samotných formátů k zajištění ochrany dat je nutné si připomenout, že všechny níže uvedené formáty jsou kromě síly použitého šifrovacího algoritmu chráněny také sílou použitého hesla. Bez volby kvalitního hesla není schopen kvalitní ochranu zajistit ani ten nejlepší šifrovací algoritmus. Na rozdíl od různých počítačových a platebních systémů, které mohou omezovat počet pokusů pro zadání hesla, jsou níže popisované soubory dány útočníkovi zcela na pospas a může tedy zkoušet prolomit jejich ochranu rychlostí několika tisíc hesel za sekundu. Z výše uvedeného tedy plyne, že heslo pro tyto soubory musí být kvalitnější než pro systémy, kde je počet chybných pokusů omezen.
Doporučení pro tvorbu hesel existuje celá řada, proto zde uvedu stručně pouze pár nejzákladnějších pravidel.

- Heslo musí obsahovat minimálně 8 znaků, nejlépe 14 a více znaků
  (program TrueCrypt dokonce doporučuje 20 a více znaků)
- V hesle se musí střídat malá a velká písmena
- Heslo musí obsahovat speciální znaky
- Heslo nesmí mít význam ve slovníku (nesmí dávat žádný smysl, nesmí být slovem)
- Heslo nesmí být údajem z okolí (rodné číslo, datum narození, telefonní číslo, atd.)

Další informace o problematice volby hesla lze nalézt například v [1]-[5].

Proč je vlastně nutné volit takto komplikovaná hesla? U příliš krátkých hesel je možné ochranu prolomit hrubou silou vyzkoušením všech možných kombinací. Například u hesel obsahujících 4 znaky je útok záležitostí průměrně několika minut, u hesel s 6 znaky pak několika dní a pro 8 znaků již několika let. Uvedená čísla jsou pouze přibližným průměrem a mohou se výrazně lišit v závislosti na výkonu počítače nebo jiného zařízení, které se pro jejich luštění použije [1]. Obecně platí, že při vzrůstající délce hesla se čas potřebný pro provedení útoku hrubou silou neúměrně zvyšuje a nelze ho tedy již spolehlivě použít.
Ale i v případě, že je heslo dostatečně dlouhé, lze provést snadno jeho prolomení tzv. slovníkovým útokem. Jedná se o techniku, kdy se jako heslo zkouší použít různá slova nebo jejich kombinace z předpřipraveného slovníku. Proto by dobré heslo nemělo mít žádný smysluplný význam, aby nebylo možné použít tento rychlý typ útoku.
Na základě výše uvedených informací je tedy nutné volbu hesla nepodceňovat. Existují ale situace, kdy i při volbě kvalitního hesla je možné soubor dešifrovat, protože používá nekvalitní šifrovací algoritmus. Touto problematikou se proto budou zabývat následující kapitoly.

Archívy s heslem

Pro ochranu libovolných souborů lze využít například komprimační programy. Mezi hojně používané formáty patří ZIP, RAR a také v poslední době velmi se rozšiřující 7z (7-Zip). Nemá cenu zde řešit, který z nich dosahuje lepšího kompresního poměru, protože to není tématem článku. Pro ochranu dat je dokonce výhodnější používat tyto archívy zcela bez komprese, protože tak dojde až k desetinásobnému zrychlení celého procesu vytváření archívu. Navíc komprimace většiny dnes používaných souborů není již příliš efektivní, protože soubory jsou obvykle komprimovány samy o sobě a to ať jde o dokumenty kancelářských balíků, obrázky nebo zvuk.

Mezi archívy je asi nejrozšířenější ZIP a to také díky široké podpoře v řadě programů a operačních systémů. Z kryptografického hlediska mohou být soubory uvnitř ZIP kontejneru chráněny pomocí tří různých šifer.

- Zip 2.0 kompatibilní šifrování (přenosné)
- 128-bit AES šifrování (silné)
- 256-bit AES šifrování (silnější)

Z vyjmenovaného přehledu je pro ochranu dat nejslabší Zip 2.0 šifrování. Na tento archív existuje spolehlivý útok při znalosti části textu uvnitř archívu. Celý útok je pak otázkou pouze čtyř minut, známe-li alespoň 4096 bytů textu nebo 60 hodin při znalosti pouze 16 bytů textu. Jako známý text lze využít například hlavičky „exe“ nebo dalších souborů, které se vždy v souborech opakují.
Za spolehlivou ochranu dat lze považovat až AES (Advanced Encryption Standard). Tato šifra je nástupcem zastaralého systému DES (Data Encryption Standard), který byl v roce 1997 prolomen.
Na šifru AES zatím neexistuje žádný efektivní útok. O kvalitě této šifry svědčí i to, že ji od roku 2003 používá americká vláda a armáda. Přesto ani data v ZIP archívech s touto šifrou nemusí být v bezpečí. V programu WinZIP do verze 8.0 se totiž vyskytovala chyba v generátoru náhodných čísel, která způsobuje, že tyto archívy lze luštit v řádu desítek minut. Od verze WinZIP 8.1 je ale tato chyba již odstraněna.
Stručně lze tedy k archívu ZIP zopakovat, že je spolehlivě chráněn pouze s použitím šifry AES. Řada programů ale nemusí tuto šifru ještě podporovat, takže nedokáží archívy s touto šifrou rozbalit. Navíc pro zajištění bezpečnosti dat je nutné v případě použití programu WinZIP sáhnout minimálně po verzi 8.1 a vyšší.

Druhý v seznamu archívů je formát RAR, který podporuje pouze jeden druh šifrování, čímž má uživatel ulehčenu úlohu, protože nemusí šifru vybírat.

- 128-bit AES šifrování

Na rozdíl od ZIP archívu se ale jedná pouze o 128 bitové AES šifrování, 256 bitová verze zde chybí. I přesto nejsou na RAR archív zatím známy žádné speciální útoky, které by umožňovaly prolomení jeho ochrany jiným způsobem než slovníkovým útokem nebo hrubou silou.

Poslední v krátkém seznamu je uveden formát 7z. Protože se jedná o formát nejmladší, tak je také opatřen nejsilnější šifrou.

- 256-bit AES šifrování

Stejně jako u archívu RAR zde uživatel nemá na výběr, takže se při výběru šifry rovněž nemůže splést.

