Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 14, číslo 9-10/2012 **1. říjen**

9-10/2012

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info/
(1306 registrovaných odběratelů)

Obsah :

Příloha: neoglyfy.pdf , ukázka ze sešitu Batěk A. S.: Neoglyfy I., str. 4 – str. 13
(http://crypto-world.info/casop14/neoglyfy.pdf)

A. Pointerová šifra a nízkoriziková náhrada AES

RNDr. Vlastimil Klíma, nezávislý kryptolog – konzultant a KNZ s.r.o.,
v.klima@volny.cz

Abstrakt. V tomto článku navrhujeme koncept Pointerové blokové šifry a jako jejího reprezentanta Nízkorizikovou blokovou šifru, která by měla být 3x rychlejší než AES. Jedná se zatím o studijní koncept, určený k výzkumu jeho vlastností.

Nízkoriziková kryptografie (Low Risc Cryptography) je pojem, který jsme si vymysleli a zavedli v CW 5-6/2012. Řekli jsme tam, že *Nízkoriziková kryptografie* je kryptografie pro prostředí, v kterém útočník nemá tolik možností, jako *obecný útočník* v *obecné kryptografii*.

Také jsme definovali podmínky pro jednu variantu *Nízkorizikové blokové šifry*, z vnějšího hlediska kompatibilní s AES, mající stejné vstupní a výstupní parametry. Pro jednoduchost jsme zvolili tyto podmínky takto:

- Délka bloku 128 bitů
- Délka klíče 128 bitů, klíč je definován jako 128bitový (ale není nutné, aby byly všechny bity klíče „platné“ nebo „vyplněné“, a to proto, že:)
- Požadovaná bezpečnost u Nízkorizikové kryptografie může být pouze 2^80

Tyto podmínky jsou ještě dostatečně obecné, nyní se soustředíme na konkrétní variantu Nízkorizikové blokové šifry LR-AES pro specifičtější použití:

- LR-AES je určena do prostředí 64bitových procesorů, zejména pro stolní počítače a notebooky
- Jedním klíčem je možné zašifrovat pouze jeden Pentabyte (1000 TB) dat, tj. 2^50 B / 16B = 2^46 bloků dat
- Útočník může znát nebo volit dohromady maximálně 2^46 bloků dat
- (Zvažujeme ještě: Útočník má k dispozici pouze tolik operací na jeho technice, které odpovídají 2^64 průběhům blokové šifry (přitom je lhostejné, zda se mění otevřený text nebo klíč nebo obojí). Toto zeslabení bezpečnosti z 2^80 na 2^64 v reálné „průmyslové“ bezpečnosti je stále pro útočníky dostatečně odrazující).
- LR-AES musí být 2x až 3x rychlejší než AES

Smyslem článku je podnítit diskusi k základní myšlence "Pointerové šifry" (skládá se de facto jen z pointerů do velkých tabulek), která je jasná, ale možná naleznete její zlepšení nebo nové nápady na LR-AES.

Vycházíme z toho, že u naprosté většiny symetrických blokových šifer jejich bezpečnost zajišťuje řada nelineárních substitučních boxů různých rozměrů. Ponejvíce jsou to rozměry 4x4 a 8x8 bitů, ale vyskytují se i S-boxy o rozměru 7x7, 5x5, 3x3 a výjimečně i 9x9 bitů. V každé SW realizaci pak musí dojít k průchodu dat přes tyto boxy, což se projeví tak, že ze 128 bitového vstupu se musí nějakými vhodnými instrukcemi "vyzobnout" postupně jeden každý bajt (3bit, 4bit, 5bit, ...) a projít s ním přes substituční tabulku. Ukázalo se, že tyto operace „vyzobnutí“ a „průchod přes tabulku“ jsou nejnáročnějšími operacemi většiny blokových šifer. Proto například u AES i DES byly navrženy triky, jak docílit zrychlení těchto operací tak, že se tyto tabulkové operace různými způsoby sdružují s využitím velkých tabulek typu 8x32. Kolik tabulkových operací potřebujeme pro AES? V každé z 10 rund (pro 128bitový klíč), je nezbytné provést minimálně jednu tabulkovou operaci na jeden bajt vstupu, tj. máme 160 tabulkových operací na celou AES. Rádi bychom aby pointerový koncept šifry umožnil spotřebovat pouze 48 tabulkových operací. Pointerová šifra by měla být tedy cca 160/48 = 3.3 krát rychlejší než AES.

Je to kryptograficky velice na hraně, protože AES zajišťuje plnou difúzi (aby každý bit vstupu ovlivňoval každý bit výstupu) až po 4 rundách, na což spotřebuje 4*16 = 64 tabulkových operací. 64 tabulkových operací je tedy absolutní minimum u AES. Docílit dostatečné kvality do 48 tabulkových operací je proto skutečně mimořádnou výzvou. Pokud by se to nepodařilo, nebylo by vhodnější použít rovnou 4 rundy AES? To by dalo algoritmus 10/4 = 2.5 krát rychlejší než AES. Tady má pointerová šifra malou výhodu, neboť Feistelova struktura u Pointerové šifry a SP-síť u AES mají jiné vlastnosti, přitom u AES bude existovat algebraický útok, zatímco u Pointerové šifry nikoli. Nevýhodou je novost konstrukce.

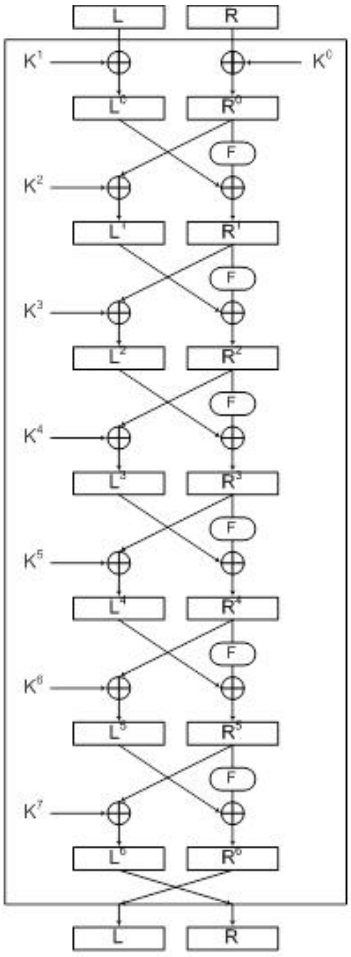
Princip Pointerové šifry

- využití tabulek typu **8x64 bitů**
- konstrukce nelineární transformace F typu 64x64 bitů
- využití principu Feistelova schématu

- stanovení minimálního počtu rund (konkrétně 6, méně než 6 rund není možné z důvodu neúplné statistické závislosti šifrového textu na klíči a na otevřeném textu)

Blokové schéma Pointerové šifry v krocích

1. Příprava rundovních klíčů – ze 128bitového klíče se připraví 8 64bitových rundovních klíčů
2. Zašumění (whitenning) – nejprve je na 64bitovou levou (L) a 64bitovou pravou (R) polovinu otevřeného textu přixorován rundovní klíč: $(L^0, R^0) = (L \oplus K^1, R \oplus K^0)$
3. Šest shodných rund i = 0, ..., 5, lišících se pouze v hodnotě rundovního klíče, který se používá jeden v každé rundě, r: $\{0,1\}^{64} \times \{0,1\}^{64} \rightarrow \{0,1\}^{64} \times \{0,1\}^{64}$: $(L^i, R^i) \rightarrow (L^{i+1}, R^{i+1}) = (R^i \oplus K^{i+2}, F(R^i \oplus L^i)$
4. Závěrečné prohození levé a pravé strany (tato operace může být ve finální verzi vyřazena)



Obr.: Blokové schéma LR-AES

Zatím v konstrukci Pointerové šifry nevidíme nic moc nového, kromě přesunutí xorování rundovního klíče, typicky realizované ve funkci F, na levou stranu. Důvod je prostý, moderní 64bitové procesory obvykle využívají paralelní instrukce, a když je zaneprázdněna pravá strana prací na funkci F, *může* na levé straně proběhnout operace xor s rundovním klíčem takříkajíc zadarmo. Pokud ano, získali jsme, pokud ne, nic jsme neztratili. Z kryptografického hlediska můžeme s rundovním klíčem ve schématu sjet do další rundy, kde bude součástí funkce F, tedy je to klasická definice Feistelovy šifry. Podstatné je, že přixorování rundovních klíčů je navrženo tak, aby na počátku i na závěr blokové šifry konci došlo k zašumění vstupu a výstupu rundovními klíči (na konci to zajišťují rundovní klíče K^6 a K^7).

