Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 9, číslo 5/2007 **17. květen 2007**

5/2007

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1262 registrovaných odběratelů)

Obsah : str.

A. Z dějin československé kryptografie, část I.
Československý šifrátor MAGDA

Mgr. Karel Šklíba (karel.skliba@crypto-world.info**)**

Počátek vývoje šifrovacích strojů v Československu lze datovat asi do roku 1930. Až do roku 1938 byl jediným šifrovacím strojem, který byl vyvinut ve větší sérii v československé armádě, pneumatický mechanický šifrovací stroj Štolba. Od roku 1945 do roku 1955 se na československém ministerstvu obrany postupně pracovalo na vývoji několika typů šifrovacích strojů. Byly to stroje Štolba 2, Heda, Karel, Panlist, Magda, Boba, Era, Ela a Věra. Celý tento vývoj byl prováděn dosti primitivně s velmi špatnými výsledky. Žádný z uvedených strojů nebyl použit v armádním ani jiném provozu, neboť již tehdy prováděné kryptoanalýzy neměly kladný výsledek. Tehdy odhadovaná finanční ztráta na neúspěšném vývoji činila 15 milionů Kč. V letech 1945 až 1955 došlo v československé armádě k širokému používání trofejních šifrovacích strojů ANNA, ENIGMA a SCHLÜSSELGERÄT. Situace se změnila až v roce 1955, kdy byla vytvořena Zvláštní správa ministerstva vnitra, která řídila a koordinovala šifrovou službu v Československu.

Šifrovací stroj Magda byl zcela mechanický šifrátor pro šifrování off-line (v tehdejší terminologii tzv. předběžné šifrování). Princip tohoto stroje byl okopírován ze systému navrženého švédským konstruktérem Borisem Hagelinem. Mnoho variant tohoto systému bylo používáno za 2. světové války, zřejmě nejvíce v americké armádě pod označením M-209 a ve francouzské armádě pod označením C-36, což odpovídalo původnímu značení výrobků firmy HAGELIN.

Magda byla vyvíjena pro potřeby československé armády přibližně v letech 1950 až 1953 jako polní šifrátor a v letech 1954 – 1955 bylo vyrobeno asi 600 kusů těchto zařízení v České zbrojovce Brno. Vývoj byl započat ještě za vedení slavného prvorepublikového československého konstruktéra plk. Ing. Štolby (byl dvojnásobným inženýrem strojním a elektrotechniky), který se proslavil jako špičkový mechanik konstrukcí pneumatických diskových šifrátorů ve 30. letech 20. století a z generálního štábu odešel (pravděpodobně do důchodu) v roce 1953. Na vývoji šifrátoru Magda začal pracovat mjr. Ing. Oldřich Hrudka, který přišel do konstrukční kanceláře z Tesly Karlín a který také navrhl název zařízení podle křestního jména své babičky. Vojenská konstrukční kancelář generálního štábu sídlila tehdy v 5. patře budovy v Praze – Dejvicích na dnešním Vítězném náměstí a její vedení převzal po odchodu Ing. Štolby asi v roce 1953 Ing. Hrudka. Ing. Hrudka dostal za konstrukci Magdy finanční odměnu a později, když se prokázala malá kryptologická bezpečnost a zejména konstrukční nedostatky zařízení, měl velké obavy z případného postihu. Přestože šifrátor Magda nebyl nikdy nasazen do armádního ani jiného provozu a až na pár

výjimek bylo všech několik set vyrobených kusů sešrotováno, lze konstatovat, že Magda byl stroj celkem kvalitně navržený a vyrobený pro polní použití, avšak svou koncepcí odpovídal předválečnému období a v roce 1955 již byl zastaralý.

Popis šifrovacího stroje Magda

Šifrovací stroj Magda měl rozměry šířka 15 cm, hloubka 16 cm a výška 11 cm a měl hmotnost 4 kg. Vlastní zařízení mělo 4 nožičky z tvrdé gumy a bylo jej možné uzavřít do ocelového krytu s uchem na přenášení. V krytu byl zevnitř umístěn držák na 4 kusy papírové pásky široké cca 15 mm, která se používala pro tisk otevřeného a šifrového textu. Vlastní šifrovací mechanismus se skládal z pěti kol s výsuvnými kolíčky a s přilehlými ozubenými koly k zajištění pohybu kolíčkových kol, dále z bubnu, na jehož lištách se nacházeli tzv. jezdci a dále z tzv. molety a mechanismu tiskacích koleček pro tisk šifrového a otevřeného textu.

Kola šifrovacího stroje Magda

Pro popis slouží očíslování kol zleva doprava, tj. kolo číslo 1 bude kolo zcela vlevo při pohledu na stroj a kolo číslo 5 bude kolo zcela vpravo.

kolo číslo 1 velikost 30
označení jednotlivých poloh:
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 1 2 3 4

kolo číslo 2 velikost 29
označení jednotlivých poloh:
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 1 2 3

kolo číslo 3 velikost 28
označení jednotlivých poloh:
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 1 2

kolo číslo 4 velikost 27
označení jednotlivých poloh:
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 1

kolo číslo 5 velikost 26
označení jednotlivých poloh:
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

V každé z takto označených jednotlivých poloh každého kola byl ocelový kolíček buď v pasivním stavu vysunutý doleva (v této poloze neovlivňovalo toto kolo tvorbu hesla) nebo

v aktivním stavu vysunutý doprava (v této poloze ovlivňovalo toto kolo tvorbu hesla). Vysunutí kolíčků doprava nebo doleva v každé poloze každého kola byla první částí tzv. vnitřního nastavení šifrátoru Magda. Na přední části stroje byla přes výše popsaná pohyblivá kola umístěna lišta s okénky, ve kterých bylo vidět označení právě aktivních poloh jednotlivých kol. Tato pětice písmen a číslic označující počáteční polohu kol při začátku šifrování nebo dešifrace byla první částí tzv. vnějšího nastavení šifrátoru Magda. Všechna popsaná kola krokovala pravidelně o 1 krok při zašifrování či dešifraci 1 znaku a krokování žádného kola neovlivňovalo krokování či poloha kolíčků na kolech ostatních. Zajímavostí bylo, že pro zvýšení bezpečnosti měla ozubená kola (zajišťující pohyb kol s kolíčky) nestandardní zuby. Aby nebylo možné vyrábět duplikáty, byla na zubech tzv. evolventa o hodnotě 1,2, maximálně 1,5.

Buben s jezdci šifrovacího stroje Magda

Buben šifrátoru Magda byl umístěn v zadní části stroje vpravo za sadou kol a byl pevně spojen se sklápěcí klikou, kterou byl zajišťován jeho pohyb. Buben měl 26 lišt označených 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. Na každé liště bubnu byli umístěni dva jezdci. Lišta upevněná nad bubnem vzadu označovala 5 aktivních poloh jezdců proti jednotlivým kolům a 2 pasivní polohy, kdy jezdci na liště umístění v těchto polohách se nepodíleli na vytváření hodnoty hesla. Aktivní polohy pro umístění jezdců byly označeny 1 2 3 4 5 a pasivní polohy byly umístěny mezi aktivními polohami 1-2 a 4-5. Pasivní polohy byly označeny znakem 0.