Tab 1: Porovnání ochrany jednotlivých archívů

Archív \ Šifrování	**Slabé**	**Silné**	**Silnější**
ZIP	Zip 2.0 kompatibilní	128-bit AES	256-bit AES
RAR		128-bit AES	
7z			256-bit AES

Z přehledu v tabulce 1 vyplývá, že nejvýhodnější je využívat archív 7z, protože zaručuje, že bude vždy ochráněn silným 256-bit AES šifrováním. Díky tomu, že se jedná o formát nejmladší, patří k jeho dalším výhodám možnost zašifrovat i názvy souborů v archívu a podpora velikosti archívu až do 16000000000 GB. Z dalších výhod lze zmínit podporu v operačních systémech Linuxu i Windows a šíření komprimačního programu zdarma. Další podrobnosti o tomto formátu lze získat v [9].

TrueCrypt

Při použití archívů s hesly sice zajistíme bezpečné přenášení souborů mezi počítači, ale již nezajistíme potřebnou ochranu dat v počítači samotném. Chceme-li soubory modifikovat nebo jinak používat, musíme je z archívu nejdříve vybalit na disk. Útočník pak může tyto soubory na disku snadno najít v nešifrované podobě a to i v případě, že jsou smazány nebo ještě v horším případě pouze přesunuty do koše.

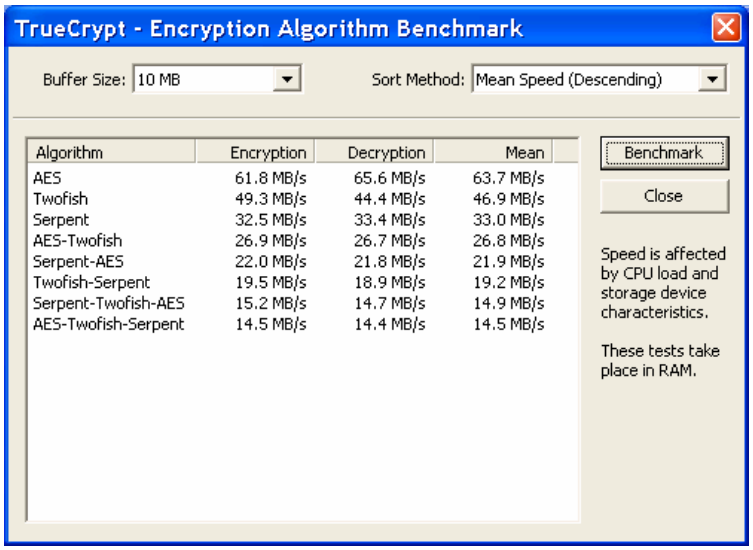
Řešit tuto situaci lze například zašifrováním disku, na který se budou soubory rozbalovat. Mezi nejznámější nástroje k tomuto účelu patří program TrueCrypt. Mezi jeho základní vlastnosti patří možnost vytvořit virtuální šifrovaný disk na jiném disku, nebo zašifrovat celý oddíl disku včetně přenosných disků připojených přes USB. Dokonce lze zašifrovat i disk, na kterém je nainstalován operační systém Windows.

K nejdůležitější součásti programu TrueCrypt ale patří použité šifrovací algoritmy. Program nabízí hned tři různé šifry, které používají dlouhé 256 bitové klíče. První v řadě je algoritmus AES (Advanced Encryption Standard) jinak také nazývaný Rijndael. Algoritmus Rijndael je vítězem soutěže z roku 1998 o návrh AES, proto se obvykle také používá pod tímto názvem. Dalšími dvěma kandidáty v této soutěži byly šifry Serpent a Twofish, které program TrueCrypt také podporuje. Pro zajímavost je výsledné pořadí pěti finalistů soutěže o AES zobrazeno v následující tabulce 2.

Tab 2: Výsledky finále soutěže o návrh AES

Jméno	Hlasů pro	Hlasů proti	Celkem
Rijndael (AES)	86	10	76
Serpent	59	7	52
Twofish	31	21	10
RC6	23	37	-14
MARS	13	83	-70

Kromě samotných šifer AES (Rijndael), Serpent a Twofish umožňuje program TrueCrypt také použití jejich kombinací, kdy dojde k několikanásobnému zašifrování dat pro jejich lepší ochranu. Toto několikanásobné šifrování ale zvyšuje nároky na výkon systému, jak ukazuje přehled dosažitelných rychlostí pro jednotlivé šifry v systému TrueCrypt na obrázku 1.



Obr 1: Test rychlostí algoritmů použitých v programu TrueCrypt

Kromě praktického testu rychlostí umí TrueCrypt také zakázat zápis do swapovacího souboru systému, kam by se mohla data ukládat v nešifrované podobě. Mezi vlastnosti programu, které si zaslouží ještě vyzdvihnout, patří například i návod, jak správně vymyslet heslo, který se zobrazuje přímo při jeho zadávání. Volba správného hesla je totiž velmi důležitá pro zajištění ochrany dat, jak popisuje první kapitola, ale ve většině jiných programů na to není uživatel obvykle upozorněn.
Na závěr této kapitoly lze ještě uvést, že z pohledu ochrany dat může být program TrueCrypt při použití kombinace několika algoritmů ještě účinnější než archív 7z. Navíc při připojení virtuálního disku lze data používat přímo bez nutnosti je nejdříve z archívu vybalovat.

Microsoft Office

Přestože je ochrana pomocí programu TrueCrypt velice účinná, její nevýhodou je, že se musí do počítače instalovat samotný program TrueCrypt. To může vypadat jako zbytečná komplikace při snaze ochránit třeba jeden dokument. Proto lze pro uzamčení jednoho dokumentu využít ochranu, kterou nabízí přímo kancelářský balík Microsoft Office.
Následující text bude zaměřen převážně na dokumenty programů Word a Excel, ale ochrana dalších dokumentů tohoto kancelářského balíků je analogická.