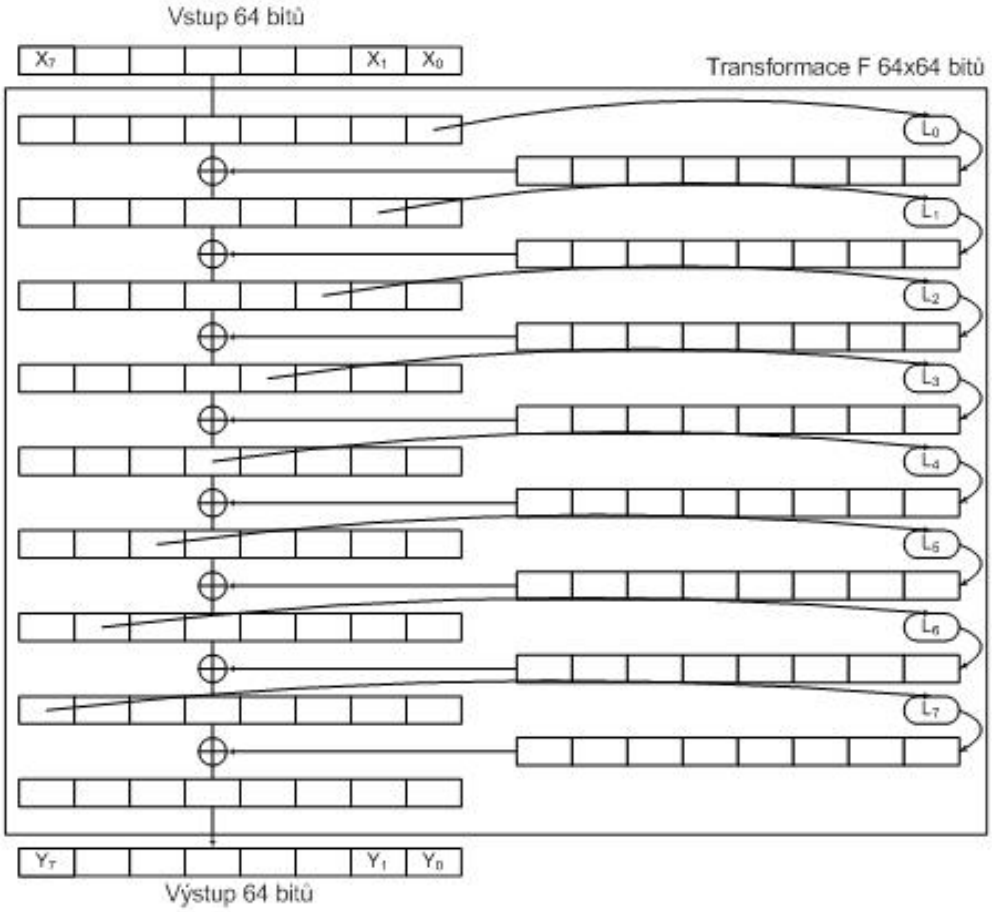
Nelineární transformace F

Označme 64bitový vstup do funkce F jako řetězec 64 bitů X, jehož jednotlivé bajty očíslujeme takto: $X = X_0 \,||\, X_1 \,||\, ... \,||\, X_7$. Například když X = „abcdefgh“, pak X_0 = 0x61 („a“), X_1 = 0x62 („b“), atd. Podobně označíme 64bitový výstup F(X) = Y a jeho bajty $Y = Y_0 \,||\, Y_1 \,||\, ... \,||\, Y_7$. Dále budeme používat osm pevných substitučních tabulek (large S-box) typu 8x64, které označíme L_0, L_1,..., L_7. Potom celá transformace F je definována pseudokódem jako pouhých osm přičtení tabulkových hodnot následovně.

```
for (i = 0 to 7)
X = X ⊕ Li(Xi)
```

Obr.: Transformace F

Transformaci F : $\{0,1\}^{64} \rightarrow \{0,1\}^{64}$: $\{X_7, X_6, ..., X_0\} \rightarrow \{Y_7, Y_6, ..., Y_0\}$ znázorňuje obrázek.



Obr.: Transformace F

Protože L_i (i = 0, ..., 7) jsou tabulky typu 8x64 bitů, jednotlivé bajty výstupu $L_i(x) = (L_{i7}(x), L_{i6}(x), ..., L_{i0}(x))$ jsou nám důvěrně známé S-boxy typu 8x8 bitů. Máme tak 64 S-boxů L_{ij},i = 0, ..., 7, j = 0, ...,7.
Zastavíme se nyní u prvního kroku transformace F. Vstup (X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0) se transformuje na výstup
($X_7 \oplus L_{07}(X_0)$, $X_6 \oplus L_{06}(X_0)$, $X_5 \oplus L_{05}(X_0)$, $X_4 \oplus L_{04}(X_0)$, $X_3 \oplus L_{03}(X_0)$, $X_2 \oplus L_{02}(X_0)$, $X_1 \oplus L_{01}(X_0)$, $X_0 \oplus L_{00}(X_0)$).

Základním požadavkem pro transformaci F je, aby byla bijekcí. Pokud by nebyla, jednalo by se o nebalancovanou funkci F, která má větší náchylnost na útok diferenciální a lineární kryptoanalýzou (rozbor této možnosti stojí velice za pozornost, ale teď ho přeskočíme). Volíme proto jednotlivé kroky funkce F jako bijektivní zobrazení.

Proto i první zobrazení prvního bajtu $X_0 \rightarrow X_0 \oplus L_{00}(X_0)$ musí být nějakým bijektivním substitučním boxem typu 8x8 (označme ho S_{00}). Takže to obrátíme a zvolíme nejprve nějaký vhodný bijektivní substituční box S_{00} typu 8x8 a poté definujeme $L_{00}(X_0) = X_0 \oplus S_{00}(X_0)$ pro každé X_0. Tím je zajištěno, že bajt X_0 sám projde jednoduchým tradičním S-boxem typu 8x8!

Jako bonus navíc prostřednictvím $L_{07}(X_0)$, $L_{06}(X_0)$, ..., $L_{01}(X_0)$ ovlivní všechny zbývající bajty X_7, X_6, ..., X_1. Ostatní složky $L_{07}(x)$, $L_{06}(x)$, ..., $L_{01}(x)$ tabulky L_0 definujeme přímo jako nějaké vhodné bijektivní S-boxy $S_{07}(x)$, $S_{06}(x)$, ..., $S_{01}(x)$ typu 8x8. Podobně v dalších krocích pro i = 1, ..., 7 definujeme vždy i-tou složku tabulky L_i jako $L_{ii}(x) = x \oplus S_{ii}(x)$ pro každé x, kde S_{ii} je nějaký bijektivní S-box typu 8x8 a ostatní složky L_i definujeme opět jako nějaké bijektivní S-boxy $S_{i7}(x)$, $S_{i6}(x)$, ..., $S_{i1}(x)$ typu 8x8 .

K definici všech tabulek L_{ij} tak potřebujeme 64 S-boxů S_{ij} typu 8x8. Ideální by bylo, aby všechny tyto S-boxy byly vzájemně nezávislé a nejlépe náhodně vybrané z množiny všech bijektivních S-boxů.

Každé uhnutí z tohoto pravidla nahrává kryptoanalýze avšak snižuje náročnost na paměť.

Tvorba rundovních klíčů

Tvorba rundovních klíčů musí být velmi jednoduchá a bezkonkurenčně jednodušší než u AES. Také musí být velmi jednoduché z chodu a bez přípravy rundovních klíčů začít dešifrovat. To u AES bohužel nejde, neboť rundovní klíče, které vznikají při zašifrování naposled, se nedají z klíče okamžitě vypočítat. To je další výhoda Pointerové šifry.

Nechť K je 128 bitový klíč LR-AES. Rundovní klíče definujeme takto:

$K_0 = K$,

$K_1 = K \oplus Const_1$,

$K_2 = K \oplus Const_2$,

$K_3 = K \oplus Const_3$,

$K_4 = K \oplus Const_4$,

$K_5 = K \oplus Const_5$,

$K_6 = K \oplus Const_6$,

$K_7 = K$,

kde $Const_1$, ..., $Const_6$ jsou vhodně zvolené navzájem různé konstanty. Konkrétně nechť například

$Const_1$ = 0x0000000000000001,

$Const_2$ = 0x0000000000000002,

$Const_3$ = 0x0000000000000003,

$Const_4$ = 0x0000000000000004,

$Const_5$ = 0x0000000000000005,

$Const_6$ = 0x0000000000000006.

Z kryptologického hlediska plní konstanty roli odlišovače jednotlivých rundovních funkcí. Pokud se podíváme na obrázek blokové šifry, snadno nahlédneme, že například v rundovním klíči K_1 můžeme ponechat hodnotu K a konstantu $Const_1$ můžeme přesunout do další rundy za funkci F. Čili pokud modifikujeme funkci F v

následující rundě tak, že místo původní funkce F tam bude $F \oplus Const_1$, pak máme totožné schéma. Změnilo se to, že jsou stejné rundovní klíče (všechny rovny K), ale jednotlivé rundovní funkce jsou nyní rozdílné (liší se od původní stejné funkce F o různé rundovní konstanty). Tohoto triku se může využít k malému urychlení tím, že operace $F \oplus Const$ se včlení vždy do poslední tabulky L_7 tak, že na tabulku L_7 se přixoruje daná rundovní konstanta Const. Všechny tabulky budou tedy ve všech rundách stejné, kromě L_{7i}, které budou v každé rundě jiné. Takto jednoduché schéma rundovních klíčů evokuje různé útoky, a to je také zamýšlenou výzvou pro kryptoanalytiky.

Zašifrování a dešifrování

Dešifrování probíhá podle stejného schématu jako zašifrování, pouze pořadí klíčů se obrátí. Tj. při zašifrování se použijí jako rundovní klíče K_0, ..., K_7 výše definované, a při zašifrování to budou klíče

$K_0 = K$,
$K_1 = K \oplus Const_6$,
$K_2 = K \oplus Const_5$,
$K_3 = K \oplus Const_4$,
$K_4 = K \oplus Const_3$,
$K_5 = K \oplus Const_2$,
$K_6 = K \oplus Const_1$,
$K_7 = K$.

Teď už nezbývá nic jiného, než Vám popřát hodně úspěchů v útocích na tuto výzvu. Copak se nenajde útok na šifru, která používá jen 48 tabulkových operací a primitivní přípravu klíčů?

Pokud nepřijdete na žádný útok, čeká Vás příště varianta Pointerové šifry, která je ještě rychlejší a troufalejší, ovšem pokud nepřijdete s takovým návrhem sami...

B. Kryptografické zabezpečení prodeje lihovin

RNDr. Radomír Palovský, CSc., fakulta informatiky VŠE, palovsky@vse.cz

V současné napjaté atmosféře kolem nelegálního prodeje alkoholu, přesněji lihovin, jsou hledány možnosti budoucích schémat distribuce, které nelegálním cestám zhorší nebo až znemožní průchodnost. Tímto článkem bych rád demonstroval koncept ochrany legální výroby s využitím kryptografie. Techniky kryptografie jsou v prvé řadě veřejností chápány jako techniky pro ochranu informací v digitálních mediích, a z prvního pohledu nemusí být jasné, jak by se takovou technikou mohla chránit láhev alkoholu. Nicméně je dobré si uvědomit známou poučku z počítačové bezpečnosti: Bezpečnost je ochrana informací, nejen dat. A informace se neztrácí, převedeme-li data na jiné médium, třeba vytištěním. Jako vhodný kód pro převod digitálních dat z počítače na tištěnou plochu a nazpět se jeví QR kódy [1], které, mají vysokou efektivitu bitů na plochu, čtyřstupňovou škálu úrovně redundance pro spolehlivé přečtení kódu při částečně zničené předloze, a mnohastupňovou škálu velikosti, přičemž v nejmenším případě je to záznam 5 dekadických cifer a v největším případě až 23,648 bitů (při nejnižší úrovni redundance). Použitím QR kódu se z prodávané lahve stane (s výjimkou obsahu) digitální medium.