Moleta a tisková kolečka šifrovacího stroje Magda

Moleta a 2 tisková kolečka byly umístěny pod krytem v levé přední části stroje. (Další popis stroje nemusí být zcela přesný, protože dostupné informace z literatury a výstav historické šifrovací techniky v květnu 1982 a 18.4.1985 nejsou dostatečně podrobné). Moleta bylo kolečko s vyznačením 26 poloh a jednotlivé polohy byly označeny:
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 .

Tisková kolečka otevřeného a šifrového textu byla umístěna recipročně na stejné hřídelce s moletou a obsahovala znaky 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
A Z Y X W V U T S R Q P O N M L K J I H G F E D C B

Posun molety vůči dvěma recipročním tiskovým kolečkům pravděpodobně byl druhým směnným prvkem vnějšího nastavení tohoto šifrátoru. Tisková páska procházela přes tisková kolečka a ostrým výčnělkem na dalším otočném hřídeli se rozřezávala na dvě poloviny (zřejmě jednu s šifrovým a druhou s otevřeným textem).

Šifrování a dešifrace.

Ve svisle protaženém okénku na přední části stroje se na červenou značku posunulo požadované písmeno otevřeného textu. Otočení molety k nastavení požadovaného písmene se provedlo knoflíkem na levé straně stroje. Potom se otočilo vyklopenou klikou na pravé straně stroje až nadoraz. Došlo tím k otočení bubnu s jezdci a k jednomu kroku všech pěti kol s kolíčky a na papírovou pásku se otiskla 2 příslušná písmena. Dešifrace se zřejmě prováděla analogicky.

Označme: S – znak šifrového textu (26 znaků mezinárodní abecedy)
O – znak otevřeného textu (26 znaků mezinárodní abecedy)
H – hodnota hesla (26 možností)

Pak šifrování probíhalo pravděpodobně dle rovnice

$$S = O + H \pmod{26}$$

A dešifrace pravděpodobně dle rovnice

$$O = S + H \pmod{26}$$

Poznámka ke zpestření

U vyrobených prototypů šifrovacího stroje Magda přeskakovala nechtěně moleta o 1 znak, pokud se prudce otočilo klikou. To byla nepřijatelná konstrukční chyba, kterou bylo nutno bezpodmínečně odstranit. Šéfkonstruktér Ing. Hrudka někde potají získal trofejní šifrátor originální Hagelinovy konstrukce a celý jej rozebral. Zjistil, že fígl byl ve středové páce na kole molety, která na obou koncích zapadala do zubů kola a zamezovala tak nechtěnému pohybu o 1 znak na kole molety při prudším otočení klikou. Hrudka to ostatním konstruktérům neprozradil a nutil je k dalším experimentům k odstranění vady. Oni vycítili „levárnu“ a vlezli mu v jeho nepřítomnosti do kanceláře, kde rozebraný stroj objevili. Konstrukční chybu podle toho odstranili a předkládali to jako svůj objev.

Podle známých informací se 1 kus šifrátoru Magda vyskytoval v roce 1997 ve školícím středisku ministerstva vnitra v Pardubicích a několik kusů by mělo být v držení muzejních fondů ministerstva obrany.

Bez velké nadsázky lze konstatovat, že mechanické šifrovací stroje vyráběné v první polovině minulého století sice nebyly tak sofistikované a technicky složité jako tiskařské sázecí stroje, ale rozhodně patřily ke špičkovým mechanickým zařízením, která lidé ve svých dosavadních kulturních dějinách byli schopni vyprodukovat.

B. Řešení dubnové úlohy

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

V letošním dubnovém čísle e-zinu Crypto-World jsem otiskl výzvu k prolomení následujícího šifrového textu:

Soutěžní úloha 4/2007

```
04235 04006 04008 04210 04017 04009 04005 04003 04007
04220 04002 04004 04021 04004 04003 04321 04017 04001
04228 04009 04013 04009 04001 04002 04008 04002 04001
04046 04005 04002 04187 04001 04004 04201 04003 04009
04232 04018 04003 04193 04001 04007 04198 04020 04003
04170 04004 04006 04215 04018 04007 04221 04002 04002
```

Tato výzva byla zveřejněna také v NEWS na naší domovské stránce (17.4.) a byla také zpřístupněná na serverech soom.cz a root.cz .
http://crypto-world.info/news/index.php?prispevek=4992&sekce=s

Domníval jsem se, že text, který byl zašifrován nejzákladnější knižní šifrou, bude poměrně brzy rozluštěn, neboť v e-zinu 4/2007 jsem uvedl řadu indicií. Především se hned ve dvou článcích tohoto čísla píše o některých verzích knižní šifry. Konkrétně v článku *„Zachycené a šifrové telegramy dokazují, že demokraté se během voleb snažili podplácet!“* popisuji slovníkový kód založený na dohodnuté knize a v článku *„Kircherovo šifrování aneb Dobrý voják Švejk“* je uvedena varianta Kircherova knižního šifrování (hledání ekvivalentního slova na protější stránce dohodnuté knihy). O jakou dohodnutou knihu by se mělo jednat jsem se snažil luštitelům napovědět v doporučené literatuře, kde je uveden pouze e-zin se soutěžní úlohou a dále moje knížka „*Kryptologie, šifrování a tajná písma, edice OKO, Albatros 2006*“.

Použitý způsob šifrování

1) Zvolí se dohodnutá kniha, která je dostupná oběma stranám
   (příklad : „*Kryptologie, šifrování a tajná písma*“).
2) Slovo otevřeného textu se vyhledá v knize (na libovolném místě)
   (příklad: kniha).
3) Zapíší se souřadnice tohoto slova, konkrétně stránka, řádek, pořadí slova na řádku
   (prázdné řádky se nepočítají),
   (kniha … strana 210, řádek 17, pořadí slova na řádku 9).
4) Dále se použije následující jednoduché formátování šifrového slova, každá ze souřadnic, které určují příslušné slovo otevřeného textu, se doplní zleva pomocí nul na trojcifernou skupinu
   (příklad 210 017 009).
5) Formátování šifrového textu bylo dále upraveno tak, aby bylo pro luštění co nejjednodušší. Ze šifrových skupin se nevytvoří řetězec, který by se dále rozdělil např. na pětice, ale nejprve se jednotlivé trojice doplní o skupinu 04, tím vznikají skupiny o pěti cifrách. Použité formátování zachovává poměrně dobře strukturu stránka/řádka/pořadí slova. Navíc je téměř na první pohled vidět, že skupina 04 je nadbytečná…
   (příklad: …. 04210 04017 04009 …)

Nesnažil jsem se předložit těžkou úlohu, ale naopak měla to být „odpočinková“ zábavná dubnová úloha. Proto jsem se domníval, že řešení přijdou „obratem“ a z tohoto důvodu jsem také vyhlásil, že po obdržení dvou správných řešení bude informace o prolomení zveřejněna v NEWS. Informace měla sloužit další řešitelům, aby zbytečně nezasílali svá řešení v domnění, že získají některou ze dvou cen (ceny viz e-zin 4/2007).

Věřím, že zveřejnění úlohy v dubnovém – aprílovém čísle dostatečně omluví PR znění mnou připraveného otevřeného textu. Také se touto cestou omlouvám těm řešitelům, kteří nemají ke knížce přístup (již prodáno cca 6000 ks) …

Otevřený text:
Nejlepší kniha o kryptologii, kterou jsem četl, je Kryptologie, šifrování a tajná písma.
Doporučuji ji všem lidem.
Vítěz.