Na začátek by bylo dobré se zmínit, že dokumenty MS Office lze chránit více hesly. První heslo slouží pro otevření dokumentu a další pro povolení jeho editace. O kryptografickou ochranu se jedná pouze v případě hesla pro otevření dokumentu. Hesla pro zápis do dokumentu neposkytují žádnou ochranu dat, protože záleží pouze na programu, který dokument otevírá, jestli bude toto omezení dodržovat. Hesla pro zamezení zápisu tedy slouží pouze k ochraně proti nechtěnému přepsání dokumentu, nikoli pro ochranu jeho obsahu. Kryptografickou ochranu dokumentu tedy zajišťuje pouze heslo pro otevření dokumentu.
Dále je nutné zmínit, že balík MS Office již není nejmladší, takže se i ochrana v různých verzích dokumentů u něj postupně vyvíjí, jak ukazuje tabulka 3.
V nejstarších dokumentech byla ochrana provedena prostým xorováním hesla a uloženého textu. Tuto ochranu lze snadno prolomit uhodnutím jednoho slova v dokumentu. Novější MS Office 97/2000 již používá pokročilejší šifrování, ale pouze s 40bitovým klíčem, jehož prolomení hrubou silou lze úspěšné provést do 5 dní. Navíc proti takto chráněným dokumentů

lze použít i speciální útok s názvem „Rainbow attack“, který je schopen pomocí 4GB předgenerovaných dat prolomit 99,5% všech dokumentů do jedné minuty.

Tab 3: Šifrování dokumentů MS Office

Verze	Algoritmus	Zabezpečení
Office 95 a starší	XOR - prosté xorování textu s heslem	Velmi slabé
Office 97/2000	Kompatibilní se sadou Office (40-bit klíč)	Slabé
Office XP/2003	RC4 - chybně generován inicializační vektor (128-bit klíč)	Slabé
Office 2007	128-bit AES (v registrech lze zvýšit na 256-bit AES)	Silné

V následujících verzích XP/2003, které jsou dnes nejčastěji používány, se Microsoft dopustil stejné chyby jako v případě XOR šifrování u Office 95. Sice je zde použito RC4 šifrování, ale při ukládání souboru je použit stále stejný inicializační vektor pro generování pseudonáhodné postupnosti. Důsledkem této situace je, že k prolomení ochrany stačí mít dvě různé verze stejného souboru. Po operaci XOR mezi těmito verzemi nám totiž vznikne:

$$C_3 = C_1 \oplus C_2 = Z_1 \oplus K_1 \oplus Z_2 \oplus K_2$$

Ale chyba v MS Office způsobuje, že pro klíče platí $K_1 = K_2$ takže lze dále psát.

$$C_3 = Z_1 \oplus K \oplus Z_2 \oplus K = Z_1 \oplus Z_2 \oplus K \oplus K = Z_1 \oplus Z_2 \oplus 0$$
$$C_3 = Z_1 \oplus Z_2$$

Z výše popsané operace nám tedy vznikne kryptogram, kde je stará verze souboru zašifrována novější verzí téhož souboru, a nikoliv pseudonáhodnou postupností, jak by bylo pro zajištění ochrany potřeba [10].
Také samotná šifra RC4 není v současné době již považována za bezpečnou a přestává se používat. K jejímu prolomení došlo například i v protokolu WEP, který se používá v bezdrátových WiFi sítích.
V nejnovějších MS Office 2007 je již pro ochranu dokumentů použito 128-bit AES šifrování a není zatím znám žádný způsob pro její prolomení. Pro zvýšení ochrany lze šifrovací klíč prodloužit na 256 bitů, toto nastavení ovšem nelze provést přímo v MS Office, ale je nutné zvýšit zabezpečení celého systému promocí systémového registru [11].
Zarážející na MS Office zůstává, že chyba v MS Office 2003 nebyla zatím žádnou záplatou opravena a nepomůže ani instalace rozšíření „MS Office Compatibility Pack“, který umožní Office 2003 načítat a ukládat soubory v novém formátu Office 2007, kde je již problém vyřešen. Bezpečné šifrování dokumentů v MS Office je v současné době tedy možné pouze v nejnovější verzi MS Office 2007 [11].

OpenOffice.org

Alternativou k MS Office je stále populárnější kancelářský balík OpenOffice.org. Součástí tohoto balíku je rovněž možnost chránit dokumenty pomocí hesla. OpenOffice.org ukládá soubory dle OASIS specifikace OpenDocument v1.0 [12]. Dle této specifikace je dokument tvořen XML dokumenty, které jsou zabaleny do jednoho ZIP archívu. Na první pohled by se tedy mohlo zdát, že pro ochranu dokumentu by mohla být využita ochrana použitého ZIP formátu, ale tak tomu ve skutečnosti není.
OpenDocument používá vždy ZIP archív bez hesla. Šifrovány jsou v něm až jednotlivé soubory (XML, obrázky a další). Každý soubor v ZIP archívu je šifrován samostatně

s vlastním inicializačním vektorem a vlastním zasolením. Přehled informací o jednotlivých šifrovaných souborech je pak k dispozici v souboru s názvem „META-INF\manifest.xml“, který je vždy uvnitř každého ZIP archívu, který OpenOffice.org vytvoří.
Po stručném seznámení, co je vlastně šifrováno, můžeme přikročit k samotnému šifrovacímu algoritmu. V případě formátu OpenDocument se jedná o blokovou šifru Blowfish. Šifra Blowfish podporuje klíče v délce 32 – 448 bitů. OpenDocument využívá klíče délky 128 bitů.
Mezi výhody šifry Blowfish patří její vysoká rychlost. V současné době není znám efektivní způsob jejího prolomení. Sice se objevilo několik článku o jejím úspěšném prolomení, ale jednalo se vždy pouze o modifikace této šifry. Plná šifra Blowfish s 16 rundami zatím prolomena nebyla. Mezi její známé nevýhody patří existence slabých klíčů, jejich použití je ale velmi nepravděpodobné. Přesto se tato šifra již spíše přestává používat. Například z programu TrueCrypt byla vyřazena v březnu 2007.

Adobe Portable Document Format (PDF)

Poslední kapitola článku je vyhrazena často používanému formátu PDF. Tento dokument může obsahovat několik druhů ochran, ale pouze v jednom případě se jedná o ochranu kryptografickou.
V první řadě je možné u dokumentu nastavit omezení pro tisk, kopírování obsahu, vkládání poznámek atd. Tato ochrana neobsahuje žádné kryptografické metody, tudíž záleží čistě na použitém prohlížeči, jestli bude tato omezení respektovat.
Dále je v PDF definováno heslo autora dokumentu, které opravňuje k editaci dokumentu. Stejně jako v předchozím případě záleží pouze na editoru, jestli bude toto omezení respektovat.
Poslední ochrana, která je definována v PDF, slouží k zamezení čtení dokumentu. Tato ochrana je jako jediná založená na kryptografických metodách, proto ji nelze snadno obejít použitím vhodného programu.
V současné době již PDF podporuje ochranu pomocí AES, ale starší verze tento algoritmus šifrování nepodporovaly, přesto se ještě stále používají v různých PDF tiskárnách atd., proto zde je uveden přehled vývoje šifrování u jednotlivých verzí PDF.