Nyní k vlastnímu návrhu, konceptu elementů a funkcí, které zvýší ochranu spotřebitele před padělaným alkoholem se zapojením zabezpečení pomocí kryptografických prostředků.

Bezpečnostní cíle, které tento koncept má naplnit, jsou:

1. Jednoznačné, nezpochybnitelné a neodmítnutelné svázaní konkrétního výrobce, konkrétní láhve (resp. balení), konkrétního kolku nalepeného na právě této lahvi a konkrétního času plnění lahve.
2. Informace uvedené v bodě 1. nebude možné zfalšovat.
3. Informace uvedené v bodě 1. bude možné verifikovat každým, kdo disponuje jednoduchým čtecím zařízením. Čtecím zařízením by byla jednoduchá aplikace do naprosté většiny současných mobilních telefonů s fotoaparátem.

Subjekty, které v průběhu procesu budou mezi sebou interagovat, jsou:

1. Státní správa – vydává licence na výrobu alkoholu a vydává potřebné doklady pro Certifikační autoritu, že subjekt je oprávněn žádat o certifikát pro digitální podpis pro podpisování lihovin.
2. Certifikační autorita (CA) – vydává certifikáty pro digitální podpis pro podpis lihovin pouze oprávněným subjektům, a časová razítka pro jednotlivá balení (lahve).

3. Státní tiskárna cenin – vydává kolky (kontrolní pásky). Ty jsou na rozdíl od současných kolků opatřeny oblastí pro strojové čtení, která obsahuje vytištěnou strojově čitelnou hodnotu totožnou s vytištěnou hodnotou standardně čitelnou člověkem. Tato oblast by byla opatřena bezpečnostními prvky ceniny v papíru, aby nebylo možno tuto strojově čitelnou oblast zaměnit za jinou. Jako pravděpodobně nejlepší se jeví použít kód „micro QR code“ ve verzi M3 v nejvyšší úrovni redundance.

4. Likérka – vlastní soukromé kódy svého digitálního podpisu (vydané certifikáty CA na své kódy) a podepisuje každé balení, které vyrobí. Na rozdíl od současnosti musí mít likérka vyrobeny etikety (zadní etikety) s prázdným bílým nepotištěným čtvercovým polem specifikovaných rozměrů. Volné pole je určené pro tisk QR kódu, který verifikuje vyrobenou lahev.

5. Kontrolor/verifikátor – má certifikáty CA likérek, zařízení schopné číst a převést QR kódy (většina mobilů s fotoaparátem a volně dostupným softwarem na čtení QR kódů) a verifikační aplikaci, kterou bude nutno vytvořit.

Zjednodušené schéma konceptu.

1. CA vydá digitální podpis pro podepisování lihovin pouze takovému subjektu, který se prokáže potřebnými oprávněními státní správy pro tuto činnost.

2. Státní tiskárna cenin vydá kolky, jednoznačné, číslované a se strojově čitelným polem, a dodá je likérce.

3. Likérka přečte strojovým způsobem číslo kolku. Požádá CA o kvalifikované časové razítko k tomuto číslu kolku. Vytvoří QR kód, který bude obsahovat identifikaci likérky, identifikaci šarže alkoholu, číslo láhve, popřípadě vymezené další údaje identifikující produkt či proces, dále získané časové razítko a digitální podpis všech uvedených údajů tedy: čísla kolku, identifikaci likérky, čísla šarže, láhve, další údajů a časového razítka. Natiskne QR kód na etiketu lahev opatřené odpovídajícím kolkem.

4. Verifikace pravosti – QR kódy umí v současnosti přečíst v podstatě každý mobil s digitálním fotoaparátem. Aplikaci, která by provedla vyhodnocení, by bylo nutné vytvořit, ale naprogramovaní takové aplikace do mobilu není příliš náročné, prvotní odhad nepřesahuje 100 člověkohodin práce; veškeré potřebné kryptografické funkce (i funkce čtení QR kódu) jsou součástí knihoven, a je pouze nutné je správně složit dohromady. Před provedením verifikace je nutné do mobilu nahrát certifikáty digitálních podpisů akreditovaných likérek. Ty očekávám, že by byly k dispozici zdarma na stránkách likérek, stránkách certifikační autority, stránkách ministerstva zemědělství, popřípadě jiného státního orgánu. Verifikace by probíhala tak, že kontrolor vyfotografuje strojově čitelnou část kolku (micro QR kód) a hlavní QR kód na lahvi, mobil převede QR kódy na údaje a následně aplikace vyhodnotí a verifikuje platnost digitálního podpisu.

(ilustrační obrázek doplněn redakcí)

Výhody popsaného konceptu:

1. Jednoduchá a levná verifikace. Proces verifikace umožní verifikovat pravost lahve/balení nejen orgánům státní správy, ale i konečným spotřebitelům. Aplikaci na verifikaci by stát mohl/měl poskytnout volně k dispozici k použití občanům. Pak by i každý občan před nákupem mohl verifikovat pravost lahve pouhým vyfotografováním dvou obrázků na lahvi.

2. Odolnost. Útočníkům/padělatelům by nestačilo ukrást/získat/padělat kolky, k jejich úspěšnému použití by museli získat soukromé kódy k digitálnímu podpisu pro konkrétní likérku, a navíc získat ještě potřebná časová razítka CA pro provedení validního digitálního podpisu. Dokonce při krádeži kolků a ještě navíc krádeži soukromých klíčů digitálního podpisu by útočníci neměli vyhráno, protože by potřebovali ještě získávat časová razítka, a pokud by se jim i podařilo získávat časová razítka k ukradeným kolkům, tak časové razítko by jednoznačně identifikovalo použití klíčů po zneplatnění soukromých klíčů oprávněné likérky, a tedy falzifikát (za předpokladu, že likérka by krádež odhalila a nahlásila bezpečnostní incident CA). Podobný účinek by měla i periodická výměna klíčů likérky, staré klíče, i když ukradené a neodhalené, by nemohly být použity.

3. Za předpokladu centralizace vydávání časových razítek do jedné CA bude mít státní správa průběžný přehled o vyrobených baleních jednotlivých likérek.

Náklady systému:

- Náklady státu – náklady na výrobu a tisk nových kolků, náklady na vytvoření verifikační aplikace, případně dovybavení kontrolních orgánů potřebnými telefony.

- Náklady likérek:

    1. Fixní náklady se týkají hlavně pořízení technického zařízení pro zákaznický tisk na jednotlivé lahve (balení), a zařízení na synchronizaci. Tedy zabezpečení, že konkrétní kolek konkrétního čísla a konkrétní nálepka se zákaznickým QR kódem k příslušnému kolku budou umístěny na jednu a tutéž láhev. Další fixní náklady se týkají pořízení příslušného certifikátu digitálního podpisu.

    2. Provozní náklady se týkají položek:

        1. Zákaznický tisk QR kódu. V případě použití kvalitních zařízení je jistě možné se dostat výrazně pod hodnoty 0,10 Kč na nálepku, protože současné kvalitní tiskové zařízení je schopné tisknout v hodnotách 0,12 Kč na stránku A4, a plocha QR kódu bude výrazně nižší.

        2. Náklady na časová razítka, které se v současnosti pohybují u 0,50 Kč za razítko u velkých objemů. Patrně by náklady za razítka bylo možné snížit centralizováním, tedy situací, kdy by stát vybral ve výběrovém řízení jedinou CA oprávněnou obsluhovat digitální podpisy likérek, a dohodl v rámci řízení výhodnou cenu za časová razítka. CA by tím měla garantované velké objemy.

        3. Náklady na kolky (tyto náklady již likérky mají.)

Proces se zabezpečením synchronizace kolku a etikety by mohl patřit k obtížnějším prvkům pro realizaci u likérky. Je dobré zdůraznit, že kryptografická síla konceptu je dosti založena na tom, že informace, které digitální podpis likérky podepisuje, se nikde nevyskytují na jednom místě, část je na kolku a část na etiketě. Bez kolku nejdou informace z etikety verifikovat, a ani z informací z etikety nejde hledat, jaké číslo na kolku má být. Na druhou stranu tato kryptografická bezpečnostní výhoda neposkytuje likérce žádné vodítko v procesu synchronizace, který kolek patří ke které etiketě, a rozpoznání případného „předbíhání“ nebo „zpožďování“ kolků proti etiketám při umisťování na lahve. Pokud by se likérka pokusila získat vodítko pro synchronizaci tím, že by někam na etiketu si „tajně“ tiskla číslo kolku, významně tím oslabí bezpečnost konceptu. V tom případě obsahuje etiketa všechny informace a případný útočník by mohl lahev znovu naplnit, opatřit pravým kolkem a ten upravit pouze ve strojově čitelné části tak, aby číslo v micro QR kódu kolku odpovídalo tomu, které je na etiketě. Odhalení by pak záleželo čistě na tom, jestli si verifikátor všimne, že kolek je pozměněn ve strojově čitelné části nebo že číslo strojově přečtené z kolku neodpovídá číslu uvedenému na kolku a čitelném člověkem.

Nicméně je možné koncept modifikovat tak, aby synchronizační čísla si likérka vytisknout mohla. Tato čísla by mohla být např. 4 ciferná čísla, která se budou cyklicky protáčet a likérka si je vytiskne stejně na oba subjekty tedy na kolek (do dalšího připraveného místa) a na etiketu. Tato čísla neponesou žádnou kryptograficky důležitou informaci, umožní likérce synchronizaci a na druhou stranu také nijak bezpečnost nenaruší.

Problémy se synchronizací by mohly mít jak malé likérky, které etikety lepí ručně, tak i velké v případě, jak se občas stane, chybného zpracování etiket automatickým zařízením a slepením dvou etiket a nalepením jich obou na jedinou lahev.

Slabiny:

1. Okopírování celé legální lahve včetně QR kódu a kolku s jeho QR kódem vytvoří novou nerozlišitelnou legální láhev. Nicméně takovému celému okopírování neodolá nic, co není součástí materiálu lahve. V případě navrhované kryptografické ochrany by ochranou proti kopírování celé lahve musely být bezpečností prvky kolku. Je vhodné poznamenat, že případná falzifikující kopie by musela být se skutečným padělkem původního kolku, protože jiný ukradený nebo jinak získaný kolek by byl odhalen verifikačním algoritmem. A i takováto situace by mohla být indikována v hromadném případě tím, že kontrolor vidí opakovaně stejný výsledek verifikačního procesu.

