Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 8, číslo 1/2006 **15. leden 2006**

1/2006

Připravil: Mgr. Pavel Vondruška
Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1075 registrovaných odběratelů)

Obsah : str.

A. Elektronická fakturace (přehled některých požadavků)

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

V EU, ale i v ČR, se postupně začíná používat elektronická fakturace, při níž předávané doklady mohou existovat pouze v elektronické podobě a mohou sloužit jako plnohodnotné daňové doklady. Tento přístup se však prosazuje velmi pomalu a to bez ohledu na to, že subjektům, které jej používají, přináší řadu významných výhod. Jmenujme především snížení nákladů na přenos, vyšší rychlost zpracování, nižší chybovost a snížení nákladů při zadávání do účetního systému, nižší náklady na archivaci (snížení nákladů na údržbu a provoz klasického archivu). Důvodem pomalého zavádění byla především nejasnost národní legislativy, nedůvěra v tento druh komunikace a také klasická neochota podstoupit riziko být jeden z prvních, kdo takto bude postupovat (co na to daňový úřad?). SPIS (sdružení pro informační systémy) se již v roce 2003 pokusil upozornit, že elektronická fakturace je i za stavu tehdejší legislativy možná. Následně se aktivně podílel na připomínkách, které vedly k upřesnění zákona o DPH. Poslední úprava zákona o DPH vstoupila v platnost 1.10.2005. Osobně se domnívám, že aktuální legislativa proces elektronické fakturace (tj. předání elektronické faktury, archivace, prokazování důvěryhodnosti původu) upravuje dostatečně a tento proces je plně ve shodě s požadavky EU. Článek je pouze velmi stručným výběrem některých požadavků (citací z konkrétních právních předpisů) na tento proces a to jak z pohledu obecných pravidel Evropské unie (odstavec 1), naší národní legislativy (odstavec 2), tak i z hlediska možnosti využití elektronické fakturace v některých vybraných členských zemích (závěrečný odstavec 3).

1. Právní rámec na úrovni práva Evropských společenství

1.1 Směrnice Rady 2001/115/ES

Základním dokladem je Směrnice Rady 2001/115/ES ze dne 20. prosince 2001 měnící Směrnici 77/388/EHS s cílem zjednodušit, modernizovat a harmonizovat podmínky stanovené pro fakturaci v případě daně z přidané hodnoty. Podívejme se na některé nejdůležitější teze:

*Faktury mohou být odeslány v papírové formě nebo elektronicky v případě, že **zákazník** je schopen elektronickou verzi faktury přijmout elektronickými prostředky.*

*Faktury odeslané elektronickými prostředky budou přijaty **členskými státy (tj. i jejich finančnímu úřady na základě prováděcího zákona)** v případě zaručení pravosti původu a integrity obsahu těchto faktur:*

- *prostřednictvím zaručeného elektronického podpisu ve smyslu článku 2(2) Směrnice 1999/93/ES Evropského parlamentu a Rady ze dne 13. prosince 1999 o společném rámci pro elektronické podpisy (9). Členské státy mohou požadovat, aby elektronický podpis byl založen na kvalifikované certifikaci a vytvořen bezpečným nástrojem tvorby podpisu ve smyslu článku 2(6) a (10) zmíněné směrnice,nebo*

- *prostřednictvím elektronické výměny dat (EDI) podle článku 2 Doporučení Komise 1994/820/ES ze dne 19. října 1994 vztahující se k právním aspektům elektronické výměny dat (10), kde dohoda o výměně předkládá postupy zaručující autenticitu původu a integritu dat*

Autenticita původu a integrita obsahu faktur stejně tak jako jejich čitelnost musí být zaručena během celého období úchovy. Údaje faktur nesmí být měněny a musí zůstat čitelné po celé období stanovené pro úchovu.

Členské státy určí časové období, po které musí osoby podléhající dani uchovávat faktury za zboží nebo služby dodané na jejich území a faktury přijaté osobami podléhajícími dani usazenými na jejich území

Pro zajištění plnění výše uvedených podmínek **mohou** členské státy vyžadovat uchovávání faktur v původní formě odeslání, tj. papírové či elektronické.

U faktur uchovávaných elektronicky mohou dále požadovat uchovávání údajů zaručujících autenticitu původu a integritu obsahu faktur.

Přenos nebo úchova faktur „elektronickými prostředky" znamená přenos nebo zpřístupnění a úchovu faktur příjemci s použitím elektronického zařízení pro zpracování (včetně digitální komprese), úchovu dat, použití telegrafu, radiového přenosu, optických a jiných elektromagnetických prostředků.

1.2 Doporučení Komise 1994/820/ES ze dne 19. října 1994 o právních aspektech elektronické výměny informací.

EDI komunikace, která je v předchozí Směrnici výslovně zmíněna jako metoda vhodná pro přenos elektronických faktur, je upravena a popsána zejména v tomto doporučení z roku 1994. Jako příloha je v tomto doporučení uveden formulář Evropské vzorové dohody o elektronické výměně dat a komentář k této dohodě. Všem, kteří EDI používají, doporučuji použít text této dohody.

1.3 Směrnice 1999/93/ES Evropského parlamentu a Rady ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy

Uvedená směrnice je u nás dostatečně známa. Náš zákon o elektronické fakturaci z ní vychází a je s ní kompatibilní. Pojmy této Směrnice jsou zavedeny i v našem zákoně a procesy, která tato Směrnice předpokládá, jsou u nás zavedeny a upraveny (zaručený elektronický podpis, kvalifikovaný certifikát, oznámení o vydávání kvalifikovaných certifikátů, akreditace, bezpečné nástroje pro elektronický podpis …)

II. Úprava v platném právním řádu České republiky

2.1 Zákon o DPH

Nejdůležitějším předpisem, který tuto oblast upravuje, je pochopitelně zákona o dani z přidané hodnoty č.235/2004 Sb.. Ten zákon byl naposledy novelizován zákonem č. 377/2005 Sb. (zákon o finančních konglomerátech). Tato nepřímá novela upřesňuje podmínky vystavování a uchovávání daňových dokladů podle tohoto zákona přesným odkazem na zákon o elektronickém podpisu, včetně určení druhu takového podpisu.

Stav po novele zákonem č. 377/2005 (účinnost od 1.října 2005)

§ 26 Vystavování daňových dokladů

(3) Plátce, který uskutečňuje zdanitelné plnění nebo plnění osvobozené od daně s nárokem na odpočet daně, může zplnomocnit k vystavení daňového dokladu svým jménem

a) osobu, pro kterou se zdanitelné plnění nebo plnění osvobozené od daně s nárokem na odpočet daně uskutečňuje, pokud se plátce, který zdanitelné plnění nebo plnění osvobozené od daně s nárokem na odpočet daně uskutečňuje, písemně zaváže, že přijme všechny takto vystavené daňové doklady, nebo
b) třetí osobu.