Tab 4: Vývoj ochrany u formátu PDF

Formát	Prohlížeč	Algoritmus	Zabezpečení
PDF 1.1	Acrobat 2.0	Zavedena první ochrana	
PDF 1.2 - 1.3	Acrobat 3.0 - 4.0	Proprietární 40-bit šifra	Velmi slabé
PDF 1.4 - 1.5	Acrobat 5.0 - 6.0	Proprietární RC4 128-bit	Slabé
PDF 1.6 - 1.7	Acrobat 7.0 - 8.0	RC4 až 256-bit DES až 128-bit **Triple DES 168-bit** RC2 až 128-bit AES 128-bit AES 192-bit AES 256-bit	Silné

Z tabulky 4 je patrné, že do verze PDF 1.3 je možné dokumenty snadno dešifrovat a to jak hrubou silou, tak dokonce i rychlejšími speciálními útoky. Následující verze PDF 1.4 - 1.5 používají šifru RC4, která není v současné době také již považována za bezpečnou a pomalu se od ní upouští. Od verze PDF 1.6 je nově zavedena podpora celé řady algoritmů, které by měly být prohlížeče schopny podporovat při dešifrování. Pro šifrování ale používají produkty společnosti Adobe pouze algoritmus Triple DES, jak je uvedeno ve specifikaci „PDF

Reference sixth edition“ [15]. Algoritmus Triple DES používá 168 bitový klíč a nejsou proti němu známy žádné efektivní útoky. Přesto se často přestává používat, protože je pomalejší než modernější AES.

Závěr

Z výše popsaných informací vyplývá, že pro zajištění kvalitní ochrany souborů je nutné zvolit nejen kvalitní heslo, ale i typ souboru, který podporuje dostatečně moderní šifrovací algoritmus. Většina současných formátů v nejnovějších verzích používá algoritmus AES, který jim zajišťuje vysokou ochranu a současně je i velmi rychlý.

Literatura

[1] Bezpečné heslo. [online]. [cit 2008-7-10] Dostupné z: http://cs.wikipedia.org/wiki/Bezpe%C4%8Dn%C3%A9_heslo

[2] Vytváření silnějších hesel. [online]. [cit 2008-7-10] Dostupné z: http://www.microsoft.com/cze/athome/security/privacy/password.mspx

[3] Nástroj pro kontrolu hesla. [online]. [cit 2008-7-10] Dostupné z: http://www.microsoft.com/cze/athome/security/privacy/password_checker.mspx

[4] Šustr J.: (Ne)bezpečná hesla. [online]. [cit 2008-7-10] Dostupné z: http://www.systemonline.cz/clanky/ne-bezpecna-hesla.htm

[5] Häring D.: Jak zvolit bezpečné heslo? [online]. [cit 2008-7-10] Dostupné z: http://www.linuxzone.cz/index.phtml?idc=398&ids=1

[6] WinZip. [online]. [cit 2008-7-10] Dostupné z:http://www.winzip.com/prodpagewz.htm

[7] WinRar. [online]. [cit 2008-7-10] Dostupné z:http://www.rarlab.com/rar_archiver.htm

[8] 7-Zip. [online]. [cit 2008-7-10] Dostupné z:http://www.7-zip.org/cs/7zf.html

[9] TrueCrypt. [online]. [cit 2008-7-10] Dostupné z: http://www.truecrypt.org

[10] Hongjun Wu: The Misuse of RC4 in Microsoft Word and Excel. [online]. [cit 2008-7-10] Dostupné z: http://eprint.iacr.org/2005/007.pdf

[11] Justin Klein Keane: Microsoft Office Encryption 2003 and 2007. [online]. [cit 2008-7-10] Dostupné z: http://www.madirish.net/?article=207

[12] OASIS Standards and Other Approved Work. [online]. [cit 2008-7-10] Dostupné z: http://www.oasis-open.org/specs/index.php#opendocumentv1.0

[13] Open Document Format for Office Applications (OpenDocument) v1.0, May 2005. [online]. [cit 2008-7-10] Dostupné z: http://www.oasis-open.org/committees/download.php/12572/OpenDocument-v1.0-os.pdf

[14] Adobe PDF Technology Center. [online]. [cit 2008-7-10] Dostupné z: http://www.adobe.com/devnet/pdf/pdf_reference.html

[15] PDF Reference and Related Documentation, April 2007. [online]. [cit 2008-7-10] Dostupné z: http://www.adobe.com/devnet/acrobat/pdfs/pdf_reference.pdf

[16] Stručná historie formátu PDF. [online]. [cit 2008-7-10] Dostupné z: http://homepage.mac.com/ondrej/prezentace/PDF-historie.html

[17] Pinkava J.: Úvod do kryptologie, květen 1998. [online]. [cit 2008-7-10] Dostupné z: http://crypto-world.info/pinkava/uvod/uvod98.pdf

[18] Popis šifry Blowfish. [online]. [cit 2008-7-10] Dostupné z: http://moon.felk.cvut.cz/~pjv/Jak/_info/i677/html/blowfish.htm