2. Obtížnost hromadné verifikace. Vzhledem k tomu, že verifikace se provádí fotografií kolku a lahve, je nemožné přímo verifikovat obsahy uzavřených větších balení. Nicméně tento koncept je možné přímo rozšířit i na větší balení. Pak by bylo vhodné mít přesně specifikované polohy strojových polí kolků a verifikačního QR kódu na balení, aby bylo možné použít strojové automatické čtečky.

Body k řešení:

1. Omezená velikost vršků lahve a QR kódy tištěné na válcový povrch a snímané při verifikaci plošnou fotografií vytváří otázky, jaký je optimální poměr mezi množstvím informace a praktickou čitelností.

2. Pro vršky lahve to znamená: jaká maximální velikost micro QR je ještě použitelná?

3. Pro hlavní verifikační QR kódy: jaká plocha je přijatelná pro rezervaci pro QR kód a jaká mapa je ještě vhodná, a kolik informace pro spolehlivé fungování potřebujeme.

4. Souvisí to s otázkou, jaké informace bude třeba ukládat do QR kódu a jaký algoritmus použít k digitálnímu podpisu, aby výsledný QR kód byl spolehlivě čitelný a dostatečně bezpečný.

   Nicméně i přes uvedené některé nevyjasněné otázky, které jsou spíše hledáním optimálních hodnot a ne bezpečnostní slabinou, nabízí koncept dostatečnou bezpečnost, odolnost a spolehlivost.

Citace:

[1] Denso Wave Incorporaded: QR code features [online]. 2010 [cit. 2012-09-26] Dostupné z WWW: http://www.qrcode.com/en/qrfeature.html

C. Kryptologické perličky 2

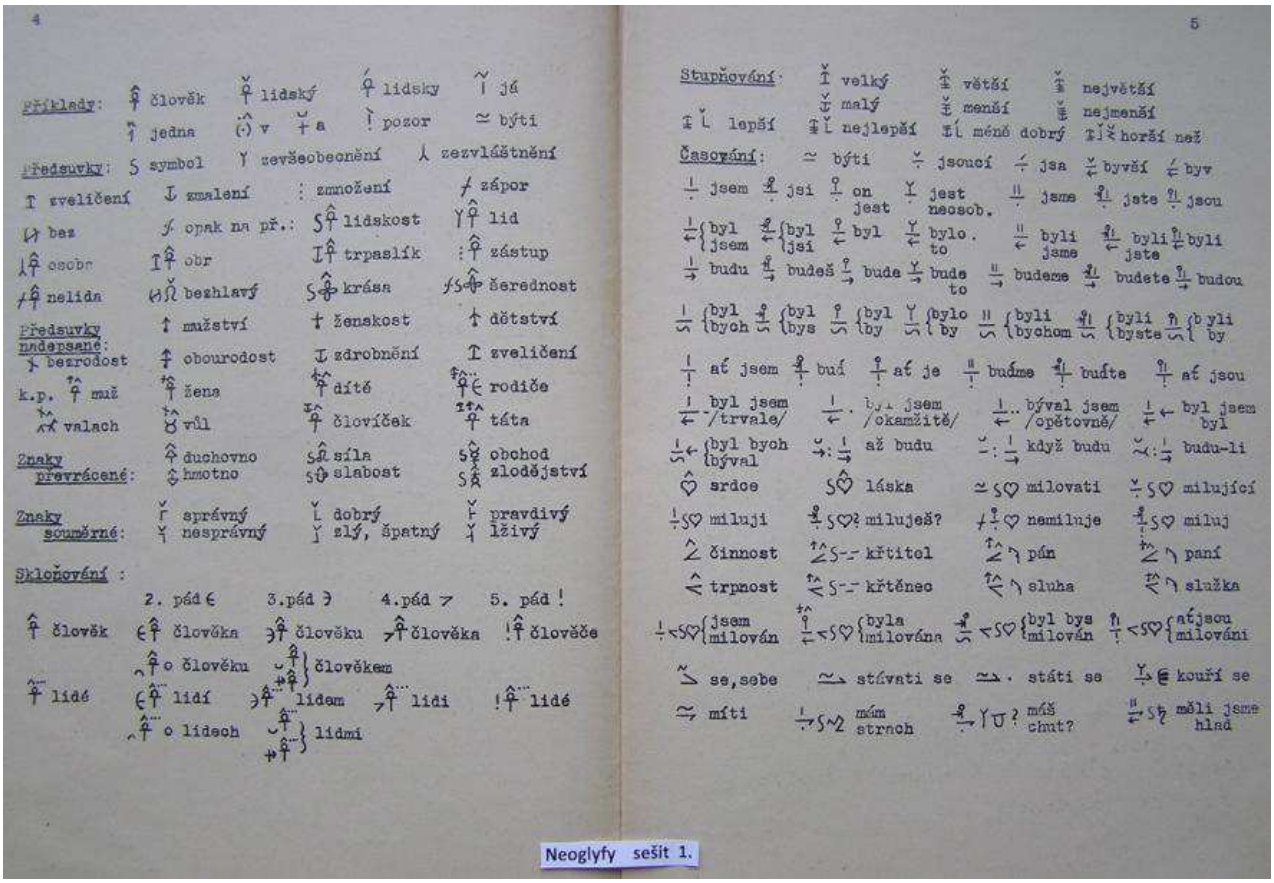
Mgr. Karel Šklíba (karel.skliba@cryptoworld.info)

V tomto příspěvku bych si dovolil přiblížit systém světového písma neoglyfů PhDr. Alexandra Sommera Batěka, jehož osobnost byla stručně charakterizována v článku minulém. Připomeňme ještě, že graduovaný chemik (1899) doktor Sommer Batěk byl významným bojovníkem proti démonům alkoholu, tabáku a prostituce, vegetariánem, aktivistou skautu, Armády spásy, Ligy lesní moudrosti, Sokola a organizace YMCA, otužilcem, volnomyšlenkářem, pacifistou, propagátorem theosofie, okultismu a spiritismu i spisovatelem scifi literatury. To není zdaleka vše. Některým jeho aktivitám může konkurovat jen Jára Cimrman. Pokusil se o vynález ozometru (přístroje na měření vůní), zavedl pěstování rebarbory na Plzeňsko, konal úspěšné pokusy s rychlením růstu ředkvičky elektrickým proudem (bohužel rostly zejména listy a kořenová část zůstávala zakrslá), vynalezl vodu proti pocení nohou (ta se neujala), za války zreformoval systém evidence osobního majetku válečných zajatců v táboře ve Feldbachu, vytvořil pratelný poklop na potraviny, učil Angličany rozlišovat Čechy a Maďarsko, propagoval správné dýchání a žvýkání, vytvořil formologii (vědu o tvoření těla živého), propagoval kočovné vyučování a sám přednášel slovenským pasákům ovcí esperanto, dělníkům v Podbrezové harmonickou gymnastiku, cikánům na taneční zábavě přednášel o správném dýchání (tzv. fletcherování) a vojákům hrál loutkové divadlo o pohlavní zdrženlivosti. Tento výčet asi stačí, ale věřte či nevěřte, není ani zdaleka úplný (viz podrobněji Batěk Sommer A.: Jak jsem padesát let žil a pracoval. B. Kočí, Praha 1925). Nelze ještě nezmínit vynález tzv. trháku, což byla kniha, ve které měly listy u hřbetu perforaci, aby je bylo možné snadno vytrhávat a lepit si je například na nábytek. Vladimír Borecký ve stati „Dvojí zdroj absurdní komiky“ uvádí při vymezení tzv. obzvláštníků české provenience Sommera Batěka v tematické skupině medicína a hygiena (za jeho sofistikované protialkoholní postupy) a zejména v tematické skupině lingvistika (za jeho pokus o vytvoření univerzálního obrázkového písma, které by mohlo být čteno v každém jazyce). Takováto snaha je vzácná, není však zcela ojedinělá. O generaci mladší MUDr. Jan Lukeš rovněž sestavil pro svých šestnáct umělých jazyků zvláštní abecedy s roztodivnými grafémy. Borecký zmiňuje ještě Josefa Diviše, který vykreslil důmyslně svou staročeskou runovou abecedu, tvořící základ jeho myslivecké (neboli myslitelské) latiny, v souvislosti s objevem Zlaté knihy z období

panování kněžny Libuše. Je jen škoda, že tyto osobnosti nemohl psychiatr Antonín Heveroch zahrnout do svého díla „O podivínech a lidech nápadných“ z roku 1905. Tuto knihu dobře znal Jaroslav Hašek a vybíral si podle ní typy svých literárních postav. Mimochodem podle Wikipedie je Sommer Batěk parodován ve Váchalově Krvavém románu.

Alexandr Sommer Batěk se narodil v Prádle u Nepomuku 15. 6. 1874 v domě čp. 13, na kterém má pamětní desku. Ta byla slavnostně odhalena 15 .6. 1975 a při této příležitosti byla na chodbě prádelské školy uspořádána výstavka Batěkova díla. Batěkův otec Emanuel působil pět let v Prádle jako učitel. Matka byla rozená Sommerová a právě na její památku rozšířil později syn své příjmení. Batěk studoval chemii v Praze na Karlově univerzitě a doktorátu z filozofie dosáhl za disertační práci „Revize atomové váhy ceria“, za kterou získal i cenu České akademie spojenou s odměnou 200 zlatých. To mu umožnilo cestu do Anglie a Francie. Po návratu pracoval jako chemik a chemii vyučoval v Praze, pak v Jičíně a Plzni. Jeho pozdější práce ve fyzikální chemii měly v českém prostředí zásadní význam a jsou vzpomenuty v článku „Vzpomínka na da Vinciho české chemie“ v Chemických listech č. 102 (2008). V roce 1908 se zúčastnil protialkoholního sjezdu v Praze, kde byl zvolen do předsednictva. Roku 1912 se přestěhoval s rodinou zpět do Prahy, měl již 3 děti a chtěl se stát soukromým docentem na Karlově univerzitě. Batěkova habilitační práce však nebyla akceptována a nepřijetí na vysokou školu mělo zásadní vliv na jeho další popularizační činnost. Jeho záběr byl neuvěřitelně široký, po celé Praze, zejména pak na Staroměstském náměstí, konal prakticky denně na různá témata veřejné přednášky, které pak vydával tiskem. Jeden pozoruhodný článek se jmenuje „Spojené státy evropské“ a poukazuje v něm na nutnost sjednotit Evropu. Napsal utopický román „Ocelové paže“ pod pseudonymem Helliar, dále „Dějiny hnutí mírového“ a spisy „Abstinence“ a „Zpověď pijákova“. Založil eubiotiku neboli dobrožilství, což je nauka o krásném a dokonalém životě. V Národní knihovně je zaznamenáno 271 děl tohoto autora. Z výše uvedeného výčtu je patrné, že to nejsou zdaleka pouze neoglyfy, které by doktora Sommera Batěka kvalifikovaly do extraligy českých mašíblů (zkratka slov magor-šílenec-blbec) (viz. Borecký V.: Zrcadlo obzvláštního (z našich mašíblů). Hynek, Praha 1999).