(4) Daňový doklad může být vystaven se souhlasem osoby, pro kterou se uskutečňuje zdanitelné plnění nebo plnění osvobozené od daně s nárokem na odpočet daně, i v elektronické podobě, pokud jej plátce nebo osoba uvedená v odstavci 3 opatřila zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu nebo elektronickou značkou založenou na kvalifikovaném systémovém certifikátu podle zvláštního právního předpisu[20] nebo pokud je zaručena věrohodnost původu a neporušitelnost obsahu daňového dokladu elektronickou výměnou informací (EDI)[21] .

§ 27 Uchovávání daňových dokladů

(2) Daňový doklad v písemné formě lze převést do elektronické podoby a uchovávat pouze v této podobě, pokud metoda použitá pro převod a uchování zaručuje věrohodnost původu, a pokud je daňový doklad převedený do elektronické podoby opatřen zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu[20] nebo označen elektronickou značkou založenou na kvalifikovaném systémovém certifikátu[20] osoby odpovědné za jeho převod.

§ 30 Daňové doklady při dovozu a vývozu zboží

(5) Pokud je celní prohlášení podáno plátcem se souhlasem celního orgánu elektronicky, musí být opatřeno zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu, který byl vydán akreditovaným poskytovatelem certifikačních služeb, podle zvláštního právního předpisu[20], nebo označeno elektronickou značkou založenou na kvalifikovaném systémovém certifikátu, který byl vydán akreditovaným poskytovatelem certifikačních služeb[20].

2.2 Zákon o účetnictví

Také zákon o účetnictví č. 563/1991 umožňuje, aby účetnictví i jednotlivé účetní doklady v čistě elektronické podobě byly nejen vyhotovovány (§ 11 a § 33/2)b) ZÚ), ale i uchovávány (§ 31/2 ZÚ). Takové dokumenty nemusejí být čitelné bez dalšího, pokud účetní jednotka

[20] *Zákon č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů.*
[21] *Čl. 2 Doporučení komise 1994/820/ES ze dne 19. října 1994 o právních aspektech elektronické výměny informací."*

disponuje vybavením, které dokument učiní čitelným (§ 33/2,6 ZÚ). Účetní záznam musí být podepsán, byť i elektronickým podpisem, splňuje-li jeho technická podoba požadavek průkaznosti (§ 33a/4,5 ZÚ).

§ 11 Účetní doklady

(1) Účetní doklady jsou průkazné účetní záznamy, které musí obsahovat
…
f) podpisový záznam podle § 33a odst. 4 osoby odpovědné za účetní případ a podpisový záznam osoby odpovědné za jeho zaúčtování.

§ 31 Uchovávání účetních dokladů

(1) Účetní jednotky jsou povinny uschovávat účetní záznamy pro účely vedení účetnictví po dobu stanovenou v odstavci 2 nebo 3. Nestanoví-li tento zákon jinak, platí pro nakládání s nimi zvláštní právní předpisy[28].

§ 33 Účetní záznam
…
(2) Účetní záznam může mít písemnou nebo technickou formu. Pro účely tohoto zákona se považuje za

a) písemnou formu účetní záznam provedený rukopisem, psacím strojem, tiskařskými nebo reprografickými technikami anebo tiskovým výstupním zařízením výpočetní techniky, jehož obsah je pro fyzickou osobu čitelný,

b) technickou formu účetní záznam provedený elektronickým, optickým nebo jiným způsobem nespadajícím pod písmeno a), který umožňuje jeho převedení do formy, v níž je jeho obsah pro fyzickou osobu čitelný.
…

(6) Účetní jednotky mohou vést účetní záznamy i ve formě, ve které je jejich obsah bez dalšího nečitelný; v tomto případě jsou povinny disponovat takovými prostředky, nosiči a vybavením (§ 4 odst. 10), které umožní provést převod účetních záznamů do formy, ve které je jejich obsah pro fyzickou osobu čitelný. Pro potřeby ověřování účetní závěrky auditorem (§ 20), jejího zveřejňování (§ 21a) a pro potřeby orgánů podle § 37 odst. 3 jsou účetní jednotky povinny na požádání umožnit oprávněným osobám seznámit se s obsahem jimi určených účetních záznamů v uvedené formě. Tyto povinnosti mají účetní jednotky po dobu, po kterou jsou povinny vést nebo uschovávat uvedené účetní záznamy. Stanovení těchto povinností na smluvním základě není dotčeno.
…
(8) Účetní jednotky jsou povinny zajistit ochranu účetních záznamů a jejich obsahu, použitých technických prostředků, nosičů informací a programového vybavení před jejich zneužitím, poškozením, zničením, neoprávněnou změnou či přístupem k nim, ztrátou nebo odcizením.

[28] Zákon č. 97/1974 Sb. , o archivnictví, ve znění pozdějších předpisů . Poznámka : Tento zákon byl nahrazen zákonem č. 499/2004 Sb. o archivnictví a spisové službě (aniž by byla novelizován odkaz v zákoně o účetnictví)

§ 33a Průkaznost účetního záznamu
…
(4) Podpisovým záznamem se rozumí účetní záznam, jehož obsahem je vlastnoruční podpis nebo elektronický podpis podle zvláštního právního předpisu [30a] anebo obdobný průkazný účetní záznam v technické formě. Na obě formy podpisového záznamu se přitom pohlíží stejně a obě mohou být použity na místě, kde se vyžaduje vlastnoruční podpis.

(5) Připojením podpisového záznamu se rozumí u účetního záznamu v písemné formě jeho podepsání vlastnoručním podpisem, u účetního záznamu v technické formě jeho podepsání elektronickým podpisem podle zvláštního právního předpisu[30a] anebo obdobným průkazným účetním záznamem v technické formě.

§ 34 Přenos účetního záznamu

(1) Přenos účetního záznamu může být uskutečněn pouze prostřednictvím informačního systému nebo jiným způsobem, který splňuje požadavky průkaznosti a dále požadavky ochrany a bezpečnosti odpovídající charakteru přenášených informací podle zvláštních právních předpisů.[31]

(2) Požadavky průkaznosti a jiné požadavky uvedené v odstavci 1 jsou splněny i v případě, je-li přenos účetního záznamu uskutečněn prostřednictvím třetí osoby odlišné od účetních jednotek, pokud tato osoba splňuje požadavky podle zvláštních právních předpisů. [31]

2.3 Zákon o elektronickém podpisu

Úplné znění tohoto předoisu je Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb. a zákonem č. 440/2004 Sb.

Následující pojmy se vyskytují v bodě 2.1 a 2.2, a proto uvádíme jejich přesné vymezení dané aktuálním znění zákona.

§ 2 Vymezení některých pojmů

b) zaručeným elektronickým podpisem elektronický podpis, který splňuje následující požadavky
1. je jednoznačně spojen s podepisující osobou,
2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,

---

[30a] Zákon č. 227/2000 Sb. , o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů

[31] Zákon č. 227/2000 Sb. , o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů

c) elektronickou značkou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky
1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,
2. byly vytvořeny a připojeny k datové zprávě pomocí prostředku pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,

l) kvalifikovaným certifikátem certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb,

m) kvalifikovaným systémovým certifikátem certifikát, který má náležitosti podle § 12a a byl vydán kvalifikovaným poskytovatelem certifikačních služeb,

i) kvalifikovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen „kvalifikované certifikační služby“) a splnil ohlašovací povinnost podle § 6.