Šifrování
Vyhledání souřadnic (stránka, řádka, pořadí slova na řádce) v dohodnuté knize a zformátování do trojic:

Nejlepší	235 006 008
kniha	210 017 009
o	005 003 007
kryptologii,	220 002 004
kterou	021 004 003
jsem	321 017 001
četl,	228 009 013
je	009 001 002
Kryptologie,	008 002 001
šifrování	046 005 002
a	187 001 004
tajná	201 003 009
písma.	232 018 003
Doporučuji	193 001 007
ji	198 020 003
všem	170 004 006
lidem.	215 018 007
Vítěz.	221 002 002

Zformátování šifrového textu do skupin po pěticích (po doplnění skupiny 04 ke každé souřadnici) dává výsledný zveřejněný šifrový text.

Přes velkou odezvu ze strany čtenářů a řadu dotazů nebyla šifra během týdne pokořena! Proto jsem zveřejnil 29.4. nápovědu, ze které poměrně jasně plynulo, že se využije dohodnutá kniha *Kryptologie, šifrování a tajná písma* a dále, že se jedná o nějaký typ knižní šifry (http://crypto-world.info/news/index.php?prispevek=5065&sekce=s).

Po této nápovědě začala přicházet správná řešení. Jako prvý poslal správné řešení **Roman Cinkais** (30. dubna 2007, 16:34), druhým úspěšným řešitelem se stal **Martin Bálik** (2. května 2007, 0:47). Ještě tentýž den dopoledne pak zaslali svá řešení další tři luštitelé….

Vítězům a všem úspěšným řešitelům blahopřeji !!!!
Ostatním zúčastněným čtenářům děkuji za účast v soutěži a děkuji za zajímavé a milé e-maily a podněty k pravidelné podzimní soutěži, ke které si vás dovoluji touto cestou již s předstihem pozvat!

C. Bealovy šifry

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

V minulém e-zinu a v předchozím článku jsme si připomněli některé běžné varianty knižních šifer. Jednou z nejjednodušších metod je šifra, která se někdy označuje jako „druhá Bealova šifra“ nebo jednoduše „Bealova šifra“.

Tato šifra a související příběh nebyly prozatím v české literatuře příliš popularizovány. Snad jedinou a čestnou výjimkou je Singhova „Kniha kódů a šifer“. Autor se zde tomuto v USA nesmírně populárnímu tématu podrobně věnuje na str. 88 - 103.
Další informace lze vyhledat v mnoha zdrojích na Internetu. Doporučuji začít „domácí stránkou legendy“ [1] resp. informacemi v anglické verzi encyklopedie Wikipedia [2]. Naopak nedoporučuji stránky některých „lovců pokladů“, včetně stránek členů Společnosti Bealových šifer, které obsahují informace, které nebývají zcela podloženy realitou a jsou někdy spíše zbožným přáním těchto osob než výsledkem skutečného bádání …

Příběh

1885
Muž, jehož identita zůstala dodnes utajena, kontaktuje váženého občana Lynchburgu, okresního zeměměřiče Jamese B. Warda. Obrací se na něj s prosbou, zda by byl ochoten jej zastupovat a vydal jím připravenou knihu. V knize údajně uvádí vše, co ví o zakopaném pokladu, který nebyl dosud pravděpodobně vyzvednut. Pan Ward souhlasí a zajistí vytištění jeho útlé knížky (23 stran), která se stane výzvou řešitelům záhad, speciálně pak kryptologům a hledačům pokladů.

1885
Dříve, než dojde k distribuci knihy, je většina nákladu zničena při velkém požáru skladu. Přesto kniha vzbudí pořádný rozruch, který přetrvává až do současnosti.

V knize je popsán následující příběh:

Leden – březen 1820
Do hotelu Washington v Lynchburgu ve Virginii, který patří Robertu Morrissovi, se přistěhoval cizinec jménem Thomas J. Beale. S nikým zde nemluvil ani o své minulosti, ani o účelu své návštěvy. Strávil v hotelu zimu a v březnu odjíždí.

Leden – březen 1822
Cizinec se opět ubytuje ve stejném hotelu. V březnu 1822 opět odjíždí. Majiteli hotelu při odchodu předává uzamčenou kovovou skřínku a prosí jej o její pečlivé uschování. Podle něj skřínka obsahuje hodnotné a důležité listiny. Hostinský Morriss ukládá skřínku do svého sejfu.

9. květen 1822
Beale zasílá ze St. Louis panu Morrissovi dopis, ve kterém odhaluje skutečný obsah skřínky. Jsou v ní dokumenty, na nichž závisí jak jeho bohatství, tak bohatství jeho přátel. Beale se bojí, že kdyby zemřel, pak kolegové nebo jejich příbuzní by se k penězům nedostali. Proto jej prosí, aby skřínku opatroval a kdyby se snad on nebo kdokoli z jím pověřených kolegů pro skřínku nevrátil, aby ji po deseti letech otevřel. Ve skřínce najde dokumenty, které jsou však

bez klíče nečitelné. Beale dále píše, že odpovídající klíč k dešifrování zanechal v dopise, který předal jinému svému příteli. Dopis je zapečetěný a adresovaný na pana Morrisse s pokynem „neodesílat do června 1832“. S pomocí klíče, který takto dostanete, píše Beale, již snadno pochopíte, co je třeba.

Červen 1832
Dopis s klíčem nedorazil a pan Morriss nechává proto skřínku uzavřenu, pravděpodobně se domnívá, že by její obsah bez klíče stejně nebyl schopen pochopit.

1845
Pan Morriss skřínku přece jen násilím otevírá. Nachází zde tři zašifrované zprávy. V příloze k článku jsou označeny jako Šifra č. 1, Šifra č. 2, Šifra č. 3. Dále je zde anglicky psaný dopis. V něm pan Beale popisuje, jak se v roce 1817 on a jeho 29 přátel toulá po loveckých oblastech Západu. V březnu společně vyrazí na sever ze Santa Fé a sledují velké stádo buvolů. Naleznou však zlato. Z lovců se stávají zlatokopové. Za pomoci místního indiánského kmene vytěží velké množství zlata a stříbra, které najdou poblíž zlatonosného naleziště. Rozhodnou se přestěhovat své získané bohatství na bezpečnější místo, a proto roku 1820 odváží pan Beale vykopané zásoby ukrýt domů do Virginie. Zlato a stříbro údajně ukrývá při své prvé návštěvě v Lynchburgu. Tedy v době, kdy poprvé bydlel v Morrissově hotelu. Odtud se vrací zpět ke svým přátelům, aby společně dále dolovali. V roce 1822 se vrací a přiváží další nakutané zásoby zlata a stříbra a opět je přidává k již ukrytým zásobám. Byl také kolegy pověřen, aby vyhledal vhodnou důvěryhodnou osobu a té přenechal potřebné informace o jejich pokladu. To proto, kdyby se snad s nimi na pláních něco přihodilo, aby se jejich rodiny dostaly k pokladu. Proto ponechal potřebné údaje v uzamčené skříňce u pana Morrisse. Podle Beala obsahuje prvý zašifrovaný dopis přesné místo, kde je poklad ukryt, druhý je soupis jeho složení a třetí je seznam příbuzných, kteří mají dostat podíl.
Pan Morriss předpokládal, že po tolika letech jsou již pan Beale a jeho přátelé mrtvi, ale přesto chtěl vykonat to, co slíbil. Bez klíče, který slíbeným dopisem nepřišel, nebyl schopen zašifrované dopisy přečíst. Údajně jej to celý život trápilo a ve volných chvílích se snažil dopisy dešifrovat.