Neoglyfy jsou jakési hieroglyfy, což vytváří jistou potíž při jejich popisu, neboť pro jejich zobrazení v žádném editoru nejsou k dispozici příslušné fonty. Na stejný problém pravděpodobně narážel sám Batěk z důvodu obtížnosti knižní sazby. Přestože v letech 1931 až 1936 vydal čtyři vydání publikace „Neoglyfy I“, vždy ale jen ve formě souboru šestnáctistránkových sešitů. Sešitů bylo 37 a mohly se vkládat do připravených desek.



Ukázka ze sešitu Batěk S.A: Neoglyfy I., v příloze neoglyfy.pdf jsou k dispozici strany 4 -13 tohoto sešitu

Není známo, že by „Neoglyfy“ byly vydány i jako vázaná knižní monografie. Pravděpodobně ne. Byl to i důvod finanční, neboť většinu svých publikaci vydával Sommer Batěk vlastním nákladem a sám je distribuoval. Vydávání vázaných knih bylo určitě dražší než vydávání brožovaných sešitů. Kromě „Neoglyfů I“, nazvaných učebnice, vydal ještě „Neoglyfy dětem“ a „Neoglyfy mládeži“. První zmínka o neoglyfech se však pravděpodobně objevila v jeho osmnáctistránkové publikaci „Zázrak písma: vznik a vývoj písma, písmo uzlové, čárkové, klínové a obrázkové, hieroglyfy, písmo předmětové, čínské, abeceda Morseova a Neoglyfy“. Ta byla

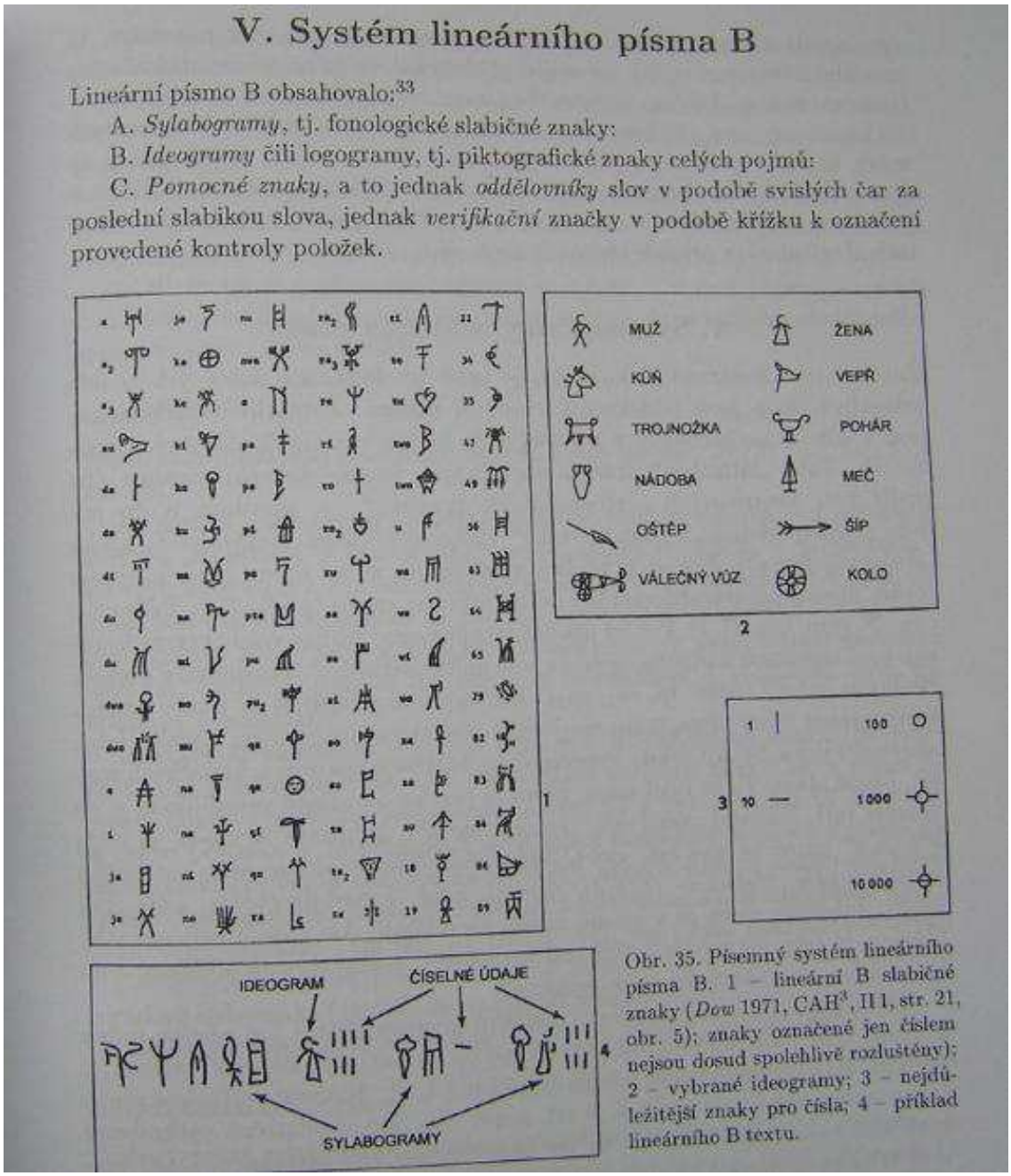
vydána jako soukromý tisk knihtiskárny Karel Mašín v Kladně pro účastníky osmého bibliofilského večera, konaného v sobotu 31. října 1931 v Praze.

Autor hned v úvodu definuje neoglyfy jako „znaky pojmů, které v různých řečech se vyjadřují různými zvuky. Neoglyf jest ideogram tj. obraz myšlenky a není poután na slova různých jazyků“. Tento jeho obraz myšlenky, tj. slova nebo výjimečně složeného výrazu (zatím uvažujeme bez ohledu na gramatiku a syntaxi zapisovaného textu), je většinou interpretován zcela naivní ikonou, která představuje grafickou podobu čili obrázek významu daného slova. Například myšlenka vyjádřená zvukově v češtině slovem „prase“ je zapsána ikonou prasátka, jak ji maluje čtyřleté dítě a jak ji můžeme znát z obrázků na školních lavicích v nižších ročnících. Jenom nemá ten zakroucený ocásek. Slovo „srdce“ je zobrazeno srdíčkem, ale slovo „láska“ již není zobrazeno srdíčkem proťatým Amorovým šípem, jak by bylo možno předpokládat, ale srdíčkem opatřeným tzv. determinativem nadepsaným a ještě tzv. determinativem předraženým. Ovšem k otázce gramatiky i sémantiky se ještě vrátíme později. To platí pro mnoho slov, ale ne pro všechna. Otázkou je, proč se mezi 360 základních neoglyfů, publikovaných v prvním sešitě, objevují v jazyce velmi nepatrně frekventovaná slova jako „vémě“, „voština“, „fíkový list“ nebo „bič“ a „důtky“ (viz obrazová příloha), u kterých zobrazení jednoduché grafické ikony vyžaduje dosti velkou fantazii. Protože všeobecné znalosti autora byly téměř univerzální, použil všechny ikony, které již dříve znal. Triviálně pro slovo paragraf použil překvapivě neoglyf §. Pro výrazy používané ve vysvětlivkách na geografických mapách použil jako neoglyfy příslušné obvyklé mapové značky. Pro matematické výrazy použil obvyklé matematické znaky, např. „nekonečno“ zapsal neoglyfem ∞ . Stejně se ale dostal do problému nedostatku ikon pro své neoglyfy, a tak např. slova „chlorid sodný“ označil neoglyfem NaCl (asi v zajetí své profese chemika). Abychom autorovi nekřivdili – použil i příslušné determinativy pro substantivum a adjektivum. Podobně pro slovo „uhlík“ použil základní neoglyf C a tak podobně. Je to jediná větší výjimka, kdy se v neoglyfech objevila grafická podoba znaků latinky. Druhou výjimkou jsou názvy rostlin, které jsou zobrazovány psanými latinskými názvy. Některé neoglyfy však jsou daleko sofistikovanější. Ojediněle pro některé chemické sloučeniny, které měly již v minulosti zavedené alchymistické značky, použil tyto jako neoglyfy (např. „sůl“). Pro jména těles sluneční soustavy využil jako neoglyfy příslušné astronomické značky. Astrologické značky různých souhvězdí aplikoval na výrazy, které souhvězdí

pojmenovávají, např. astrologické označení souhvězdí Panny představuje neoglyf pro slovo „panna“. Totéž platí pro slova „býk“, „rak“, „beran“, „lev“, „štír“ apod. Naopak slovo „pavouk“ je zobrazeno ikonou reálně připomínající klíště. Se smyslem pro detail uveďme, že „klíště“ je zobrazeno složeným neoglyfem ze symbolů pro „hmyz“ a „nůžky“. Gótské runové písmo autora nijak neinspirovalo, neboť se nepodařilo nalézt žádnou shodu. Porovnání bylo provedeno s publikacemi Koch Rudolf: The Book of Signs, Doven Publications, London 1930 (česky Votobia 1997), Priesner Claus, Figala Karin: Alchemie. Lexikon einer hermetischen Wissenschaft, G.H.Beck, München 1998 (česky Vyšehrad 2006) a internetovými zdroji. Zajímavé je i porovnání neoglyfů s jinými známými grafemickými systémy. Trochu připomíná nejstarší varianty klínového písma prvního typu nebo grafémy protosinajské (Genouillac Henri de: Tablettes summérienes archaiques, Paul Geuthner,Paris 1909, Zemánek, Vavroušek, Čech, Bičovský, Rychtařík: Jazyky starého orientu, FF UK, Praha 2010).