III. Přehled požadavků na proces elektronické fakturace v jednotlivých vybraných členských státech EU

Země	Nutný předchozí souhlas daňového úřadu	Výměna elektronických faktur (možnosti)	Archivace (doba, možnost archivace u třetí strany, lze mimo území státu, je vyžadováno potvrzení?)
Česká republika	Ne	EDI Zaručený elektronický podpis (Vyžadován kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát)	10 let Třetí strana Na i mimo území státu bez potvrzení
Španělsko	Ne	**EDI (+elektronický podpis)** Zaručený elektronický podpis (Vyžadován kvalifikovaný certifikát)	4 let Třetí strana Mimo území státu Papírová forma
Itálie	Ne	EDI Zaručený elektronický podpis (Vyžadován kvalifikovaný certifikát + časové razítko + jedenkrát ročně v tištěné podobě dokument o tom, co je archivováno)	10 let Třetí strana Mimo území státu Bez potvrzení

Německo	Ano	EDI Zaručený elektronický podpis (Vyžadován kvalifikovaný certifikát)	10 let Třetí strana Mimo území státu Bez potvrzení
Rakousko	Ne	EDI Zaručený elektronický podpis (je určena odpovědná osoba, která vlastní certifikát)	10 let Třetí strana Mimo území státu Bez potvrzení
Velká Británie	Ano	EDI Zaručený elektronický podpis (Není vyžadován kvalifikovaný certifikát) Subjekty musí být ke komunikace autorizovány	6 let Třetí strana Mimo území státu Bez potvrzení
Belgie	Ano	EDI Zaručený elektronický podpis (Není vyžadován kvalifikovaný certifikát)	10 let Třetí strana Mimo území státu Potvrzení
Francie	Ano (do konce roku 2005)	EDI Zaručený elektronický podpis (Není vyžadován kvalifikovaný certifikát)	7 let Třetí strana Mimo území státu Potvrzení
Irsko	Ne	EDI Zaručený elektronický podpis (Není vyžadován kvalifikovaný certifikát) Další doplňující požadavky	6 let Třetí strana Mimo území státu Bez potvrzení
Nizozemí	Ne	EDI Zaručený elektronický podpis (Není vyžadován kvalifikovaný certifikát)	7 let Třetí strana Mimo území státu Potvrzení
Lucembursko	Ne	EDI Zaručený elektronický podpis (Není vyžadován kvalifikovaný certifikát)	10 let Třetí strana Mimo území státu Potvrzení
Norsko	Ne	Žádné specifické požadavky nejsou vyžadovány	10 let Třetí strana Na území státu

B. Biometrie a kryptografie. Pár poznámek.

Ing. Jaroslav Pinkava, CSc., Zoner software s.r.o. (Jaroslav.Pinkava@zoner.cz)

1. Úvod

Přečtení článku [4] mě přivedlo k některým otázkám. Jak to tedy vlastně se vztahem biometrie a kryptografie? Lze v postupech založených na biometrii nalézt dostatečnou bezpečnost ve vztahu ke kryptografickým klíčům?

Autoři článku [4] si svůj pohled poněkud zjednodušili, posuzují pouze:
- vhodnost biometrického postupu ke kryptografickým účelům – redukuje se "v podstatě" na tzv. rozlišovací schopnost (jedince ve velké populaci),
- a jediná další poznámka dotýkající se kryptografie je obsažena v závěru článku – a týká se opakovatelnosti generování klíče.

Citovaná disertace [5] pak diskutuje:
- délku kryptografického klíče,
- postup pro generování klíče, digitálního certifikátu

Formulace v uvedeném článku a citované disertaci mě neuspokojili, naopak mě donutili poohlédnout se po jiných pramenech. Solidní informace, které se dotýkají aktuálního popisu problematiky, lze nalézt v [1].

2. Kryptografické klíče

Samozřejmě nároky na vlastnosti kryptografických klíčů jsou různé – závisí to na použitém kryptografickém algoritmu, na systému, ve kterém je algoritmus využíván, na požadavcích na bezpečnost atd. Přesto lze vyčlenit některé společné momenty:

- dostatečná velikost množiny možných klíčů. To je nejčastěji diskutovaná vlastnost, promítá se třeba do požadavků na délku klíče pro symetrickou šifru (počet bitů – 80, 128, 256), na délku klíče asymetrických algoritmů, atd.
- důležitým doplňkem předešlé vlastnosti je požadavek náhodného výběru klíče, tj. jednotlivé klíče jsou z množiny všech klíčů vybírány se stejnou pravděpodobností, vzájemně nezávisle – splnění tohoto požadavku je vyhodnocováno obvykle celou škálou statistických testů.
- kryptografický klíč je chráněn proti nežádoucímu zveřejnění či úniku informace o jeho hodnotě. Týká se to jak uložení samotného klíče, tak i případného přenosu klíče druhé straně. Např. se může jednat i o přesun hodnoty klíče z místa, kde klíč byl vygenerován, na místo, kde bude použit atd.
- možnost revokace klíče a možnost jeho nahrazení nově vygenerovaným klíčem. To je důležité v situacích, kdy starý klíč již neposkytuje dostatečnou bezpečnost - byl kompromitován, nebo je používán již dlouhou dobu atd.

To jsou jen některé z požadavků, se kterými se můžeme setkat v kryptografické praxi. Hlubší požadavky jsou definovány v návaznosti na hodnocení, certifikaci kryptografického systému (např. NIST – dokument FIPS 140-2 – http://csrc.ncsl.nist.gov/publications/fips/fips140-2/fips1402.pdf).
A nověji (to ještě třeba zmíněný dokument NIST nezachytil) se objevují požadavky na ochranu před únikem informací postranními kanály a požadavky na s tím související zabezpečení.

Není však cílem těchto úvah vytvářet "maximalistické" nároky. Výše uvedené čtyři body lze však považovat za rozumný obecný základ.

3. Biometrie, základní postupy

Jen velmi stručně. Dnes již existuje celá škála používaných biometrických postupů (sloužících k identifikaci jedince) – otisky prstů, otisk duhovky, biometrie cév na dlani, biometrie obličeje, hlasu atd. Z pohledu, který je důležitý pro obsah tohoto článku, nás zajímá digitalizovaná podoba změřených biometrických informací. Biometrické informace jsou specifické svým charakterem. Jsou rozmazané (fuzzy), měření, která jsou třeba posunutá v čase, mohou vést k mírně odlišným výsledkům [3]. Jsou neodlučně (v podstatě) svázány s jedincem, jehož biometrické charakteristiky byly měřeny. Biometrické postupy jsou poměrně široce využívány pro autentizaci jednotlivce. Mj. jiné je zde vhodné zmínit současné požadavky na využití tzv. dvoufaktorové autentizace, kde se počítá se širokým využitím biometrických postupů. Některé kritické poznámky, které se týkají omezení dvoufaktorové autentizace zformuloval Bruce Schneier [2].