1862
Ve věku osmdesáti čtyř let se pan Morriss svěřuje s celým příběhem svému příteli. Muži, jehož identita zůstává utajena. Panu Morrissovi šlo o to, aby byla zachována naděje, že šifry budou vyluštěny a bude splněn slib panu Bealovi, tj. že podíl na pokladu dostanou žijící příbuzní zlatokopů.

1862-1884
V následujících letech se onen neznámý muž snaží vyluštit obsah všech tří zašifrovaných dopisů sám. Daří se mu vyluštit pouze druhý z dopisů. Byl zašifrován pomocí *Deklarace nezávislosti* (originální znění včetně očíslování slov je uvedeno v příloze k článku).

Šifrový text začíná takto: 115, 73, 24, 807, 37, ….

Postup dešifrování je poměrně jednoduchý. Nejprve vyhledáme slova, která jsou určena příslušným pořadovým číslem, v textu *Deklarace nezávislosti*.

instituted (115)
hold (73)
another (24)

into (807)
equal (37)

Následně použijeme z těchto slov pouze prvá písmena a dostaneme hledaný otevřený text:
I haie ….

Celý dešifrovaný text druhého dopisu (v angličtině) naleznete opět v příloze a to za Šifrou č.2.

Poznámka č.1:
Otevřený text správně začíná **I have.** Zde a na dalších místech textu č. 2 jsou chyby, které snad vznikly chybným šifrováním.

Poznámka č.2:
Pro uvedený způsob šifrování/dešifrování se vžil název Bealova knižní šifra. V případě samotné Šifry č. 2 však není „správně použita“. Správně se u této knižní šifry každá šifrová skupina použije pouze jedenkrát. Zmíněná šifrová skupina 37, která nahrazuje otevřený znak E se v Šifře č. 2 vyskytuje 13x. Přitom v *Deklaraci nezávislosti* je dostatek jiných slov, která začínají na E a tedy by mohl být tento znak nahrazen bez problémů pokaždé jinou šifrovou skupinou (např. 7, 33, 37, 49, 79, 85, 89, 138,. ... , 1275, 1313). Takto se z relativně silné šifry (zejména pokud dohodnutý klíčový text není luštitelům dostupný) stává šifra slabší, která je vlastně pouze různě kvalitní variantou homofonní šifry.

1885
Po mnoha letech pokusů se neznámý muž vzdal naděje, že vyluští i šifru č. 1 a č. 3. Celý příběh sepsal a vydává jej ve spolupráci s Jamsem B.Wardem. A to jsme již zase na začátku našeho článku.

Luštění …

Prvními, kteří se Bealovou šifrou dlouhodobě zabývali, byli bratři Hartové. Zkoušeli různé způsoby, jak zbylé dvě šifry rozluštit, ale nepodařilo se jim to. Prvý z bratrů se vzdal marných pokusů v r. 1912, ale druhý pokračoval až do r. 1952.

Jejich následovníkem byl H. Herbert, který se problémem zabýval více jak padesát let a to od r. 1923.

Následovaly pokusy tisíců dalších amatérů…

O rozluštění se nepokoušeli jen amatéři, ale i profesionální kryptologové jako například Herbert O. Yardley nebo William Friedman.

Možným důvodem, proč ještě zbylé dva dokumenty nebyly rozluštěny, může být, že byl použit k zašifrování nějaký jednorázový text tj. text, který byl vytvořen jen k tomuto účelu a měl být zaslán jako klíč panu Morrissovi. Pokud nebude nalezen, nebo byl-li zničen, není prakticky naděje na rozluštění.

Další úvahy vedou k tomu, že možná autor knížky šifru č.1 a č.3 úmyslně pozměnil, neboť doufal, že klíč existuje a ten, kdo jej má k dispozici, jej bude kontaktovat a k pokladu se dostanou společně…

Vyskytly se i názory, že to celé je šikovný podvrh. Kryptolog Luis Kruh provedl textovou srovnávací slohovou analýzu a tvrdí, že text knížky i dopisů vykazuje nenahodilé shody a tudíž je napsal jeden a tentýž člověk a příběh je tedy vymyšlený.

Na druhou stranu existují i různé zajímavé důkazy vnitřních vazeb mezi šifrou č. 1 a *Deklarací nezávislosti*. Kdyby se jednalo o podvrh a autor knihy by šifrové texty jen náhodně vytvořil, pak by zde tato vazba nemohla vzniknout… Např. pokud se použije postup luštění šifry 2 na šifru 1, dostaneme řetězec ABFDEFGHIIJKLMMNOHPP. Takováto „abecední“ sekvence nemůže vzniknout náhodně. V roce 1980 publikoval Jim Gillogly v časopise Cryptologia odhad, ve kterém vypočítává, že takovýto řetězec může vzniknout s pravděpodobnosti 1 : deseti triliónům… (písmenem K začínají v deklaraci nezávislosti jen 4 slova a písmenem J deset slov …) .

Proti pravosti příběhu mluví např. použité slovo „stampede“ (splašený úprk koní), které bylo údajně použito v Bealově dopise v zamčené skřínce. Toto slovo se prý začalo používat později až snad kolem roku 1830…

Zastánce pravosti zastupuje historik Peter Viemeister, který své výzkumy shrnul do knihy *The Beale Treasure - History of a Mystery*. Ten tvrdí, že příběh se odehrává na historickém základu. Například zjistil, že existovalo několik mužů, jejichž životní osudy by nebyly v rozporu s daty uvedenými v knize. Podařilo se mu také například zaznamenat čejenskou legendu, datovanou do roku 1820 o zlatě a stříbře, které bylo odvezeno ze Západu a zakopáno v horách na východě. V poštovním seznamu města St. Luis z roku 1820 nalezl jméno Thomas Beall. Což by mohlo být v souladu s tím, že Beale v tomto městě při své cestě s Lynchburgu pobýval a s tím, že odtud roku 1822 poslal dopis s popisem, co je uloženo v kovové skřínce …

Lze pokračovat dále a dále. Řadu argumentů pro a proti najdete v pracích členů Společnosti Bealových šifer. Najdete zde informace o tom, že ten a ten šifru již téměř rozluštil a našel ty a ty závislosti nebo dokonce, že text rozluštil a poklad vykopal apod.
Přehled některých „řešení“ Bealových šifer najdete např. v [3].

Mimo kryptologů se zabývají hledáním pokladů amatérští i profesionální hledači pokladů. Cena zakopaného pokladu je opravdu lákavá. Odhady se pohybují od dvaceti do třiceti miliónů dolarů.

Tito lidé se snaží ve svých postupech využít informace z druhého, rozluštěného dopisu. Zde je zmínka o tom, že se poklad nalézá asi čtyři míle od Buford´s, a tak předpokládají, že se jedná o obec Buford resp. Bufordovu hospodu blízko města Bedford. Díky tomu sem dodnes přijíždí hledači pokladů, z čehož malé městečko docela dobře prosperuje. Podnikavci jim mimo ubytování nabízí i zapůjčení veškerého potřebného nářadí k hledání pokladu….