Obr. 18. Věštebný nápis na hovězí lopatce, 13.–12. stol. př. n. l.
(Převzato z KEIGHTLEY 1978: Fig. 14)

Syntax složených neoglyfů samozřejmě připomíná syntax složených egyptských hieroglyfů, což je však zcela přirozené. S moderní podobou východoasijských druhů písma nemají neoglyfy nic společného. Archaické čínské písmo však již některé neoglyfy připomíná (viz ilustrace – zdroj Zádrapa Lukáš, Pejčochová Michaela: Čínské písmo, Academia, Praha 2009). Nejvíce neoglyfy připomínají archaické texty řecké, zejména mykénské lineární písmo B (viz ilustrace – zdroj Bartoněk Antonín: Písmo a jazyk mykénské řečtiny, Masarykova univerzita, Brno 2007, Urbancová Daniela, Blažek Václav: Národy starověké Itálie, jejich jazyky a písma, Host, Brno 2008).



Obr. 35. Písemný systém lineárního písma B. 1 – lineární B slabičné znaky (*Dow* 1971, CAH[3], II 1, str. 21, obr. 5); znaky označené jen číslem nejsou dosud spolehlivě rozluštěny; 2 – vybrané ideogramy; 3 – nejdůležitější znaky pro čísla; 4 – příklad lineárního B textu.

Gramatika neoglyfických textů je relativně jednoduchá, ale správné čtení těchto textů je dosti obtížné. Bylo by zajímavé zjistit, kolik lidí se vůbec neoglyfické písmo učilo či případně naučilo. Asi velmi málo, možná jen sám autor. Když pomineme nadšení pro kuriozity, tak je to víceméně ztráta času. Každý neoglyf se skládá ze značek (grafémů), kterých jsou 3 druhy:

1. základní,
2. determinativy nadepsané (tj. psané nad základní),
3. determinativy předražené (tj. psané před základní).

Determinativy nadepsané vyjadřují slovní druh:

Stříška	^	substantiva
obrácená stříška	v	adjektiva
klička	/\/	pronomina
písmeno	n	numeralia
vlnka	~	verba (infinitiv)
lomítko	/	adverbia
tečka a stříška	.^	propozice
měsíček	□	konjunkce
obrácené lomítko	\	interjekce

(partikule jako slovní druh nebyly v roce 1936 definovány).

Další determinativy, kterými je tvořena gramatika slov a syntax textu, a některé základní neoglyfy jsou uvedeny v obrazové příloze, která představuje podstatnou část prvního sešitu neoglyfů. Sešity 2 až 17 představují systém neoglyfů podle tematických okruhů a příslušná cvičení. Sešit 18 a část sešitu 19 obsahují jakýsi slovník neogflyficko-český, který zahrnuje odkazy na stránky, kde byl příslušný neoglyf definován. Sešity 19 až 37 tvoří slovník česko – neoglyfycký, obsahující zároveň výklad jednotlivých slov a pojmů. Očividná je snaha autora o seriozní dílo, které je budováno promyšleně se snahou o úplnost. Zřetelná je však i naivita tohoto snažení. V každém případě je systém neoglyfů doktora Sommera Batěka raritou i v evropském nebo i světovém měřítku.

D. Záhada kódexu Rohonczi

Eugen Antal, ÚIM FEI, STU v Bratislave, (eugen.antal@stuba.sk)

1 Úvod

„Lebo nič nie je také skryté, aby nevyšlo najavo, ani také utajené, aby sa neprezradilo a nedostalo sa na verejnosť.” (Lk 8:17)

V knižnici Maďarskej akadémie vied v Budapešti pod označením K114 [1] leží jedna záhadná malá kniha. Pomenovanie dostala podľa miesta nájdenia mesta Rohoncz (dnešný Rechnitz, Rakúsko), kde bol objavený v roku 1838. Jedná sa o skoro 450 stranový rukopis malého rozmeru, ktorého obsah je doteraz neznámy. [2]

Rukopisu bolo venovaných pomerne málo vedeckých prác, záujem o tento rukopis začal rásť až v posledných rokoch, a to iba z dôvodu medializácie. Záujem však o túto knihu stále zaostáva za najslávnejším nerozlúšteným rukopisom, ktorým je tzv. Voynich-ov rukopis.

2 Základné fakty

Rohonczi kódex je 2cm hrubá kniha veľkosti 10x12 cm. Obsahuje 448 strán. Niekoľko desiatok listov sa oddelilo od prednej a od zadnej časti knihy a nemá titulnú stranu. Listy sú vyrobené z papiera (nie z pergamenu, čo bolo bežne používané v odhadovanom období vzniku knihy). Kódex je popísaný záhadnými symbolmi, ktoré nepripomínajú žiadne doteraz známe písmo. Okrem toho obsahuje aj vyše 80 naivných kresieb, väčšinou s náboženským motívom.
Každá strana knihy obsahuje v priemere 9 až 15 riadkov, kde v každom riadku je 15 až 25 symbolov. [3]

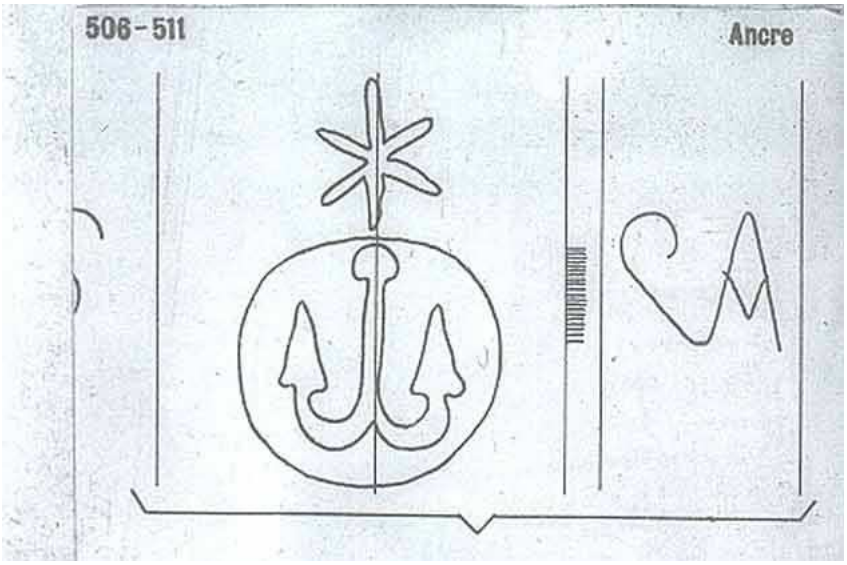
Prvé známe umiestnenie knihy bola knižnica Batthyányiovcov. Od roku 1838, kedy Gustáv Batthyány daroval svoju knižnicu MTA (Maďarská Akadémia Vied) je umiestnená Budapešti. [4]

Kniha je dostupná k prehliadnutiu len s povolením, bol však zhotovený mikrofilm (MF 1173/II), ktorý je sprístupnený aj pre návštevníkov knižnice. [3] Naskenované strany sú dostupné aj pre verejnosť na stránke [5].

3 Datovanie

Dôležitým krokom pred samotným skúmaním obsahu knihy je zistiť pravdepodobné obdobie vzniku.

Podľa nájdeného vodoznaku na papieri, vznik papiera sa datuje na rok 1530-1540 (katalóg vodoznakov Briquet). [2]



Obr. 1. Vodoznak z katalógu Briquet [prevzaté z 5]

Rukopis preskúmal aj uznávaný analytik historických dokumentov, Joe Nickell – nie však v laboratórnych podmienkach. Po analýze atramentu určil druh pera (brad pen) a atrament (iron-gallotannate ink) a datoval ich na približne rovnaký čas, 16.-17.str. [2]

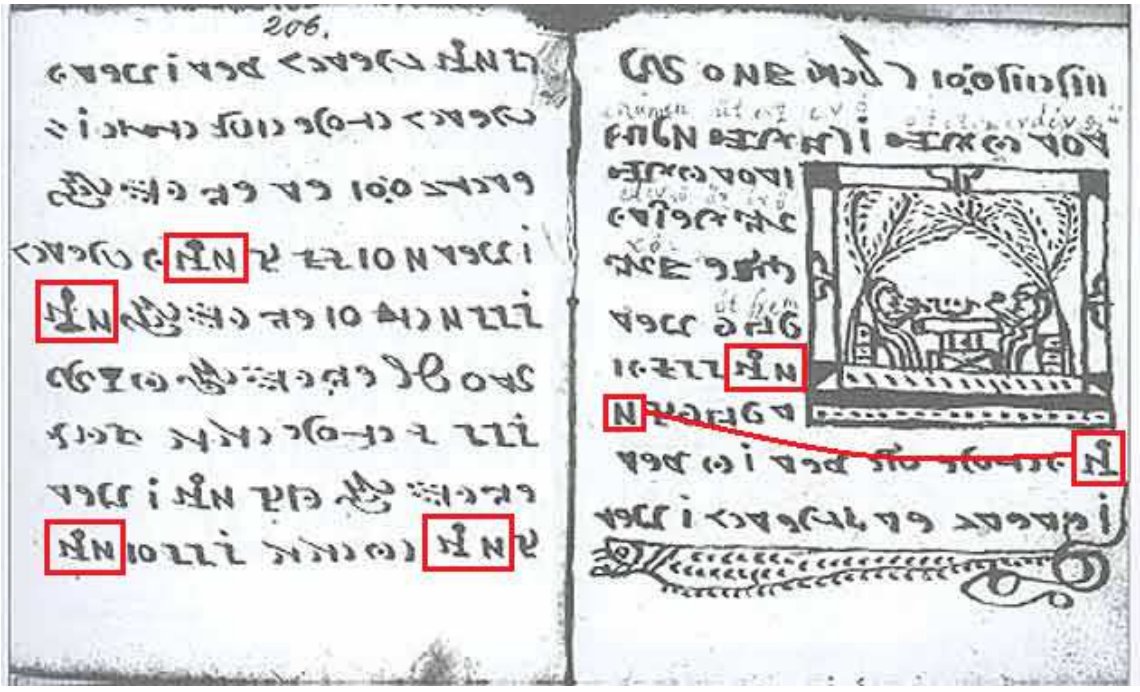
Ďalšie informácie o čase vzniku môžu prezradiť aj samotné kresby. Gábor Tokai po ich preskúmaní došiel k záveru, že konštrukcia kostolov na kresbách pripomína 16.-17.str. [6]

4 Symboly

Kniha obsahuje vyše 150 neznámych symbolov, ktoré nepripomínajú žiadne známe písmo. Sú to pomerne zložité symboly s nejasnou štruktúrou medzier. Nie je možné jednoznačne určiť či symboly reprezentujú slová, slabiky alebo písmená. Niektoré symboly sa často opakujú a niektoré postupnosti symbolov sa vyskytujú spoločne. V knihe je viditeľná prítomnosť variačných prvkov pri jednotlivých symboloch ako bodky, polkruhy a viac bodiek.