4. Co může biometrie poskytnout ve vztahu ke kryptografickým postupům

V článku [1] najde zainteresovaný čtenář v tomto směru všechny podstatné informace, tak jak je přináší současný stav výzkumu problematiky. V úvodu autoři charakterizují hlavní problémy, kterými je nutno se zabývat při implementaci biometrických postupů pro kryptografické účely. Pro přehled:

1) Uložené šablony obsahují šum, naopak vygenerovaný kryptografický klíč vyžaduje jednoznačnost, jinak příslušné protokoly nefungují. Tj. je třeba se zabývat jednoznačností použitého postupu.
2) Je třeba zvažovat otázky ochrany a utajení získaných informací (biometrická data uložená v centrálních databázích).
3) Samotná biometrická data nejsou příliš tajná. Otisky prstů jsou zanechávány na sklenicích, obraz sítnice sejme skrytá kamera atd.
4) Důležitá je také společenská akceptace příslušné biometrické technologie (např. strach lidí před únikem medicinských dat).
5) Při posuzování konkrétní biometrické metody pak mohou vzniknout i další otázky, které souvisí s konkrétními vlastnostmi dané implementace (bezpečnostní aj. hlediska).
V této souvislosti autoři citují specifiku problému odvození "biometrického klíče" při využití biometrie duhovky.

A co více - postupy navržené autory práce [1] řeší i problém revokace a obnovy klíče.

5. Závěr

Nebylo cílem tohoto krátkého článku odsunout biometrii mimo zorné pole kryptografie a ani to není smysluplné. Biometrie a kryptografie v současnosti definují svůj vztah, styčné body, resp. naopak dělící čáry. Při posuzování využitelnosti biometrických postupů pro kryptografické účely je třeba důkladně posoudit celou řadu ohledů, nelze se spokojit s dílčími konstatováními. Lze tedy bohužel zpochybnit takové závěry (ve vztahu k využitelnosti a bezpečnosti odvozených kryptografických postupů), které se opírají pouze o argumentace typu - dostatečná entropické síla příslušné biometrické charakteristiky.

6. Literatura:

[1] Hao, Feng; Anderson, Ross; Daugman, John: Combining cryptography with biometrics effectively, University of Cambridge, Computer Laboratory. July 2005 (http://www.cl.cam.ac.uk/users/jgd1000/biocrypto.pdf)

[2] Schneier, Bruce: např.: Scandinavian Attack Against Two-Factor Authentication (http://www.schneier.com/blog/archives/2005/10/scandinavian_at_1.html), ale i další jeho vyjádření (na blogu, v článcích).

[3] Dodin, Yevgeniy; Reyzin, Leonid; Smith, Adam: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data

[4] Drahanský, Martin; Orság, Filip: Může biometrie sloužit ke kryptografii?, Crypto-World 11/2005

[5] Drahanský, Martin: Biometric Security Systems - Fingerprint Recognition Technology, Brno, CZ, 2005, s. 140 (http://www.fit.vutbr.cz/research/pubs/theses/Drahansky.pdf)

C. KEYMAKER 2005 – nejlepší práce

V roce 2005 byla poprvé uspořádána soutěž o nejlepší studentskou práci v oblasti informační bezpečnosti a kryptologie pod názvem **KEYMAKER 2005**. Soutěž vyhlásila a organizovala skupina **Brno University Security Laboratory** za podpory firmy Grisoft, a.s. a mediálních partnerů e-zinu **Crypto-World** a časopisu **DSM**. Další informace k soutěži můžete najít na webové stránce http://www.buslab.cz/mkb/cfp_keymaker.htm.

Pořadí soutěže bylo slavnostně vyhlášeno 1.12.2005 na **MKB 2005** (Mikulášská kryptobesídka, http://www.buslab.cz/mkb/), kde také současně zazněla prezentace nejlépe hodnocené práce a to diplomanta MFF UK Praha Jiřího Vábka.

KEYMAKER 2005 – konečné pořadí
1. **Jiří Vábek** - Kryptoanalýza německé vojenské šifry Enigma - Rejewski a záhada třetího rotoru
2. **Peter Pecho** - Prihlasovanie čipovou kartou do Unixu
3. **Martin Drahanský** - Fingerprint Key Generation
4. až 6. místo: Marek Kluzo, Juraj Ondruš a Tomáš Doseděl.

Se zkrácenou verzí vítězné práce se nyní můžete seznámit.

Kryptoanalýza německé vojenské šifry Enigma - Rejewski a záhada třetího rotoru

Jiří Vábek, MFF UK Praha, vabek@karlin.mff.cuni.cz

Abstrakt

Tento příspěvek je založen na mé diplomové práci s názvem Kryptoanalýza německé vojenské šifry Enigma. Přestože se jedná o šifrovací přístroj z 2. světové války, téma je stále živé. Nejen kvůli několika stále nevyjasněným skutečnostem, ale i jako ukázka obecných principů kryptografie a kryptoanalýzy, z kterých se můžeme poučit i dnes. Ve stručnosti je prezentována konstrukce a princip fungování Enigmy. Dále potom jeden z hlavních výsledků práce polského matematika Mariana Rejewského, princip odhalování vnitřního propojení v rotorech. Popis je doplněn o novou část, tzv. odhalení třetího rotoru, které není v dostupné literatuře uspokojivě vysvětleno. Uvádím zde jednu možnou metodu, kterou mohl Rejewski použít. Metoda je založena na podobných myšlenkových postupech, jaké používal Rejewski, a je doplněna o vymezení podmínek, za jakých mohla být použita, a o výpočet pravděpodobnosti, že byla použitelná vzhledem k množství zachyceného šifrového materiálu, který měl mít podle dostupných zdrojů Rejewski k dispozici.