Přehled možných řešení

A) Příběh je pravdivý

- Bealovy šifry 1, 3 jsou zašifrovány stejným způsobem jako šifra č.2, ale jako klíč byl použit jiný obecně dostupný text (Bible, slovník, noviny ,…)
- Bealovy šifry 1, 3 jsou zašifrovány stejným způsobem jako šifra č.2, ale jako klíč byl použit unikátní text připravený pouze pro dešifrování, který není dostupný
- Bealovy šifry 1, 3 jsou zašifrovány pomocí *Deklarace nezávislosti*, ale je použito ještě jisté předšifrování nebo přešifrování nebo je použit jiný složitější algoritmus výběru slov / písmen z tohoto textu…
- Bealovy šifry 1, 3 byly úmyslně pozměněny autorem knihy, jenž nechtěl šifrový text s popisem uložení pokladu zveřejnit. Chtěl snad touto cestou jen získat kontakt na případného držitele klíče k dešifrování. Jen autor (vlastník správných šifrových textů) a držitel klíče pak mohou společně poklad najít …
- Bealovy šifry 1, 3 byly již rozluštěny a poklad vybrán (konspirační teorie tvrdí, že tak např. již provedla NSA, CIA apod.)
- Bealovy šifry 1, 3 nebyly rozluštěny, ale poklad byl podle indicií v šifře č.2 a informací v knize nalezen a vykopán

B) Příběh není pravdivý

- Autor (resp. nakladatel) chtěl napsat knihu, která by se dobře prodávala, proto zvolil tuto formu, neboť předpokládal, že by mohl vydělat na zájmu lidí o tajemství a poklady
- Vydání knihy mělo za cíl zvýšit zájem lidí o návštěvu Bedfordu, Lynchburgu…
- Autor napsal knihu pro své potěšení, ale nechtěl ji vydat pod svým „váženým“ jménem a být s ní spojován .

Osobní názor :

- jedná se o hoax

Za všechny bohaté odkazy:

[1] http://unmuseum.org/beal.htm
[2] http://en.wikipedia.org/wiki/Beale_ciphers
[3] http://smd173.tripod.com/Beale/Solutions.htm
[4] Simon Singh: Kniha kódů a šifer, Dokořán, 2003

Přílohy

Šifra č. 1

```
71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16,
111, 95, 84, 341, 975, 14, 40, 64, 27, 81, 139, 213, 63, 90,
1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485, 604, 230, 436,
664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401,
370, 11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94,
73, 416, 918, 263, 28, 500, 538, 356, 117, 136, 219, 27, 176,
```

130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283, 118, 320,
138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61,
304, 12, 21, 24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184,
360, 780, 18, 64, 463, 474, 131, 160, 79, 73, 440, 95, 18, 64,
581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62, 116, 97,
103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150,
59, 568, 614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18,
21, 136, 872, 15, 28, 170, 88, 4, 30, 44, 112, 18, 147, 436,
195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461, 44,
106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38,
416, 89, 71, 216, 728, 965, 818, 2, 38, 121, 195, 14, 326,
148, 234, 18, 55, 131, 234, 361, 824, 5, 81, 623, 48, 961, 19,
26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86,
36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284,
919, 861, 326, 985, 233, 64, 68, 232, 431, 960, 50, 29, 81,
216, 321, 603, 14, 612, 81, 360, 36, 51, 62, 194, 78, 60, 200,
314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464,
895, 10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875,
78, 14, 23, 111, 109, 62, 31, 501, 823, 216, 280, 34, 24, 150,
1000, 162, 286, 19, 21, 17, 340, 19, 242, 31, 86, 234, 140,
607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95,
122, 216, 548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236,
154, 211, 10, 98, 34, 119, 56, 216, 119, 71, 218, 1164, 1496,
1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617, 84, 290,
80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543,
897, 624, 18, 212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418,
16, 140, 230, 460, 538, 19, 27, 88, 612, 1431, 90, 716, 275,
74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132, 40,
102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324,
403, 912, 227, 936, 447, 55, 86, 34, 43, 212, 107, 96, 314,
264, 1065, 323, 428, 601, 203, 124, 95, 216, 814, 2906, 654,
820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41,
17, 84, 221, 736, 820, 214, 11, 60, 760

Šifra č. 2

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140,
47, 29, 107, 79, 84, 56, 239, 10, 26, 811, 5, 196, 308, 85,
52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122, 106, 95, 53,
58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118,
71, 140, 287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12,
47, 43, 59, 807, 45, 316, 101, 41, 78, 154, 1005, 122, 138,
191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196,
81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287,
63, 3, 6, 191, 122, 43, 234, 400, 106, 290, 314, 47, 48, 81,
96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46, 10, 113, 140,
353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37,
105, 28, 248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98,
117, 511, 62, 51, 220, 37, 113, 140, 807, 138, 540, 8, 44,

287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107, 603,
220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61,
52, 33, 30, 5, 38, 8, 14, 84, 57, 540, 217, 115, 71, 29, 84,
63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53, 79, 118, 51,
44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557,
211, 505, 125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205,
140, 344, 26, 811, 138, 115, 48, 73, 34, 205, 316, 607, 63,
220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121, 12,
95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138,
30, 31, 62, 67, 41, 85, 63, 10, 106, 807, 138, 8, 113, 20, 32,
33, 37, 353, 287, 140, 47, 85, 50, 37, 49, 47, 64, 6, 7, 71,
33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94,
511, 2, 270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106,
44, 486, 230, 353, 211, 200, 31, 10, 38, 140, 297, 61, 603,
320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250, 557,
246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250,
10, 15, 35, 106, 160, 113, 31, 102, 406, 230, 540, 320, 29,
66, 33, 101, 807, 138, 301, 316, 353, 320, 220, 37, 52, 28,
540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11,
110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85,
400, 38, 43, 77, 14, 27, 8, 47, 138, 63, 140, 44, 35, 22, 177,
106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25, 44, 48, 7, 26,
46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96,
41, 51, 50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138,
582, 98, 643, 32, 107, 140, 112, 26, 85, 138, 540, 53, 20,
125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150, 112, 71,
14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 33, 21, 95, 220,
511, 102, 811, 30, 83, 84, 305, 620, 15, 2, 10, 8, 220, 106,
353, 105, 106, 60, 275, 72, 8, 50, 205, 185, 112, 125, 540,
65, 106, 807, 138, 96, 110, 16, 73, 33, 807, 150, 409, 400,
50, 154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8, 44,
37, 52, 40, 241, 34, 205, 38, 16, 46, 47, 85, 24, 44, 15, 64,
73, 138, 807, 85, 78, 110, 33, 420, 505, 53, 37, 38, 22, 31,
10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 135,
150, 96, 33, 84, 125, 807, 191, 96, 511, 118, 40, 370, 643,
466, 106, 41, 107, 603, 220, 275, 30, 150, 105, 49, 53, 287,
250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110, 21, 112, 140,
485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4,
25, 42, 8, 16, 811, 125, 160, 32, 205, 603, 807, 81, 96, 405,
41, 600, 136, 14, 20, 28, 26, 353, 302, 246, 8, 131, 160, 140,
84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138, 205, 51, 63,
241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288

Dešifrovaný dopis č. 2

I have deposited in the county of Bedford, about four miles from Buford's, in an excavation or vault, six feet below the surface of the ground, the following articles, belonging jointly to the parties whose names are given in number "3" herewith:

The first deposit consisted of one thousand and fourteen pounds of gold, and three thousand eight hundred and twelve pounds of silver, deposited November, 1819. The second was made December, 1821, and consisted of nineteen hundred and seven pounds of gold, and twelve hundred and eighty-eight pounds of silver; also jewels, obtained in St. Louis in exchange for silver to save transportation, and valued at $13,000.