Kniha sa číta zprava do ľava a zhora nadol. Smer bol určený podľa rozdelenia opakujúcich sa symbolov na konci riadkov a podľa zarovnania písmen na pravú stranu listov. [3] [4]

Na nasledujúcom obrázku je vidieť, že text je zarovnaný na pravú stranu. Spôsob oddelovania často sa opakujúcej dvojice symbolov tiež naznačuje, že text sa číta zprava do ľava a zhora nadol.



Obr. 2. Vybratá strana z kódexu [prevzaté z 5, modifikované]

Láng Benedek v [2] podrobnejšie popisuje ďalšie zaujímavé fakty, ktoré zistil počas skúmania symbolov kódexu :

1. je zreteľné opotrebovanie a výmena pera pri písaní
2. málo chýb pri písaní, čo bolo neštandardné na 16. storočie – možný prepis knihy zo starších zdrojov
3. rozdiely v písme – viac autorov alebo opotrebovanie pera a zmena rýchlosti písania textu
4. integrácia textu a kresieb - jeden autor

5 Obrázky

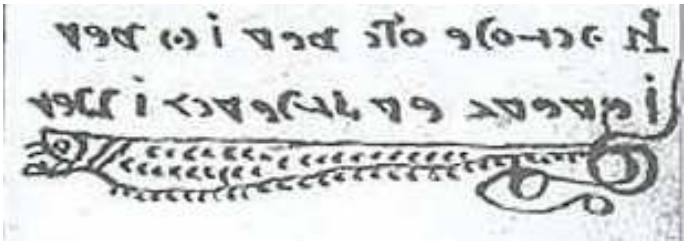
Kniha obsahuje okrem symbolov aj 84 obrázkov, ktoré sú jednoduché – „naivné“ kresby. Ich veľkosť je variabilná - od veľkosti pečiatky až na celú stranu. Väčšina obrázkov je orámovaná.

Prvá časť knihy obsahuje obrázky s jednoznačnou kresťanskou tematikou (Kristus pred Pilátom, ukrižovanie Krista), niektoré však obsahujú znaky islamskej kultúry, ako napr. špicaté brady, turban a kaftan.

Obr. 3. Ukrižovanie Krista [prevzaté z 5]

Obr. 4. Kristus pred Pilátom [prevzaté z 5]

Kniha obsahuje aj špeciálne obrázky s motívom hadov alebo rýb, ktoré pravdepodobne mohli slúžiť na ukončenie jednotlivých kapitol. [4]



Obr. 5. Ukončovací znak kapitoly v knihe [prevzaté z 5]

6 Teórie

V snahe o rozlúštenie kódexu vzniklo niekoľko zaujímavých teórií, ktoré však nie sú podložené a podľa novších analýz sú málo pravdepodobné.

Prvá nepodložená teória je **Šumérsko-maďarská** [2]**.** Autorom je maďarský elektrotechnik Attila Nyíri. Podľa jeho zistení je text kódexu písaný prirodzeným jazykom. Kódex obsahuje náboženský text – modlitby. Jednotlivé symboly spontánne

„rozpozná“ ako písmená latinskej abecedy. Pri lúštení však mal dva veľké nedostatky:

- mal k dispozícii len 2 strany kódexu, ktoré čítať dole hlavou (podľa smeru čítania, viď. kap. 4)
- ten istý znak čítal rôzne.

Najzaujímavejšia teória je **Dako-rumunská** [2], od rumunskej archeologičky Victorie Enâchiuc, ktorá študovala kódex 20 rokov. Ako výsledok predložila 800 stranové štúdium, kde popisuje jazyk kódexu ako „vulgárna latinčina“ (jediným zdrojom tohto jazyka je tento kódex). Obsah identifikovala ako opis bojov Valachov (Blakov) v 11.-12.str. a povzbudzujúce piesne, (obrázky - knieža Vlad). [9] Text čítala sprava doľava ale zdola hore, pričom symboly substituovala vždy rôzne podľa potreby. Obrázky s náboženským motívom stotožňovala s dejinami rumunskej histórie. Napr. „*príchod Ježiša do Jeruzalemu a vyhnanie kufárov z kostola*“ identifikoval, ako „*knieža Vlad sa pripravuje na spojenectvo s Bizanckou ríšou a v kostole Sova Trasiu požehná valachských bojovníkov*“.

Jej teória bola hneď kritizovaná aj Rumunskými historikmi. [2]

Ďalšia zaujímavá teória je **Sanskritská** [2], autorom ktorej je Dr. Mahesh Kuman Sigh. Pri jednej návšteve Maďarska sa mu dostalo do ruky pár listov kópie kódexu, ktoré hneď začal plynule čítať. Podľa jeho tvrdenia sa jedná o Sanskritský jazyk (tzv. bráhmi písmo) a náboženský - kresťanský text. Text čítal zľava doprava a čítal symboly rôzne.

Každá z týchto teórií obsahovala jeden spoločný vážny nedostatok, a to že autori prispôsobovali a menili význam jednotlivých symbolov podľa potreby. Určitý znak čítali na rôznych miestach rôznymi spôsobmi. Nevedeli teda jednoznačne určiť systém čítania.

Takýto spôsob „vylúštenia“ je najviac populárna aj v oblasti nezlomených klasických šifier. Príkladom je napr. pokus o vylúštenie Zodiac Z340 šifry Coreyom Starliperom

[7] - kde v krátkom čase odhalili falošné riešenie [8].

Skúmaním Rohonczi kódexu sa zaoberalo aj niekoľko ďalších autorov, ako János Jerney (prvá publikácia o kódexe 1842), Kálmán Nemethi, Ferenc Toldy, Jozef Jireček, Bernath Jülg, Mihály Munkácsi, Benedek Láng, Miklós Locsmánd, Király Zoltán Levente a ďalší.

Spôsob čítania textu u rôznych autorov sa do značnej miery líšil, odlišoval sa napríklad smer čítania alebo množstvo rozoznaných symbolov, ktorý sa u jednotlivých autorov pohyboval v rozpätí od 100 až po 800 znakov.

7 Záver

Každá záhada do okamihu, kým sa nevyrieši čelí podozreniu, že sa jedná o falzifikát. Toto podozrenie väčšinou časom narastá, každý márny pokus o vylúštenie tento dojem posilňuje. Podobne ako Voynich-ov rukopis aj Rohonczi kódex je považovaný niektorými „riešiteľmi“ za falzifikát. Dokonca aj MTA v poznámke ku knihe oficiálne uvádza, že je to falzifikát z 19.str. [3]

Dobrou otázkou však zostáva samotný dôvod, prečo by chcel niekto zmiasť budúcnosť takýmto podvodom a v takomto rozmere. Existuje niekoľko reálnych faktov, ktoré skôr odďaľujú Rohonczi kódex od štatútu falzifikát, sú to napr.:

- neobsahuje „upútajúce“ prvky – nábožensk á tematika
- kniha nevyzerá byť drahá, skôr opotrebovaná
- príliš dlhý text

Tieto fakty vyvracajú podozrenie, že sa jedná o knihu, ktorá bola vytvorená cieľom predaja za vysokú cenu.

Napriek snahám o vylúštenie záhadou zostáva samotný obsah knihy, ako aj to či sa jedná o umelý jazyk, neznámy jazyk alebo zašifrovaný text.

Literatúra

[1] Csapodi, Cs., (1973). A "Magyar Codexek" elnevezésű gyűjtemény (K 31 - K 114) [The Collection "Hungarian Codices"], Budapest, (Catalogues of the Manuscript and Old Books Department of the Library of the Hungarian Academy of Sciences, vol. 5.), pp 109.

[2] Láng B., (2011). A Rohonci kód, Jaffa, Budapest, ISBN: 978 963 9971 67 7

[3] Lochmándi M.,(2004/05). A Rohonci Kódex. Egy rejtélyes középkori írás megfejtési kísérlete, Turán 2004/6 - 2005/1, pp 41–58.

[4] Király L. Z., (2011/12). Struktúrák a Rohonci-kódex szövegében. Helyzetjelentés egy amatőr kutatásról, Theologiai Szemle 54, pp 82–93

[5] Skenované obrázky Rohonczi kódexu,
Online: http://www.dacia.org/codex/original/original.html (2012.9.14)

[6] Tokai G., (2011/12) Az első lépések a Rohonci-kódex megfejtéséhez, Élet és Tudomány LXV/52–53, LXVI/2, pp 50–53.

[7] Bruce Schneier
Online: http://www.schneier.com/blog/archives/2011/08/zodiac_cipher_c.html (2012.9.14)

[8] Online: http://oranchak.com/zodiac/corey/hoax.html (2012.9.14)

[9] Enâchiuc V. (2002). Rohonczi Codex: descifrare, transcriere şi traducere (Déchiffrement, transcription et traduction, Alcor Edimpex SLR, ISBN 973-8160-07-3.

E. Kaspersky Lab uvádí Kaspersky Internet Security 2013

Zástupce Crypto-Worldu se zúčastnil 5.9.2012 snídaně se zástupci Společnosti Kaspersky Lab, která se konala v Boscolo Prague Hotelu na Senovážném náměstí 13, v Cigar Baru umístěném v bývalém bankovním trezoru.

Kaspersky Lab na tomto setkání představil **Andrej Slobodjanik,** ředitel Kaspersky Lab pro východní Evropu. Dále zde hovořil **David Emm**, bezpečnostní analytik Kaspersky Lab z Velké Británie, **Petr Aljoškin**, marketingový manažer Kaspersky Lab, a **Andis Šteinmanis**, ředitel Kaspersky Lab pro Českou republiku.

Dovolte nám, abychom se podělili o informace z tohoto setkání. K přípravě této informace byla využita tisková zpráva, kterou k této příležitosti vydala agentura Grayling (kontakt viz závěr tohoto sdělení).