Úvod

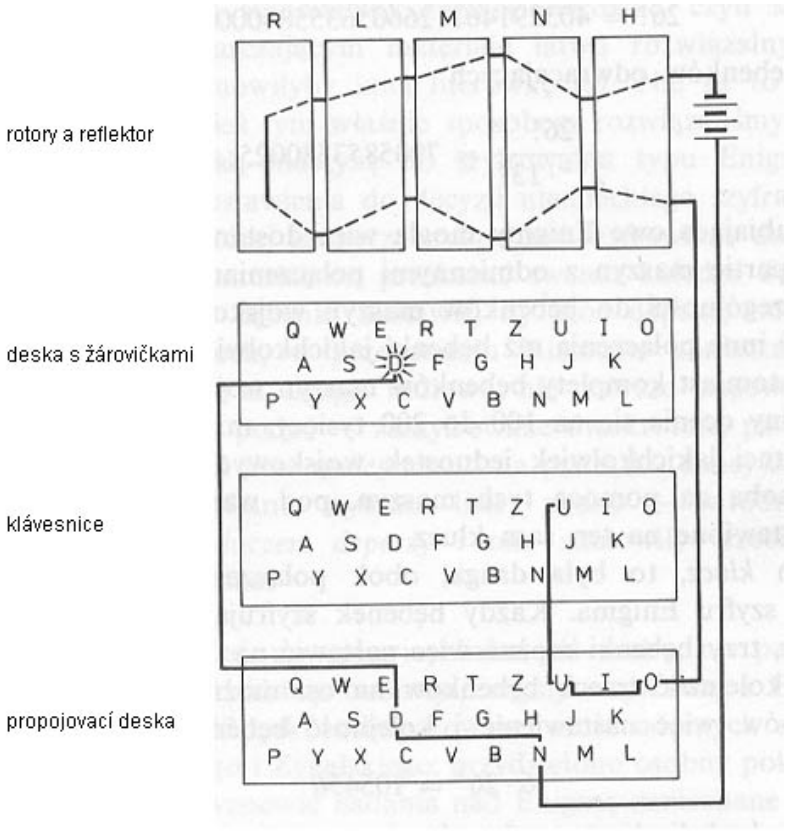
Období od první světové války až do první poloviny 20. století patřilo v kryptogafii přístrojům založeným na pohyblivých rotorech. V této souvislosti je třeba zmínit nejvýznamnější postavy, které nezávisle na sobě navrhly a patentovaly několik takovýchto přístrojů. Byli to Edward Hebern (USA), Hugo Alexander Koch (Holandsko) nebo Arvid Damm (Švédsko). Především však němec Arthur Scherbius, jehož přístroj nazvaný Enigma je dnes doslova kryptografickou legendou a jehož užití a následná kryptoanalýza výrazně ovlivnily průběh 2. světové války.

Scherbius svůj přístroj patentoval 23.2.1918 (uváděna jsou však i jiná data, např. 18.2.1918) a plánoval jej uplatnit v komerční sféře. Úspěšný však byl až o několik let později, kdy jeho přístroj zaujal německou armádu. V roce 1926 začalo Enigmu používat německé námořnictvo, v roce 1928 potom německá armáda. V tu dobu již byl součástí přístroje tzv. reflektor, kterým Scherbius mohl vylepšit svůj přístroj díky koupi patentu A. Kocha (1927). Armádní varianta se lišila od komerční varianty jiným vnitřním propojením v rotorech a instalací další součásti, propojovací desky, která podstatně zvýšila počet možných nastavení přístroje. Během třicátých let se Enigma rozšířila do všech sfér německé vojenské komunikace a během války počet přístrojů přesáhl sto tisíc [3]. Byla používána v desítkách samostatných sítích s vlastními klíči a v nejrůznějších verzích. Ještě dlouho po válce německá strana věřila, že jejich komunikace pomocí Enigmy byla bezpečná. Toto přesvědčení se však ukázalo jako fatální omyl.

Tajné služby budoucích spojenců nezahálely. Od roku 1928 se především anglická, francouzská a polská tajná služba snažila rozluštit novou německou šifru, dlouho ale bezvýsledně. Podařilo se pouze zjistit, že k šifrování je používán nový přístroj, Enigma. Nejvytrvalejší ve svém úsilí bylo Polsko, které také mělo největší obavy ze stoupající vojenské síly svého západního souseda. Polská tajná služba angažovala do svých služeb tři matematiky. Marian Rejewski (1905-1980), Henryk Zygalski (1906-1978) a Jerzy Rózycki (1907-1942) začali pracovat v „Biuro Szyfrów“ ve Varšavě 1. září 1932. Rejewski byl oddělen od svých kolegů a byla mu svěřena kryptoanalýza Enigmy.

Konstrukce Enigmy

Enigma měla vzhled klasického psacího stroje. Schematické znázornění všech hlavních součástí je na obrázku 1.



Obrázek 1: Schéma součástí Enigmy, použit obrázek z polského originálu článku

Klávesnice měla 26 písmen standardní latinské abecedy, s téměř shodným rozložením kláves jako dnešní QWERTY. Nad klávesnicí se nacházela deska s žárovkami podsvěcujícími stejně rozložených 26 písmen abecedy. Nad deskou s žárovkami, pod svrchním krytem, se nacházely 3 otočné výměnné rotory na kovové ose a reflektor. Dole pod klávesnicí se nacházela ve vojenské variantě propojovací deska, kde bylo možno pomocí několika kabelů prohodit několik dvojic písmen (nejprve 6, od 1. října 1936 byl počet zvýšen na 5-8 [4]). Z propojovací desky vedly dráty do vstupního rotoru, na který navazovaly rotory pohyblivé.

Rotory měly 26 kontaktů po obou plochých stranách rozložených do kruhu. Kontakty z jedné strany byly propojeny s kontakty z druhé strany pomocí drátků ukrytých uvnitř rotoru. Toto propojení bylo nepravidelné a pro každý ze tří rotorů jiné. Rotory byly po obvodu opatřeny zuby, které zajišťovaly pohyb daného rotoru. Navíc každý rotor měl po obvodu prstenec s 26 písmeny (v některých variantách čísly), který se dal přichytit k rotoru na 26 místech. V okénkách na krytu rotorů bylo tak možno podle těchto písmen určit polohu rotorů. Na obvodu měl navíc prstenec jeden vrub (pro každý rotor na jiném místě) pomocí kterého se přenášel pohyb na sousední rotor vlevo. Tento přenos by zajištěn součástkou ve tvaru ~T. Pokud jeden konec zapadl do vrubu, druhý konec zapadl do zubů sousedního rotoru a při příštím stisku klávesy nastal pohyb obou rotorů.

Jaká byla tedy sekvence otáčení rotorů? Rotor napravo se pootočil o 1/26 při každém stisku klávesy. Předpokládejme, že vrub na prstenci pravého rotoru je umístěn tak, aby přenos pohybu na prostřední rotor nastal, když bude v pravém okénku vidět písmeno G. Stejně tak u prostředního rotoru předpokládejme, že vrub na prstenci prostředního rotoru je umístěn tak, aby přenos pohybu na levý rotor nastal, když bude v prostředním okénku vidět písmeno R. Tři typické sekvence pozic rotorů poté mohou vypadat například takto:

```
1) A A A        2) A A F        3) A Q G
   A A B           A A G           A R H
   A A C           A B H           B S I
   A A D           A B I           B S J
    ...             ...             ...
```

První příklad ukazuje situaci, kdy se pohybuje pouze pravý rotor. Na druhém příkladě můžeme vidět přenos pohybu z pravého rotoru na prostřední. Třetí příklad popisuje situaci (relativně velmi řídkou), kdy přenos pohybu mezi pravým a prostředním rotorem je při dalším stisku klávesy následován přenosem pohybu mezi prostředním a levým rotorem. To znamená, že do původní pozice by se rotory dostaly až po 26×25×26 = 16900 stisknutích klávesy.