The above is securely packed in iron pots, with iron covers. The vault is roughly lined with stone, and the vessels rest on solid stone, and are covered with others. Paper number "1" describes the exact locality of the vault so that no difficulty will be had in finding it.

Šifra č. 3

317, 8, 92, 73, 112, 89, 67, 318, 28, 96,107, 41, 631, 78,
146, 397, 118, 98, 114, 246, 348, 116, 74, 88, 12, 65, 32, 14,
81, 19, 76, 121, 216, 85, 33, 66, 15, 108, 68, 77, 43, 24,
122, 96, 117, 36, 211, 301, 15, 44, 11, 46, 89, 18, 136, 68,
317, 28, 90, 82, 304, 71, 43, 221, 198, 176, 310, 319, 81, 99,
264, 380, 56, 37, 319, 2, 44, 53, 28, 44, 75, 98, 102, 37, 85,
107, 117, 64, 88, 136, 48, 151, 99, 175, 89, 315, 326, 78, 96,
214, 218, 311, 43, 89, 51, 90, 75, 128, 96, 33, 28, 103, 84,
65, 26, 41, 246, 84, 270, 98, 116, 32, 59, 74, 66, 69, 240,
15, 8, 121, 20, 77, 89, 31, 11, 106, 81, 191, 224, 328, 18,
75, 52, 82, 117, 201, 39, 23, 217, 27, 21, 84, 35, 54, 109,
128, 49, 77, 88, 1, 81, 217, 64, 55, 83, 116, 251, 269, 311,
96, 54, 32, 120, 18, 132, 102, 219, 211, 84, 150, 219, 275,
312, 64, 10, 106, 87, 75, 47, 21, 29, 37, 81, 44, 18, 126,
115, 132, 160, 181, 203, 76, 81, 299, 314, 337, 351, 96, 11,
28, 97, 318, 238, 106, 24, 93, 3, 19, 17, 26, 60, 73, 88, 14,
126, 138, 234, 286, 297, 321, 365, 264, 19, 22, 84, 56, 107,
98, 123, 111, 214, 136, 7, 33, 45, 40, 13, 28, 46, 42, 107,
196, 227, 344, 198, 203, 247, 116, 19, 8, 212, 230, 31, 6,
328, 65, 48, 52, 59, 41, 122, 33, 117, 11, 18, 25, 71, 36, 45,
83, 76, 89, 92, 31, 65, 70, 83, 96, 27, 33, 44, 50, 61, 24,
112, 136, 149, 176, 180, 194, 143, 171, 205, 296, 87, 12, 44,
51, 89, 98, 34, 41, 208, 173, 66, 9, 35, 16, 95, 8, 113, 175,
90, 56, 203, 19, 177, 183, 206, 157, 200, 218, 260, 291, 305,
618, 951, 320, 18, 124, 78, 65, 19, 32, 124, 48, 53, 57, 84,
96, 207, 244, 66, 82, 119, 71, 11, 86, 77, 213, 54, 82, 316,
245, 303, 86, 97, 106, 212, 18, 37, 15, 81, 89, 16, 7, 81, 39,
96, 14, 43, 216, 118, 29, 55, 109, 136, 172, 213, 64, 8, 227,
304, 611, 221, 364, 819, 375, 128, 296, 1, 18, 53, 76, 10, 15,
23, 19, 71, 84, 120, 134, 66, 73, 89, 96, 230, 48, 77, 26,
101, 127, 936, 218, 439, 178, 171, 61, 226, 313, 215, 102, 18,
167, 262, 114, 218, 66, 59, 48, 27, 19, 13, 82, 48, 162, 119,
34, 127, 139, 34, 128, 129, 74, 63, 120, 11, 54, 61, 73, 92,
180, 66, 75, 101, 124, 265, 89, 96, 126, 274, 896, 917, 434,
461, 235, 890, 312, 413, 328, 381, 96, 105, 217, 66, 118, 22,

```
77, 64, 42, 12, 7, 55, 24, 83, 67, 97, 109, 121, 135, 181,
203, 219, 228, 256, 21, 34, 77, 319, 374, 382, 675, 684, 717,
864, 203, 4, 18, 92, 16, 63, 82, 22, 46, 55, 69, 74, 112, 134,
186, 175, 119, 213, 416, 312, 343, 264, 119, 186, 218, 343,
417, 845, 951, 124, 209, 49, 617, 856, 924, 936, 72, 19, 28,
11, 35, 42, 40, 66, 85, 94, 112, 65, 82, 115, 119, 236, 244,
186, 172, 112, 85, 6, 56, 38, 44, 85, 72, 32, 47, 63, 96, 124,
217, 314, 319, 221, 644, 817, 821, 934, 922, 416, 975, 10, 22,
18, 46, 137, 181, 101, 39, 86, 103, 116, 138, 164, 212, 218,
296, 815, 380, 412, 460, 495, 675, 820, 952
```

Klíč k dešifrování dopisu č.2

DECLARATION OF INDEPENDENCE

When(1) in(2) the(3) course(4) of(5) human(6) events(7) it(8) becomes(9) necessary(10) for(11) one(12) people(13) to(14) dissolve(15) the(16) political(17) bands(18) which(19) have(20) connected(21) them(22) with(23) another(24) and(25) to(26) assume(27) among(28) the(29) powers(30) of(31) the(32) earth(33) the(34) separate(35) and(36) equal(37) station(38) to(39) which(40) the(41) laws(42) of(43) nature(44) and(45) of(46) nature's(47) god(48) entitle(49) them(50) a(51) decent(52) respect(53) to(54) the(55) opinions(56) of(57) mankind(58) requires(59) that(60) they(61) should(62) declare(63) the(64) causes(65) which(66) impel(67) them(68) to(69) the(70) separation(71) we(72) hold(73) these(74) truths(75) to(76) be(77) self(78) evident(79) that(80) all(81) men(82) are(83) created(84) equal(85) that(86) they(87) are(88) endowed(89) by(90) their(91) creator(92) with(93) certain(94) unalienable(95) rights(96) that(97) among(98) these(99) are(100) life(101) liberty(102) and(103) the(104) pursuit(105) of(106) happiness(107) that(108) to(109) secure(110) these(111) rights(112) governments(113) are(114) instituted(115) among(116) men(117) deriving(118) their(119) just(120) powers(121) from(122) the(123) consent(124) of(125) the(126) governed(127) that(128) whenever(129) any(130) form(131) of(132) government(133) becomes(134) destructive(135) of(136) these(137) ends(138) it(139) is(140) the(141) right(142) of(143) the(144) people(145) to(146) alter(147) or(148) to(149) abolish(150) it(151) and(152) to(153) institute(154) new(155) government(156) laying(157) its(158)foundation(159) on(160) such(161) principles(162) and(163) organizing(164) its(165) powers(166) in(167) such(168) form(169) as(170) to(171) them(172) shall(173) seem(174) most(175) likely(176) to(177) effect(178) their(179) safety(180) and(181) happiness(182) prudence(183) indeed(184) will(185) dictate(186) that(187) governments(188) long(189) established(190) should(191) not(192) be(193) changed(194) for(195) light(196) and(197) transient(198) causes(199) and(200) accordingly(201) all(202) experience(203) hath(204) shown(205) that(206) mankind(207) are(208) more(209) disposed(210) to(211) suffer(212) while(213) evils(214) are(215) sufferable(216) than(217) to(218) right(219) themselves(220) by(221) abolishing(222) the(223) forms(224) to(225) which(226) they(227) are(228) accustomed(229) but(230) when(231) a(232) long(233) train(234) of(235) abuses(236) and(237) usurpations(238) pursuing(239) invariably(240) the(241) same(242) object(243) evinces(244) a(245) design(246) to(247) reduce(248) them(249) under(250) absolute(251) despotism(252) it(253) is(254) their(255) right(256) it(257) is(258) their(259) duty(260) to(261) throw(262) off(263) such(264) government(265) and(266) to(267) provide(268) new(269) guards(270) for(271) their(272) future(273) security(274) such(275) has(276)