[19] RC4. [online]. [cit 2008-7-10] Dostupné z: http://en.wikipedia.org/wiki/RC4

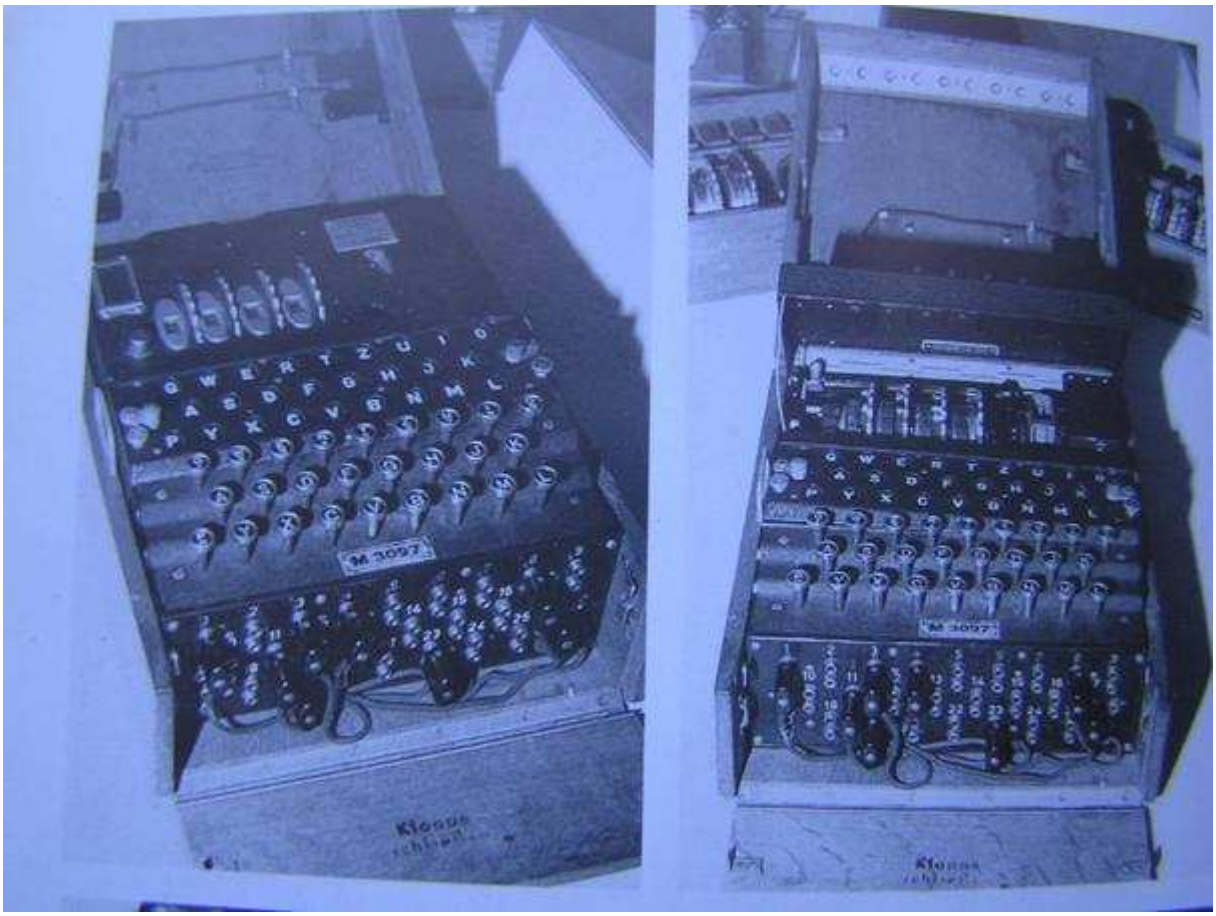
[20] Password Recovery Software. [online]. [cit 2008-7-10] Dostupné z: http://www.elcomsoft.com/prs.html

C. Z dějin československé kryptografie, část VIII.

Trofejní šifrovací stroje používané v Československu v letech 1945 - 1955. Šifrátory ENIGMA, ANNA a STANDARD

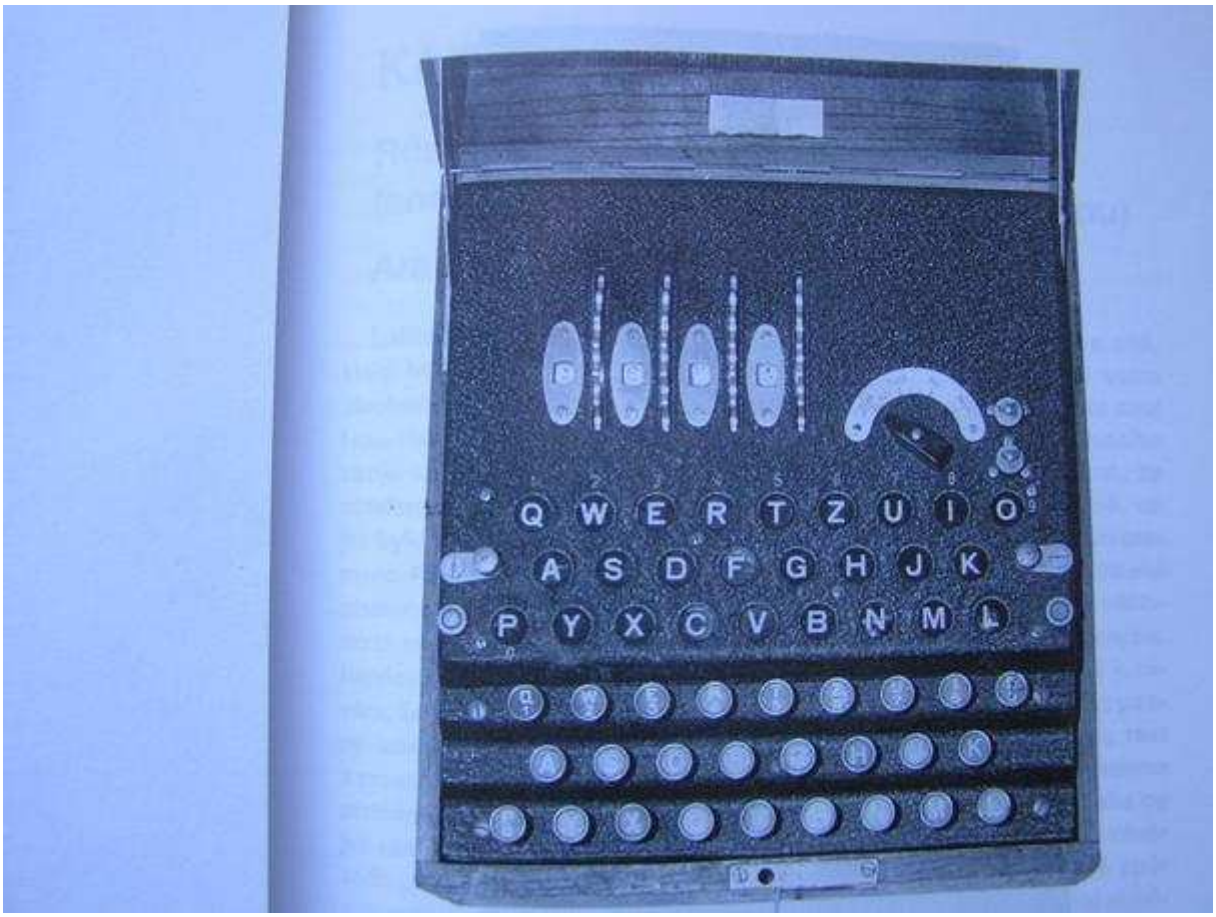
Mgr. Karel Šklíba (karel.skliba@cryptoworld.info)