Reflektor (ve většině variant, především zpočátku, statický) měl stejně jako rotory na jedné straně kontakty, které však byly navzájem nepravidelně spárovány drátky.

Jak probíhalo zašifrování? Na obrázku 1 je uveden příklad možného toku proudu přístrojem. Po stisku klávesy U došlo k pootočení pravého rotoru (eventuelně i dalších). V tu chvíli se okruh uzavřel. Proud šel z klávesnice do propojovací desky, kde se písmeno U prohodilo na písmeno O. Poté proud směřoval z propojovací desky do vstupního rotoru, odtud potom přes všechny rotory do reflektoru a zpět. Písmeno N se opět na přepojovací desce prohodilo na D. Odtud tekl proud do desky se žárovkami, kde se rozsvítila žárovička pod písmenem D, výsledkem zašifrování.

V jednom nastavení a pozici rotorů tak dával přístroj přesně určenou jednoduchou substituci. Výsledkem tak byla polyalfabetická šifra. Díky reflektoru měly tyto substituce velmi speciální vlastnost, písmena byla spárována do dvojic. Pokud bylo písmeno U zašifrováno jako D, potom se stejným nastavením bylo naopak písmeno D zašifrováno jako U. Tato vlastnost umožňovala jednoduché dešifrování. Příjemce pouze nastavil přístroj do

stejné počáteční pozice a napsáním zašifrovaného textu získal text otevřený. Zároveň však tato vlastnost velmi zjednodušila situaci při rozbití šifry.

Matematický model

Tok proudu přístrojem může být reprezentován v jazyku permutací. V tomto textu budeme pod permutací rozumět bijekci na množině {a, b, c,…, x, y, z} 26 písmen abecedy. Permutace budou označovány velkými písmeny, malá písmena budou značit prvky množiny. Hodnotu permutace A na písmenu *x* budeme zapisovat xA. Součin (složení) dvou permutací budeme zapisovat „zleva doprava“, tedy například pro dvě permutace A a D máme:

x(AD)=(xA)D.

Důvod je mimo jiné historický - konzistence se zápisem, který používal Rejewski.

Nyní si můžeme představit, že kontakty na jedné straně rotoru jsou popořadě označeny písmeny od a do z, a stejným způsobem i kontakty na druhé straně a to tak, aby protější kontakty byly označeny stejnými písmeny. Propojení drátky v rotoru nám tak definuje permutaci na množině {a, b, c,…, x, y, z}

Totéž můžeme udělat pro ostatní rotory. U reflektoru, kde jsou kontakty pouze na jedné straně, bude jejich vzájemné propojení určovat permutaci se 13 transpozicemi (cykly délky 2). Označme si permutaci definovanou reflektorem R, permutace definované rotory označme (od pravého rotoru) po řadě N, M, L. Stejně tak propojení kabely na propojovací desce definuje permutaci, kterou označíme S, a propojení z propojovací desky do vstupního rotoru permutaci, kterou označíme H. Potom pro jedno konkrétní nastavení Enigmy dostáváme výraz:

$SHNMLRL^{-1}M^{-1}N^{-1}H^{-1}S^{-1}$.

Jak přejít od tohoto statického modelu k dynamickému, který by zachycoval pohyb rotorů? Nejprve nadefinujeme permutaci P, která zobrazuje každé písmeno na svého následovníka v abecedě (na konci se z zobrazí na a). Dostáváme tak permutaci s jedním cyklem délky 26, zapsanou v cyklickém zápisu takto:

P=(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).

Co se stane, když se například rotor N pootočí o 1/26? Vezměme směr otáčení proti směru, jakým jsou označeny kontakty na rotoru v abecedním pořadí. Představme si, že před otočením je spojeno např. písmeno a ze vstupního rotoru s písmenem a na pravém rotoru. Po otočení bude a spojeno s b. To však můžeme zařídit i tak, že mezi permutaci H a N vložíme permutaci P, která nám posune písmeno a na pravém rotoru na písmeno b. Při opouštění rotoru opět vložíme tentokrát P^{-1}. Po jednom otočení pravého rotoru tak dostáváme výraz:

$SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}$.

Denní klíče a klíče zprávy

Z popisu Enigmy je vidět, že přístroj měl několik nastavitelných součástí. Můžeme tak chápat Enigmu jako šifrovací algoritmus a nastavení těchto součástí jako klíč, který musí znát příjemce i odesilatel.

V každé jednotlivé síti byly v jeden den všechny přístroje ve stejném počátečním natavení. Tomuto nastavení se říkalo denní klíč (typická doba platnosti většiny součástí zpočátku jeden den).
Denní klíč se skládal z těchto částí:

- Pořadí rotorů (*Walzenlage*) - Na začátku byly rotory pouze tři a jejich pořadí bylo měněno jednou za tři měsíce. Od 1. ledna 1936 bylo pořadí měněno jednou za měsíc a od 1. října 1936 denně [4]. Od 15.prosince 1938 byly přidány dva další rotory (na ose stále pouze tři, které se však od této chvíle vybíraly z pěti) a během války postupně ještě další tři.
- Pozice prstenců (*Ringstellung*) - Pozice, v které byly uchyceny prstence na jednotlivých rotorech. Původně měněny jednou za měsíc, později denně.
- Propojení na propojovací desce (*Stecker*) - K propojení písmen na propojovací desce se používalo 6 kabelů a propojení se měnilo denně. Od 1. října 1936 se počet pohyboval v rozmezí 5 až 8 [4], později vzrostl až na 10.
- Základní nastavení (*Grundstellung*) - Základní nastavení udává, která písmena budou vidět v okénkách krytu rotorů. Toto nastavení se měnilo denně a od 15. září 1938 již nebylo ve většině sítí součástí denního klíče.

Jak tedy vypadal šifrovací protokol? Denní klíče byly distribuovány centrálně „papírovou“ formou. Operátor nejprve nastavil přístroj podle údajů o denním klíči. Poté náhodně vybral tři písmena (člověk je však velice špatný náhodný generátor a výběr tak zdaleka nebyl náhodný) a tyto tři písmena, tzv. klíč zprávy, např. xyz, dvakrát zašifroval v pořadí xyzxyz. Tento zašifrovaný indikátor umístil na začátek zprávy. Poté změnil základní nastavení rotorů tak, aby v okénkách byla vidět jím zvolená tři písmena, a s tímto nastavením začal šifrovat samotný text.

Dešifrování probíhalo zcela analogicky. Příjemce měl přístroj nastavený podle aktuálního denního klíče. Po přijetí zprávy nejprve rozšifroval prvních šest písmen zprávy a pokud dostal dvakrát se opakující trojici písmen, věděl skoro jistě, že nedošlo k poruše indikátoru při přenosu (toto byl důvod dvojnásobného zašifrování klíče zprávy). Nastavil pak rotory do pozic zadaných klíčem zprávy a pokračoval v dešifrování zprávy.