been(277) the(278) patient(279) sufferance(280) of(281) these(282) colonies(283) and(284) such(285) is(286) now(287) the(288) necessity(289) which(290) constrains(291) them(292) to(293) alter(294) their(295) former(296) systems(297) of(298) government(299) the(300) history(301) of(302) the(303) present(304) king(305) of(306) great(307) Britain(308) is(309) a(310) history(311) of(312) repeated(313) injuries(314) and(315) usurpations(316) all(317) having(318) in(319) direct(320) object(321) the(322) establishment(323) of(324) an(325) absolute(326) tyranny(327) over(328) these(329) states(330) to(331) prove(332) this(333) let(334) facts(335) be(336) submitted(337) to(338) a(339) candid(340) world(341) he(342) has(343) refused(344) his(345) assent(346) to(347) laws(348) the(349) most(350) wholesome(351) and(352) necessary(353) for(354) the(355) public(356) good(357) he(358) has(359) forbidden(360) his(361) governors(362) to(363) pass(364) laws(365) of(366) immediate(367) and(368) pressing(369) importance(370) unless(371) suspended(372) in(373) their(374) operation(375) till(376) his(377) assent(378) should(379) be(380) obtained(381) and(382) when(383) so(384) suspended(385) he(386) has(387) utterly(388) neglected(389) to(390) attend(391) to(392) them(393) he(394) has(395) refused(396) to(397) pass(398) other(399) laws(400) for(401) the(402) accommodation(403) of(404) large(405) districts(406) of(407) people(408) unless(409) those(410) people(411) would(412) relinquish(413) the(414) right(415) of(416) representation(417) in(418) the(419) legislature(420) a(421) right(422) inestimable(423) to(424) them(425) and(426) formidable(427) to(428) tyrants(429) only(430) he(431) has(432) called(433) together(434) legislative(435) bodies(436) at(437) places(438) unusual(439) uncomfortable(440) and(441) distant(442) from(443) the(444) depository(445) of(446) their(447) public(448) records(449) for(450) the(451) sole(452) purpose(453) of(454) fatiguing(455) them(456) into(457) compliance(458) with(459) his(460) measures(461) he(462) has(463) dissolved(464) representative(465) houses(466) repeatedly(467) for(468) opposing(469) with(470) manly(471) firmness(472) his(473) invasions(474) on(475) the(476) rights(477) of(478) the(479) people(480) he(481) has(482) refused(483) for(484) a(485) long(486) time(487) after(488) such(489) dissolutions(490) to(491) cause(492) others(493) to(494) be(495) elected(496) whereby(497) the(498) legislative(499) powers(500) incapable(501) of(502) annihilation(503) have(504) returned(505) to(506) the(507) people(508) at(509) large(510) for(511) their(512) exercise(513) the(514) state(515) remaining(516) in(517) the(518) meantime(519) exposed(520) to(521) all(522) the(523) dangers(524) of(525) invasion(526) from(527) without(528) and(529) convulsions(530) within(531) he(532) has(533) endeavored(534) to(535) prevent(536) the(537) population(538) of(539) these(540) states(541) for(542) that(543) purpose(544) obstructing(545) the(546) laws(547) for(548) naturalization(549) of(550) foreigners(551) refusing(552) to(553) pass(554) others(555) to(556) encourage(557) their(558) migration(559) hither(560) and(561) raising(562) the(563) conditions(564) of(565) new(566) appropriations(567) of(568) lands(569) he(570) has(571) obstructed(572) the(573) administration(574) of(575) justice(576) by(577) refusing(578) his(579) assent(580) to(581) laws(582) for(583) establishing(584) judiciary(585) powers(586) he(587) has(588) made(589) judges(590) dependent(591) on(592) his(593) will(594) alone(595) for(596) the(597) tenure(598) of(599) their(600) offices(601) and(602) the(603) amount(604) and(605) payment(606) of(607) their(608) salaries(609) he(610) has(611) erected(612) a(613) multitude(614) of(615) new(616) offices(617) and(618) sent(619) hither(620) swarms(621) of(622) officers(623) to(624) harass(625) our(626) people(627) and(628) eat(629) out(630) their(631) substance(632) he(633) has(634) kept(635) among(636) us(637) in(638) times(639) of(640) peace(641) standing(642) armies(643) without(644) the(645) consent(646) of(647) our(648) legislatures(649) he(650) has(651) affected(652) to(653) render(654) the(655) military(656) independent(657) of(658) and(659) superior(660) to(661) the(662) civil(663) power(664) he(665) has(666) combined(667) with(668) others(669) to(670) subject(671) us(672) to(673)