Společnost Kaspersky Lab představila nejnovější verzi svých vlajkových produktů – prémiovou komplexní ochranu **Kaspersky Internet Security 2013** a nepostradatelný antivirový software **Kaspersky Anti-Virus 2013.** Oba disponují vylepšeným a snadně ovladatelným rozhraním a nabízejí nové technologie k maximální ochraně před všemi druhy nebezpečí. Protože se prostředí kybernetických hrozeb neustále mění, věnovala společnost Kaspersky Lab zvláštní pozornost ochraně potenciálně zranitelných programů pomocí jedinečné technologie Automatic Exploit Prevention (automatická ochrana před zneužitím).

Uživatelé zcela nové verze Kaspersky Internet Security budou moci využít komplexní ochrany jejich onlinových bankovních transakcí a nákupů díky aplikaci Safe Money. Oba produkty jsou také plně kompatibilní s novým operačním systémem Windows 8 a účinně chrání aplikace a data, ať už v jeho klasickém nebo dotykovém rozhraní.

„S vědomím, že se naši domácí uživatelé obávají nejvíce ztráty citlivých dat a také peněz, vyvinuli jsme zcela novou sadu obranných technologií. Kaspersky Internet Security 2013 je nyní lepší než kdy dřív v ochraně nejcennějších informací při aktivitách na internetu. S přístupem Hybrid Protection a novými technologiemi Automatic Exploit Protection a Safe Money pomáhá Kaspersky Internet Security 2013 zákazníkům vybudovat nejúčinnější bezpečnostní systém, který se snadno nastaví i spravuje,“ uvedl Eugene Kaspersky, zakladatel a ředitel Kaspersky Lab.

Hlavní přednosti Kaspersky Internet Security 2013:

- unikátní technologie Automatic Exploit Prevention
- aplikace Safe Money chránící online peněžní transakce
- zabezpečení před odezíráním psaní na klávesnici pomocí Virtual Keyboard a Secure Keyboard
- nová antivirová technologie
- anti-phishingový modul
- rychlejší a účinnější aktualizace databáze díky cloudu Kaspersky Security Network
- nová ochrana proti spamům
- plná kompatibilita s OS Windows 8
- jedinečná rodičovská ochrana

Automatic Exploit Prevention technologie byla navržena tak, aby reagovala na nejsofistikovanější hrozby – zneužitelná slabá místa v oblíbených programech. Ta jsou totiž dlouhodobě oblíbenou zbraní kybernetických zločinců k takzvaným „drive-by download“ útokům, tedy kdy je uživatel infikován už při návštěvě určité webové stránky.

Automatic Exploit Prevention chrání zákazníky Kaspersky Lab před těmito hrozbami, včetně „zero-day“ slabiny, kdy je systém infikován skrze v tu chvíli ještě neznámou nebo nepatchovanou chybu v zabezpečení v oblíbeném, nově instalovaném softwaru. Na základě bohatých zkušeností Kaspersky Lab v bezpečnosti IT je technologie Automatic Exploit Prevention schopná rozeznat neautorizovanou aktivitu, aniž by zablokovala činnost ohroženého programu jako je třeba webový prohlížeč, prohlížeč dokumentů, apod.

Technologie **Safe Money** obsahuje bohatou sadu obranných metod pro situace, kdy zacházíte s penězi online. Mezi ně patří nakupování na internetu, práce s platebními systémy typu PayPal nebo přístup na vaše bankovní konto na vašem počítači. Tato novinka, která je součástí Kaspersky Internet Security 2013, poskytuje vylepšenou ochranu bankovních operací.
Ta funguje následovně: Automaticky se zapne mód zvláštního „bezpečného webového prohlížeče“ při návštěvě bankovních stránek. Tím izoluje platební operace od dalších online aktivit a zabezpečí, aby transakce nebyla monitorována. Kontroluje navíc autentičnost samotné platební webové stránky, aby zajistil, že stránka není napadená nebo falešná.
Safe Money technologie také zhodnotí stav zabezpečení vašeho počítače a varuje před významnými hrozbami, které je třeba vyřešit před jakoukoliv platbou.
Díky aplikaci Safe Money zvítězil Kaspersky Internet Security 2013 v nezávislých testech bezpečnosti online plateb organizace Matousec.com. Jako jediný uspěl ve všech 15 bodech a umístil se daleko před konkurencí.

Virtual Keyboard (virtuální klávesnice) zajistí, že nikdo nebude z klávesnice odezírat zapisování hesla nebo čísla karty (tzv. keylogging). Před „keyloggers“ chrání i speciální nástroj **Secure Keyboard**, bezpečný ovladač vaší klávesnice.

Oba programy Kaspersky Internet Security 2013 a Kaspersky Anti-Virus 2013 pohání **nová antivirová technologie** lépe chránící před škodlivými programy, včetně těch nejsložitějších. Využívá zejména metody k boji proti komplexním hrozbám, které zastaví pokusy umístit škodlivé kódy do systémových procesů počítače. Zároveň nabízí rychlejší aktualizace antivirové databáze, protože části z ní byly přesunuty na cloudovou síť **Kaspersky Security Network**.

Ke zlepšení ochrany nabízejí nové produkty také **anti-phishingový modul** s automatickou aktualizací a vylepšenou heuristickou detekcí stránek, které se snaží ukrást vaše hesla a citlivá data. Kaspersky Internet Security 2013 obsahuje navíc novou **ochranu proti spamům**, nabízející nejspolehlivější detekci nevyžádané pošty ve vašem e-mailu.

Kaspersky Internet Security 2013 a Kaspersky Anti-Virus 2013 jsou plně **kompatibilní** s novým operačním systémem Windows 8 od Microsoftu. Kasperky Lab jeho uživatelům poskytuje plnou ochranu, s vylepšenou bezpečností aplikací v novém dotykovém rozhraní a podporou všech bezpečnostních opatření samotného

operačního systému. Nová aplikace *Kaspersky Now* poskytuje uživatelům Windows 8 rychlý přehled stavu zabezpečení jejich počítače a nabízí možnost spuštění bezpečnostních aplikací programů Kaspersky Anti-Virus a Kaspersky Internet Security přímo z nového uživatelského rozhraní, Tato aplikace je k dispozici zdarma na stránkách Windows Store.

Vylepšená **rodičovská ochrana** nejnovějších produktů Kaspersky Lab nabízí také intenzivní ochranu dětí před škodlivým obsahem na internetu a poskytuje možnost zabránit jim v přístupu na nechtěné stránky.

Více o KIS 2013 anglicky na: http://www.kaspersky.com/kaspersky_internet_security
A o KAV 2013 na: http://www.kaspersky.com/kaspersky_anti-virus

Safe Money od Kaspersky Lab chrání podle nezávislých testů peníze nejlépe ze všech

Nejnovější Safe Money technologie společnosti Kaspersky Lab vykázala v nezávislých testech bezpečnostních expertů organizace Matousec.com nejlepší skóre. Analýza zkoumala, jak efektivně si umí nejrůznější bezpečnostní řešení poradit s pokusy odcizit bankovní data během online transakcí.

Ze 14 testovaných produktů se nejlépe umístil produkt Kaspersky Internet Security 2013, který přichází na český trh právě nyní. Celkem dosáhl plných 15 bodů a uspěl tak ve všech 15 bodech testu, včetně simulace chování malwaru snažícího se ukrást data z populárních stránek jako je PayPal nebo eBay.

Kaspersky Internet Security 2013 obsahuje jedinečnou technologii Safe Money – širokou škálu nástrojů k zabezpečení proti bankovním hrozbám. Jeden z nich například umí ověřit autentičnost onlinových obchodů a webových stránek bank, další odhaluje zranitelná místa v počítači nebo působí proti odezírání činnosti klávesnice, takzvanému keyloggingu.

„Když jsme Safe Money navrhovali pro náš nový produkt, snažili jsme se ze všech sil zvážit všechny způsoby, jakými je možné ukrást informace. Účinnost tohoto přístupu, který zaručuje maximální a automatickou ochranu důležitých internetových operací, byla nyní potvrzena nezávislými analytiky. Testování Matousec.org prokázalo, že Kaspersky Internet Security 2013 poskytne našim zákazníkům nejspolehlivější ochranu jejich onlinových plateb na úrovni srovnatelné se specializovanými podnikovými řešeními,“ řekl šéf anti-malwarového výzkumu Kaspersky Lab Oleg Išanov.

Plnou verzi zprávy Matousec.com naleznete na těchto stránkách:
http://www.kaspersky.com/downloads/pdf/online_payments_threats_report_matousec.pdf
Více informací o unikátní technologii Kaspersky Lab Safe Money naleznete na: http://www.kaspersky.com/downloads/pdf/kaspersky_lab_whitepaper_safe_money_eng_final.pdf

Pro další informace prosím kontaktujte:

Michal Malysa, PR Consultant
Grayling, Mobil: 775 708 086
michal.malysa@grayling.com

Štěpán Kačena, Senior PR Consultant
Grayling, Mobil: 774 226 127
stepan.kacena@grayling.com

F. O čem jsme psali v září a říjnu 1999 – 2011

Crypto-World 9/2005

Crypto-World 9/2006

Crypto-World 9/2007

Crypto-World 9/2008

Crypto-World 9/2009

Crypto-World 9/2010

Crypto-World 10/2005

Příloha : Další informace k článku V.Klímy - prilohy.zip (53 kB)
(Obsahuje: Žádost a podpisy odborníků, Návrh Šámal, Návrh Smejkal, Návrh VK_IURE, překlad části úmluvy, průvodní dopis vk_iure, link psp, stenozáznam jednání PSP, tisk zpráva ČTK)

Crypto-World 10/2006

Příloha: doprovodné materiály k Soutěži v luštění 2006 - vystava.pdf , epilog.pdf

Crypto-World 10/2007

Crypto-World 10/2008

Příloha: simulátor historického šifrátoru Lorenz SZ 40- lorenz.zip.enp

Crypto-World 10/2009

Crypto-World 10/2010

Crypto-World 10/2011

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 autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí e-ziny, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály: http://crypto-world.info

2. Registrace / zrušení registrace

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

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška Jozef Krajčovič Vlastimil Klíma Tomáš Rosa Dušan Drábik
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Jaroslav Pinkava
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.cz ,	http://crypto.hyperlink.cz/
Dušan Drábik	Dusan.Drabik@o2bs.com ,	
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