Výpočet propojení v pravém rotoru

Vraťme se nyní k Marianu Rejewskému do roku 1932. Informace, kterou zdědil po svých předchůdcích, byla pouze znalost faktu, že je používána strojová šifra produkovaná obměnou komerčního modelu Enigmy. K dispozici měl několik desítek zašifrovaných zpráv denně. Velmi rychle odhalil, že prvních šest písmen zprávy vždy tvoří indikátor, dvakrát zašifrovaný klíč zprávy (o tom, jak na to přišel, uvedeno více v [7] nebo v [2]).

Označme si nyní písmeny A až F šest permutací definovaných šesti prvními pozicemi rotorů odvozených od denního klíče. Těchto šest permutací bylo použito k dvojímu zašifrování denního klíče. Tedy:

$$A = SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}$$
$$B = SHP^{-2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{-2}H^{-1}S^{-1}$$
$$C = SHP^{-3}NP^{-3}MLRL^{-1}M^{-1}P^{3}N^{-1}P^{-3}H^{-1}S^{-1}$$
$$D = SHP^{-4}NP^{-4}MLRL^{-1}M^{-1}P^{4}N^{-1}P^{-4}H^{-1}S^{-1}$$
$$E = SHP^{-5}NP^{-5}MLRL^{-1}M^{-1}P^{5}N^{-1}P^{-5}H^{-1}S^{-1}$$
$$F = SHP^{-6}NP^{-6}MLRL^{-1}M^{-1}P^{6}N^{-1}P^{-6}H^{-1}S^{-1}$$

Tyto rovnice platí pouze za předpokladu, že nedošlo k přetočení prostředního rotoru. Nadále budeme pracovat pouze s touto hypotézou. Pokud k přetočení rotorů došlo, bylo to možné většinou snadno odhalit.

Permutace A až F byly naneštěstí neznámé stejně jako permutace H, M, N, L, R, S. Rejewski si ale všiml, že z indikátoru lze získat následující informaci.

Předpokládejme, že zachycená zpráva má indikátor dmqvbf. Předpokládejme, že těchto šest písmen má v otevřeném textu tvar xyzxyz. To znamená, že xA=d a zároveň xD=v. Ze speciálních vlastností permutací A až F víme, že bude také platit dA=x. Substitucí za x z tohoto výrazu do xD=v tak dostaneme následující rovnost: dAD=v .

To znamená, že obraz písmene d pomocí složení permutací AD je písmeno v. Pokud máme dostatek šifrových zpráv z jednoho dne (Rejewski uvádí, že stačí zhruba 80 zpráv [5,6], nebo i 60 zpráv [4]), můžeme zrekonstruovat celou permutaci AD.

Nyní je nutné nadefinovat několik pojmů a vyslovit několik základních tvrzení.

Definice. Abeceda *je permutace na množině 26 písmen {a,b,c,…,x,y,z}, která obsahuje 13 disjunktních cyklů délky 2 (transpozic).*

Termín abeceda užívá Turing v [8] ve speciálnějším významu, pro permutaci definovanou jedním nastavením Enigmy.

Definice. Charakteristika *je permutace na množině 26 písmen {a,b,c,…,x,y,z}, která je složením dvou* abeced.

Rejewski užívá ve svých textech pojem charakteristika opět ve speciálnějším významu, pro trojici permutací AD, BE a CF. Nyní vyslovíme jedno základní známé pomocné tvrzení:

Lemma. *Dvě permutace X a Y jsou konjugované (tj. existuje Z takové, že $X=ZYZ^{-1}$) právě tehdy, když jsou stejného typu (mají stejnou cyklickou strukturu).*

Z důkazu tohoto známého lemmatu dostaneme jednoduchý návod, jak zkonstruovat permutaci Z. Stačí napsat permutaci (v zápisu pomocí cyklů) Y pod permutaci X tak, aby se cykly stejné délky nacházely pod sebou, a můžeme přímo vidět permutaci Z – obraz každého písmene je písmeno nacházející se pod ním.

To nám zároveň dává počet takových permutací Z. Označme číslem k_i počet cyklů délky i v permutaci X (nebo Y). Máme tak $k_i!$ možností, jak seřadit cykly délky i. Cyklus délky i navíc můžeme zapsat i způsoby. Potom počet všech možných permutací Z bude:

$$\prod_{i=1}^{n} i^{k_i} \cdot k_i! \text{ , kde n je maximální délka cyklu} \qquad (1)$$

Nyní následuje druhé stěžejní tvrzení (dokázané Rejewským např. v [5]):

Tvrzení. *Pro permutaci A existují dvě abecedy X a Y takové že A=XY právě tehdy, když A obsahuje sudý počet cyklů každé délky (tj.* $k_{i\ i}$*=0 mod 2, pro každé i=1,…,n).*

Rejewski tak mohl rozložit charakteristiky AD, BE a CF na jednotlivé abecedy. Tento rozklad není jednoznačný, ale právě díky často stereotypně voleným klíčům se Rejewskému podařilo vybrat ten správný rozklad (podrobnější popis např. v [4,7]).

V tuto chvíli však stále měly rovnice příliš neznámých. Naštěstí do děje zasáhla špionáž. Rejewski získal zprostředkovaně přes francouzské spojence od německého špióna (Hans-Thilo Shmidt, pseudonym Asche) sady denních klíčů ze září a října roku 1932. Mohl tak snadno zjistit permutace S a nastavení rotorů v daných dnech.

Další problém tvořila permutace H. V komerčním modelu byly dráty z klávesnice zapojeny do vstupního rotoru v pořadí, v jakém se nacházejí na klávesnici, tedy q, w, e, r, atd. Předpoklad, že u vojenské varianty jsou dráty z propojovací desky připojeny ke vstupnímu rotoru stejně, způsobil Rejewskému následně mnoho potíží. Po mnoha neúspěších nakonec zkusil změnit tento předpoklad a otestoval jinou hypotézu zachovávající jistou pravidelnost, totiž že dráty jsou ke vstupnímu rotoru připojeny podle abecedy a tudíž H je identická permutace. Kupodivu se ukázalo, že má pravdu, a rovnice se tak opět zjednodušily o jednu neznámou.