Po skončení druhé světové války se do Československa dostalo několik desítek trofejních německých šifrovacích strojů, které byly v poválečných letech používány v československé armádě pro zajišťování šifrového spojení a pro výrobu heslových materiálů. Jednalo se zejména o všeobecně známé německé diskové šifrátory ENIGMA a již méně běžné německé diskové šifrátory ANNA. Jako jednotlivé kusy byly do Československa získány německé šifrovací stroje STANDARD a SCHLÜSSELGERÄT a šifrovací stroj švédského původu C-36 CONVERTOR, který byl švédskou firmou Aktienbolaget Cryptoteknik dodáván francouzské armádě odkud se dostal do Československa. Tuto firmu založil inženýr Arvid Gerhard Damm a po jeho smrti ji převzal jeho syn, nejslavnější konstruktér šifrovacích strojů 20. století, inženýr Boris Caesar Wilhelm Hagelin (1892 – 1983). Stroje SCHLÜSSELGERÄT Schl.Ger.41 a C-36 CONVERTOR pracovaly na odlišném principu než diskové stroje typu ENIGMA. Jednalo se o stroje s vnitřní tvorbou hesla s na svou dobu velmi dlouhou periodou, které se mod 26 připočítávalo k otevřenému textu. Tento způsob vyvinul a několikrát patentoval právě Boris Hagelin. Jeden kus stroje, který pracoval na tomto principu a byl vyráběn pod označením BC-52 HAGELIN od roku 1952 švýcarskou firmou Borise Hagelina Hagelin – Cryptos A.G., byl rovněž v československé šifrové službě počátkem 60. let minulého století k dispozici. Mnoho modelů šifrovacích strojů Hagelinovy konstrukce se nachází ve firemním muzeu společnosti Crypto A.G. ve švýcarském Steinhausenu.



Legendární německý šifrovací stroj **ENIGMA** byl vyráběn v řadě verzí a modifikací. Nejrozšířenější byl třídiskový model používaný za 2. světové války německými pozemními silami Wehrmachtu. Tyto stroje vyráběla firma Chifriermaschinen Geschelschaft Heimsoeth(?) und Rinke, Berlin W35 (pravděpodobně Steglitzerstrasse 2). Do Československa se však dostaly zejména modely čtyřdiskové, které byly za 2. světové války využívané německým námořnictvem. V československé armádě bylo po 2. světové válce k dispozici několik desítek těchto šifrátorů a byly zde v letech 1950 až 1955 používány pro předběžné (off-line) šifrování. U několika útvarů se zachovaly jednotlivé kusy až do konce 80. let minulého století jako historická rarita. V roce 1985 byl k dispozici jeden funkční stroj s označením na štítku M 2384. Na ilustračním obrázku, který byl převzat z publikace Hugh Sebag-Montefiore: „ENIGMA The Battle for the Code“, Phoenix London 2001, je zobrazen tentýž model s označením na štítku M 3097.

Druhý ilustrační obrázek ENIGMY se 4 disky, s ne úplně přesnými popisky, je převzat z publikace Simon Adams: „Šifry a kódy od hieroglyfů po hackery“, Slovart Bratislava 2003.



Snímek „počeštěné“ ENIGMY je reprodukován z knihy Jiří Janeček: „Gentlemani (ne)čtou cizí dopisy“, Books Brno 1998.

Šifrátor ENIGMA M 2384 byl čtyřdiskový komutátorový obousměrný stroj o rozměrech asi 400 x 300 x 120 mm. Pro vstup textu byl opatřen mechanickou klávesnicí se dvěma registry tvaru

Q W E R T Z U I O
1 2 3 4 5 6 7 8 9

A S D F G H J K

P Y X C V B N M L
0

(druhý řádek představuje druhý číslicový registr).

Pro výstup textu sloužilo 26 kruhových průsvitných okének, které byly označeny písmeny abecedy, byly umístěny nad klávesnicí a uspořádány do třířádkové tabulky analogicky jako klávesnice

1 2 3 4 5 6 7 8 9
Q W E R T Z U I O

A S D F G H J K

P Y X C V B N M L
0
(Číslice byly vyznačeny vedle okének)

Jednotlivá okénka byla podsvícena žárovičkami na bateriový zdroj. Po zmáčknutí vstupní klávesy se sepnul kontakt příslušného elektrického obvodu, signál prošel disky a komutátorem a rozsvítila se žárovička pod příslušným okénkem výstupní tabulky. Zároveň vykonaly disky krokování podle příslušného krokovacího algoritmu. Disky krokovaly směrem dopředu, tj. k osobě šifréra, a proto abecedy nebo čísla, které označovaly v okénkách vedle disků jejich aktuální polohu, vzrůstaly. Krokovací algoritmus byl následující:

- první kolo zprava udělalo po zmáčknutí klávesy vždy 1 krok
- druhé kolo zprava udělalo zároveň jeden krok v případě, že jeho převodová páčka byla aktivována výčnělkem na obvodu prvního kola
- třetí kolo zprava udělalo zároveň jeden krok v případě, že jeho převodová páčka byla aktivována výčnělkem na obvodu druhého kola
- čtvrté kolo zprava, což byl zpětný vratný disk, udělalo zároveň jeden krok v případě, že jeho převodová páčka byla aktivována výčnělkem na obvodu třetího kola.

Všechny čtyři základní disky stroje byly označeny (pravděpodobně sériovým) číslem A863 a průchozí kola navíc římskými číslicemi I, II, III a vratný disk IV. Polohy těchto disků byly označeny velkými písmeny uspořádané mezinárodní abecedy

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z .

Výčnělky pro krokování byly na každém kole s výjimkou vratného dva nebo tři a byly označeny takto:

disk I G U
disk II M S
disk III B K V ,

což odpovídalo příslušnému značení pro polohu kola.