a(674) jurisdiction(675) foreign(676) to(677) our(678) constitution(679) and(680) unacknowledged(681) by(682) our(683) laws(684) giving(685) his(686) assent(687) to(688) their(689) acts(690) of(691) pretended(692) legislation(693) for(694) quartering(695) large(696) bodies(697) of(698) armed(699) troops(700) among(701) us(702) for(703) protecting(704) them(705) by(706) a(707) mock(708) trial(709) from(710) punishment(711) for(712) any(713) murders(714) which(715) they(716) should(717) commit(718) on(719) the(720) inhabitants(721) of(722) these(723) states(724) for(725) cutting(726) off(727) our(728) trade(729) with(730) all(731) parts(732) of(733) the(734) world(735) for(736) imposing(737) taxes(738) on(739) us(740) without(741) our(742) consent(743) for(744) depriving(745) us(746) in(747) many(748) cases(749) of(750) the(751) benefits(752) of(753) trial(754) by(755) jury(756) for(757) transporting(758) us(759) beyond(760) seas(761) to(762) be(763) tried(764) for(765) pretended(766) offenses(767) for(768) abolishing(769) the(770) free(771) system(772) of(773) English(774) laws(775) in(776) a(777) neighboring(778) province(779) establishing(780) therein(781) an(782) arbitrary(783) government(784) and(785) enlarging(786) its(787) boundaries(788) so(789) as(790) to(791) render(792) it(793) at(794) once(795) an(796) example(797) and(798) fit(799) instrument(800) for(801) introducing(802) the(803) same(804) absolute(805) rule(806) into(807) these(808) colonies(809) for(810) taking(811) away(812) our(813) charters(814) abolishing(815) our(816) most(817) valuable(818) laws(819) and(820) altering(821) fundamentally(822) the(823) forms(824) of(825) our(826) governments(827) for(828) suspending(829) our(830) own(831) legislature(832) and(833) declaring(834) themselves(835) invested(836) with(837) power(838) to(839) legislate(840) for(841) us(842) in(843) all(844) cases(845) whatsoever(846) he(847) has(848) abdicated(849) government(850) here(851) by(852) declaring(853) us(854) out(855) of(856) his(857) protection(858) and(859) waging(860) war(861) against(862) us(863) he(864) has(865) plundered(866) our(867) seas(868) ravaged(869) our(870) coasts(871) burnt(872) our(873) towns(874) and(875) destroyed(876) the(877) lives(878) of(879) our(880) people(881) he(882) is(883) at(884) this(885) time(886) transporting(887) large(888) armies(889) of(890) foreign(891) mercenaries(892) to(893) complete(894) the(895) works(896) of(897) death(898) desolation(899) and(900) tyranny(901) already(902) begun(903) with(904) circumstances(905) of(906) cruelty(907) and(&)(908) perfidy(909) scarcely(910) paralleled(911) in(912) the(913) most(914) barbarous(915) ages(916) and(917) totally(918) unworthy(919) the(920) head(921) of(922) a(923) civilized(924) nation(925) he(926) has(927) constrained(928) our(929) fellow(930) citizens(931) taken(932) captive(933) on(934) the(935) high(936) seas(937) to(938) bear(939) arms(940) against(941) their(942) country(943) to(944) become(945) the(946) executioners(947) of(948) their(949) friends(950) and(951) brethren(952) or(953) to(954) fall(955) themselves(956) by(957) their(958) hands(959) he(960) has(961) excited(962) domestic(963) insurrections(964) amongst(965) us(966) and(967) has(968) endeavored(969) to(970) bring(971) on(972) the(973) inhabitants(974) of(975) our(976) frontiers(977) the(978) merciless(979) Indian(980) savages(981) whose(982) known(983) rule(984) of(985) warfare(986) is(987) an(988) undistinguished(989) destruction(990) of(991) all(992) ages(993) sexes(994) and(995) conditions(996) in(997) every(998) stage(999) of(1000) these(1001) oppressions(1002) we(1003) have(1004) petitioned(1005) for(1006) redress(1007) in(1008) the(1009) most(1010) humble(1011) terms(1012) our(1013) repeated(1014) petitions(1015) have(1016) been(1017) answered(1018) only(1019) by(1020) repeated(1021) injury(1022) a(1023) prince(1024) whole(1025) character(1026) is(1027) thus(1028) marked(1029) by(1030) every(1031) act(1032) which(1033) may(1034) define(1035) a(1036) tyrant(1037) is(1038) unfit(1039) to(1040) be(1041) the(1042) ruler(1043) of(1044) a(1045) free(1046) people(1047) nor(1048) have(1049) we(1050) been(1051) wanting(1052) in(1053)

attention(1054) to(1055) our(1056) British(1057) brethren(1058) we(1059) have(1060) warned(1061) them(1062) from(1063) time(1064) to(1065) time(1066) of(1067) attempts(1068) by(1069) their(1070) legislature(1071) to(1072) extend(1073) an(1074) unwarrantable(1075) jurisdiction(1076) over(1077) us(1078) we(1079) have(1080) reminded(1081) them(1082) of(1083) the(1084) circumstances(1085) of(1086) our(1087) emigration(1088) and(1089) settlement(1090) here(1091) we(1092) have(1093) appealed(1094) to(1095) their(1096) native(1097) justice(1098) and(1099) magnanimity(1100) and(1101) we(1102) have(1103) conjured(1104) them(1105) by(1106) the(1107) ties(1108) of(1109) our(1110) common(1111) kindred(1112) to(1113) disavow(1114) these(1115) usurpations(1116) which(1117) would(1118) inevitably(1119) interrupt(1120) our(1121) connections(1122) and(1123) correspondence(1124) they(1125) too(1126) have(1127) been(1128) deaf(1129) to(1130) the(1131) voice(1132) of(1133) justice(1134) and(1135) of(1136) consanguinity(1137) we(1138) must(1139) therefore(1140) acquiesce(1141) in(1142) the(1143) necessity(1144) which(1145) denounces(1146) our(1147) separation(1148) and(1149) hold(1150) them(1151) as(1152) we(1153) hold(1154) the(1155) rest(1156) of(1157) mankind(1158) enemies(1159) in(1160) war(1161) in(1162) peace(1163) friends(1164) we(1165) therefore(1166) the(1167) representatives(1168) of(1169) the(1170) united(1171) states(1172) of(1173) America(1174) in(1175) general(1176) congress(1177) assembled(1178) appealing(1179) to(1180) the(1181) supreme(1182) judge(1183) of(1184) the(1185) world(1186) for(1187) the(1188) rectitude(1189) of(1190) our(1191) intentions(1192) do(1193) in(1194) the(1195) name(1196) and(1197) by(1198) authority(1199) of(1200) the(1201) good(1202) people(1203) of(1204) these(1205) colonies(1206) solemnly(1207) publish(1208) and(1209) declare(1210) that(1211) these(1212) united(1213) colonies(1214) are(1215) and(1216) of(1217) right(1218) ought(1219) to(1220) be(1221) free(1222) and(1223) independent(1224) states(1225) that(1226) they(1227) are(1228) absolved(1229) from(1230) all(1231) allegiance(1232) to(1233) the(1234) British(1235) crown(1236) and(1237) that(1238) all(1239) political(1240) connection(1241) between(1242) them(1243) and(1244) the(1245) state(1246) of(1247) great(1248) Britain(1249) is(1250) and(1251) ought(1252) to(1253) be(1254) totally(1255) dissolved(1256) and(1257) that(1258) as(1259) free(1260) and(1261) independent(1262) states(1263) they(1264) have(1265) full(1266) power(1267) to(1268) levy(1269) war(1270) conclude(1271) peace(1272) contract(1273) alliances(1274) establish(1275) commerce(1276) and(1277) to(1278) do(1279) all(1280) other(1281) acts(1282) and(1283) things(1284) which(1285) independent(1286) states(1287) may(1288) of(1289) right(1290) do(1291) and(1292) for(1293) the(1294) support(1295) of(1296) this(1297) declaration(1298) with(1299) a(1300) firm(1301) reliance(1302) on(1303) the(1304) protection(1305) of(1306) divine(1307) providence(1308) we(1309) mutually(1310) pledge(1311) to(1312) each(1313) other(1314) our(1315) lives(1316) our(1317) fortunes(1318) and(1319) our(1320) sacred(1321) honor(1322) .

D. O čem jsme psali v květnu 2000 – 2006

Crypto-World 5/2000

+ příloha : J.Hrubý , soubor QNG.PS

Crypto-World 5/2001

Příloha : priloha.zip : součástí jsou soubory obsah.rtf (obsah všech dosud vyšlých e-zinů Crypto-World) a mystery.mid (viz. článek "Záhadná páska z Prahy")

Crypto-World 5/2002

Příloha: SBKS 2002 - výzva pro autory cfp.pdf

Crypto-World 5/2003

Crypto-World 5/2004

Crypto-World 5/2005

Příloha : zpráva vysílaná radioamatérskou stanicí GB2HQ - nedele_30m.wav

Crypto-World 5/2006

E. 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/