Náhradní disky byly označeny (pravděpodobně sériovým) číslem A11522 I, A11522 II, A11522 III, A11522 IV a další A13363 I, A13363 II, A13363 III, A13363 IV a jejich polohy byly označeny čísly

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 .

Tento model šifrátoru ENIGMA byl opatřen jedním dvoupolohovým přepínačem s polohami AUS a EIN , který sloužil pro uvolnění všech čtyř disků k provedení počátečního nastavení polohy disků. Dále byl opatřen jedním čtyřpolohovým přepínačem s polohami

hell Baterie - dnl - aus - Sammler, 4V

(zkratka dunkel)

V „počeštěných“ verzích šifrátoru ENIGMA byl štítek u tohoto přepínače nahrazen slovy

Silně Slabě Vyp. Akum.
Bat.

Dvojité zdířky komutátoru byly uspořádány do tří vodorovných řad pod dřevěným odklápěcím krytem na přední části šifrátoru a byly označeny čísly

1 2 3 4 5 6 7 8 9
10 11 12 13 14 15 16 17
18 19 20 21 22 23 24 25 26

Propojení komutátoru se obvykle provádělo čtyřmi kabely opatřenými na obou koncích dvoukolíkovými zástrčkami. Propojení komutátoru spolu s vybranou sérií disků, u které bylo aktuálně vytvořeno nastavení krokovacích výčnělků, tvořilo dlouhodobé nastavení stroje. V některých sítích spojení bylo propojení komutátoru měněno každý den. Krátkodobé nastavení, odlišné pro každou zprávu, představovalo nastavení počáteční polohy čtyř disků. Šifrovací stroj ENIGMA byl opatřen elegantním dřevěným krytem.

Německý šifrovací stroj **ANNA**, který byl pracovníky československé šifrové služby familiérně nazýván Andula, pracoval na stejném principu a byl analogické konstrukce jako šifrátory ENIGMA. Byl však o generaci mladší, konstrukčně sofistikovanější a prakticky jednoúčelový pro on-line šifrování s dálnopisnými stroji. Za 2. světové války jej používal Wehrmacht, údajně zejména Rommelova armáda v Severní Africe a byl používán s dálnopisy značky LORENZ, které vyráběla firma SEL, tj. Standard Elektrik Lorenz. Podle svědectví z května 1982 byl tento šifrátor za války v SSSR luštěn. Firma SEL pravděpodobně vyráběla i šifrovací stroje ANNA a podle pamětníků byl jejich konstruktérem Ing. Weber, který po válce pracoval jako šéfkonstruktér dálnopisů československé provenience ve Zbrojovce Brno, snad do konce padesátých let. Jeho bratr, stejného jména a akademického titulu, pracoval údajně jako šéfkonstruktér v tomtéž období u západoněmecké firmy SEL. V Československu bylo po

válce k dispozici asi 50 kusů šifrovacích strojů ANNA a v letech 1950 až 1955 byly tyto trofejní šifrátory používány v Československé lidové armádě pro šifrování i pro výrobu hesla.

ANNA byl diskový komutátorový šifrátor na mechanický pohon klikou. Vstup znaku do šifrátoru byl z dálnopisu a výstup opět na dálnopis. Šifrování probíhalo sčítáním mod 2 jednotlivých bitů pětibitového dálnopisného kódu. Stroj měl 12 disků, jejichž číslování zprava doleva s příslušnými periodami kol bylo takovéto:

číslo disku	12	11	10	9	8	7	6	5	4	3	2	1
perioda disku	43	47	51	53	59	37	61	29	26	41	31	23
kontakty	6	6	6	6	5	6	2	6	6	3	3	3

Každý disk měl jednotlivé polohy označeny čísly od 01 až do hodnoty délky příslušné periody (např. 61). Disky krokovaly tak, že hodnoty označení poloh klesaly. Disky byly výměnné a je pravděpodobné, že v náhradních sadách disků existovaly i disky s ještě jinými periodami. Kromě kontaktů měly jednotlivé disky v každé poloze kolíček, který mohl být buď aktivně vysunut, nebo pasivně zasunut a vysunutý kolíček ovlivňoval krokování. Kola s čísly 1, 2, 3, 4, 5 krokovala vždy o 1 krok. Kolo číslo 5 ovlivňovalo krokování kola číslo 6 a kolo číslo 7 pravděpodobně krokovalo vždy o 1 krok. Kola číslo 6 a 7 byla řídící pro zbývající kola číslo 8, 9, 10, 11 a 12, která krokovala buď všechna o jeden krok, nebo všechna stála. To záviselo na nastavení kolíčků na řídících kolech 6 a 7.

Šifrátor ANNA měl tzv. Klartext funkci, která, pokud byla aktivována, pravděpodobně způsobovala, že krokování 6. kola o periodě 61 bylo zbrždďováno o jeden krok v závislosti na otevřeném textu. Tato záležitost však není dostatečně prozkoumána.

Popsaný šifrovací stroj ANNA byl k dispozici v roce 1985 a v roce 1997 byl jeden stroj ANNA zachován ve školicím středisku v Pardubicích.

Posledním šifrovacím strojem, který byl stejného principu a analogické konstrukce jako ENIGMA, byl šifrátor **STANDARD**. Jednalo se o diskový obousměrný komutátorový elektromechanický stroj německého původu. Šifrovací stroje STANDARD vyráběla firma Chiffriermaschinen A.G., Berlin W35, Steglitzerstrasse 2 .

Vstup znaků textu do stroje byl pomocí klávesnice o dvou registrech tvaru:

Q	**W**	**E**	**R**	**T**	**Z**	**U**	**I**	**O**	**P**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**

A	**S**	**D**	**F**	**G**	**H**	**J**	**K**	**L**	**Y**
%	**§**	**,**	**/**	**=**	**+**	**8**	**1**	**;**	**:**

X	**(*)**	**C**	**V**		**(**)**		**(***)**	**B**	**N**	**M**
-		**!**	**( )**					**?**	**,**	**.**

(*) klávesa X je červená a používala se místo mezery
(**) klávesa označena Ziffern u. Zeichen
Zwischenraum
(***) klávesa označena Buchstaben
Zwischenraum

Pod klávesnicí byl třípolohový přepínač s polohami

Klarschrift deschiffrieren chiffrieren

Výstup textu byl tiskem typů na papírový pás na válci. Tiskla se pouze malá písmena mezinárodní abecedy a znaky druhého registru. Na typovém kolečku byla na vnějším kruhu v malých písmenech srovnaná mezinárodní abeceda ve směru pohybu hodinových ručiček a pod ní na vnitřním kruhu odpovídající typy druhého registru klávesnice. Při vodorovném zobrazení obsahovalo tedy typové kolečko následující znaky:

a b c d e f g h i j k l m n o p q r s t u v w x y z
% ? ! , 3 / = + 8 8 1 ; . , 9 0 1 4 § 5 7 ( ) 2 - : 6

Šifrovací stroj STANDARD měl 4 disky všechny periody 26, které měly jednotlivé polohy označeny velkými písmeny srovnané mezinárodní abecedy

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z .

Kromě výchozí polohy kol na hřídeli se ještě na stejném hřídeli nastavovaly polohy ozubených „vaček“. Tyto ozubené „vačky“ byly čtyři o 4 různých periodách 17, 15, 13 a 11. Pro nastavení poloh byly „vačky“ označeny takto:

1. perioda 17 A B C D E F G H J K L M N O P Q R
2. perioda 15 A B C D E F G H J K L M N O P
3. perioda 13 A B C D E F G H J K L M N
4. perioda 11 A B C D E F G H J K L

Čili u stroje STANDARD se nastavovala výchozí poloha disků (každá do jedné z 26 možných poloh) a výchozí poloha ozubených „vaček“ (každá do jedné z možných poloh podle délky její periody). Šifrátor měl dále pětimístné počítadlo znaků a pohon kol byl realizován elektrickým motorem připojitelným na zdroj střídavého napětí 110V, který byl označen Gleichstrom 110V. V roce 1982 byl k dispozici 1 kus stroje STANDARD, který však byl již v roce 1985 zrezivělý a vyžadoval celkovou repasáž.

V této stati byly popsány trofejní šifrovací stroje, které byly k dispozici v československé šifrové službě v poválečném období a které byly až do první poloviny 50. let 20. století prakticky využívány zejména v československé armádě. Problematika šifrovacích strojů, které pracovaly na principu Borise Hagelina, byly k dispozici v jednotlivých kusech a v československé šifrové službě nebyly nijak prakticky využívány (kromě zásadní inspirace při konstrukci československých šifrátorů třídy MAGDA), bude laskavému čtenáři předložena v dalším pokračování. Stejně tak jako problematika malebného mechanického šifrovacího stroje z roku 1926 s názvem KRYHA CHIFFRIERMASCHINE Standard Modell, který byl svým vynálezcem a konstruktérem, ukrajinským inženýrem žijícím v Německu, Alexandrem von Kryhou opatřen malebným označením „Patentiert in allen Kulturstaaten“.

Následující doprovodné obrázky tří a čtyřdiskových šifrovacích strojů ENIGMA nafotil P.Vondruška. Jedná se o zařízení, která byla vystavena na konferenci EUROCRYPT 2003.

D. Nové knihy

Biometrie a identita člověka

Podtitul: **ve forenzních a komerčních aplikacích**
Autor: Roman Rak, Václav Matyáš, Zdeněk Říha a kolektiv
Formát: 16×24 cm, 664 stran
Datum vydání: 11.07.2008
Katalogové číslo: 7242
ISBN: 978-80-247-2365-5

Anotace

Dostává se vám do rukou zcela jedinečná a neopakovatelná kniha, jejíž mezinárodní kolektiv autorů je smíšený z řad vysokoškolských pedagogů Policejní akademie ČR, Masarykovy univerzity i dalších vysokých škol ČR, Británie, Německa a Švýcarska, ale i soudních znalců a expertů Kriminalistického ústavu. Už toto je důkaz jedinečnosti a neopakovatelnosti této knihy, jež odpovídá pohledu autorů na danou problematiku. V devatenácti kapitolách jsou detailně rozebrány jednotlivé biometrické metody a aplikace (bertilonáž, otisky prstů a dlaní, geometrie tvaru ruky, krevního řečiště dlaně i hřbetu ruky, DNA, rozpoznávání osoby dle její tváře, tvaru ucha, hlasu, oční duhovky i sítnice, podpisu i psaní na počítačové klávesnici). A to vždy ze dvou základních pohledů: ze zorného úhlu forenzních věd, tj. využití biometrických principů a aplikací pro potřeby orgánů činných v trestním řízení (policisté, kriminalisté, vyšetřovatelé, soudní znalci, obhájci a soudci) a z pohledu komerčně využitelných aplik ací pro privátní ochranu osob a majetku. Pozornost a tedy i rozsah kapitol odpovídá současnému podílu zastoupení biometrických metod na světovém trhu.
http://www.grada.cz/katalog/kniha/biometrie-a-identita-cloveka/

Autentizace elektronických transakcí a autorizace dat i uživatelů

Autor: **MATYÁŠ Václav (Vašek) - KRHOVJÁK Jan a kol.**
Rok vydání: 2008
ISBN: 9788021045569
Počet stran: 128
Vazba: brožovaná
Vydavatelství: Masarykova univerzita

Anotace

Kniha ojedinělá v pojetí i ve způsobu zpracování. Mimořádně pokrývá kompletně základní problematiku metod a technologií používaných při autentizaci a autorizaci elektronických platebních transakcích. Jednotlivé kapitoly nabízí široký záběr od výkladu základních pojmů a koncepcí, až po některá pokročilá témata řešení autentizace a autorizace. Snahou autorů je, aby publikace dokázala nabídnout zajímavé informace pro všechny kategorie čtenářů, aby pomohla s orientací těm, kteří se s danou tématikou potkávají poprvé, stejně jako zkušeným profesionálům, kterým pomůže rozšířit si jejich obzor. V první části obsahuje úvod do problematiky, výklad klíčových pojmů, souvislostí atd. Druhá část je zaměřena na trendy vývoje jednotlivých autentizačních metod a jejich známé bezpečnostní nedostatky; třetí část se věnuje současným (běžně používaným) řešením autorizace finančních transakcí. Závěrečná část diskutuje možnosti zvýšení bezpečnosti autentizačních i autorizačních postupů.

E. O čem jsme psali v létě 2000 - 2007

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

Crypto-World 78/2006

Crypto-World 78/2007

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 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	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	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/