Poté už bylo možno postupovat následovně. Nejprve si definujeme permutaci Q pro zkrácení zápisu.

$$Q = MLRL^{-1}M^{-1}$$

Nyní můžeme upravit rovnice pro A až F. Použijeme zjednodušení zápisu pro Q,všechny známé permutace převedeme na levou stranu a označíme tyto známé permutace písmeny U až Z:

$$U = P^{-1}H^{-1}S^{-1}ASHP = NP^{-1}QPN^{-1}$$
$$V = P^{-2}H^{-1}S^{-1}ASHP^{2} = NP^{-2}QP^{2}N^{-1}$$
$$W = P^{-3}H^{-1}S^{-1}ASHP^{3} = NP^{-3}QP^{3}N^{-1}$$
$$X = P^{-4}H^{-1}S^{-1}ASHP^{4} = NP^{-4}QP^{4}N^{-1}$$
$$Y = P^{-5}H^{-1}S^{-1}ASHP^{5} = NP^{-5}QP^{5}N^{-1}$$
$$Z = P^{-6}H^{-1}S^{-1}ASHP^{6} = NP^{-6}QP^{6}N^{-1}$$

Nyní vynásobíme dvě po sobě jdoucí rovnice následujícím způsobem:

$$UV = NP^{-1}QP^{-1}QPPN^{-1}$$
$$VW = NP^{-2}QP^{-1}QPP^{2}N^{-1}$$
$$WX = NP^{-3}QP^{-1}QPP^{3}N^{-1}$$
$$XY = NP^{-4}QP^{-1}QPP^{4}N^{-1}$$
$$YZ = NP^{-5}QP^{-1}QPP^{5}N^{-1}$$

Odtud můžeme eliminovat společný výraz $QP^{-1}QP$ a dostaneme následující systém rovnic:

$$UV = NPN^{-1}VWNP^{-1}N^{-1}$$
$$VW = NPN^{-1}WXNP^{-1}N^{-1}$$
$$WX = NPN^{-1}XYNP^{-1}N^{-1}$$
$$XY = NPN^{-1}YZNP^{-1}N^{-1}$$

Vidíme, že permutace UV je konjugovaná s VW pomocí NPN^{-1}, stejně tak permutace VW s permutací WX pomocí NPN^{-1}, atd. Můžeme tak téměř jistě jednoznačně spočítat výraz NPN^{-1} (přesnější rozbor uvádím v mé diplomové práci). Zároveň ale víme, že tato permutace je konjugována s permutací P, dostáváme tak 26 možností pro permutaci N, neboli propojení v pravém rotoru. Těchto 26 možností pro N navíc úzce souvisí - kontakty na jedné a na druhé straně budou vůči sobě o něco „pootočeny“ při zvolení špatné možnosti.

„Záhada“ třetího rotoru

Jak již bylo řečeno, Rejewski měl mít k dispozici pouze data o denních klíčích ze dvou měsíců ze dvou čtvrtletí, kdy se napravo vystřídaly pouze dva rotory (pořadí rotorů se v tu dobu měnilo pouze 1x za čtvrt roku). Není známo ani přesné pořadí rotorů v obou měsících, víme pouze, že napravo se vyskytoval v každém měsíci jiný rotor. Jak Rejewski odhalil propojení ve třetím rotoru?

Vysvětlení v Rejewského článcích se navzájem liší, ba dokonce lze říci, že si i odporují, pokaždé je však vyjádření velmi neurčité.

V článku [6] Rejewski tvrdí, že metoda odhalení třetího rotoru a reflektoru nepřinesla nic nového a jako pomoc posloužil autenticky zašifrovaný text. V článku [7] mluví pouze o dostatku šifrového materiálu.V článku [4] opět zmiňuje autentický příklad šifrování a uvádí, že dopočítat zbylé údaje nepředstavovalo velký problém. Nakonec v článku [5] popírá tvrzení o denních klíčích pouze ze dvou měsíců, všechny rotory se údajně měly vystřídat napravo, tato možnost se však vzhledem ke všem dalším údajům zdá velmi nepravděpodobná.

Cílem tedy bylo zrekonstruovat způsob výpočtu třetího rotoru. Jedna z možných metod následuje.

Výpočet třetího rotoru

Označme si opět rotory zleva doprava písmeny L, M, N v prvním měsíci ze dvou, z kterých známe denní klíče. Potom můžeme všechny možnosti pořadí rotorů v obou měsících zapsat do Tabulky 1:

	1.měsíc	2.měsíc	Neznámý rotor
a)	LMN	LNM	L
b)	LMN	NLM	L
c)	LMN	MNL	M
d)	LMN	NML	M

Tabulka 1: Možná pořadí rotorů ve dvou měsících.

Tuto metodu lze použít v situaci, kdy alespoň v jednom měsíci je neznámý rotor uprostřed. Když se podíváme na Tabulku 1, tento požadavek je splněn v případech b), c) a d). Vyberme si například možnost b), první měsíc.

Z tohoto měsíce budeme potřebovat data ze dvou dní, kdy levý rotor je ve stejné pozici oba dny a rozdíl pozic prostředního není 0 nebo 13.

Předpokládejme, že máme vhodné abecedy z těchto dvou dní. Označme si abecedy z prvního dne písmenem A_i, abecedy z druhého dne písmenem B_i a pozici levého rotoru kvůli zjednodušení zápisu pouze jako L. Z prvního dne tedy máme (budou nám stačit tři abecedy):

$$A_1 = P^{s1}NP^{-s1}P^{r1}MP^{-r1}LRL^{-1}P^{r1}M^{-1}P^{-r1}P^{s1}N^{-1}P^{-s1}$$
$$A_2 = P^{s1+1}NP^{-s1-1}P^{r1}MP^{-r1}LRL^{-1}P^{r1}M^{-1}P^{-r1}P^{s1+1}N^{-1}P^{-s1-1}$$
$$A_3 = P^{s1+2}NP^{-s1-2}P^{r1}MP^{-r1}LRL^{-1}P^{r1}M^{-1}P^{-r1}P^{s1+2}N^{-1}P^{-s1-2}$$

a z druhého dne:

$$B_1 = P^{s2}NP^{-s2}P^{r2}MP^{-r2}LRL^{-1}P^{r2}M^{-1}P^{-r2}P^{s2}N^{-1}P^{-s2}$$
$$B_2 = P^{s2+1}NP^{-s2-1}P^{r2}MP^{-r2}LRL^{-1}P^{r2}M^{-1}P^{-r2}P^{s2+1}N^{-1}P^{-s2-1}$$
$$B_3 = P^{s2+2}NP^{-s2-2}P^{r2}MP^{-r2}LRL^{-1}P^{r2}M^{-1}P^{-r2}P^{s2+2}N^{-1}P^{-s2-2}$$

Vyjádříme si R z rovnic pro B_i a substitucí za R do rovnic pro A_i, i=1,2,3 dostáváme:

$$A_1 = P^{s1}NP^{-s1}P^{r1}MP^{-r1}P^{r2}M^{-1}P^{-r2}P^{s2}N^{-1}P^{-s2}B_1P^{s2}NP^{-s2}\ P^{r2}MP^{-r2}P^{r1}M^{-1}P^{-r1}P^{s1}N^{-1}P^{-s1}$$

$A_2 = P^{s1+1}NP^{-s1-1}P^{r1}MP^{-r1}P^{r2}M^{-1}P^{-r2}P^{s2+1}N^{-1}P^{-s2-1}B_1P^{s2+1}NP^{-s2-1}P^{r2}MP^{-r2}P^{r1}M^{-1}P^{-r1}P^{s1+1}N^{-1}P^{-s1-1}$
$A_2 = P^{s1+2}NP^{-s1-2}P^{r1}MP^{-r1}P^{r2}M^{-1}P^{-r2}P^{s2+2}N^{-1}P^{-s2-2}B_1P^{s2+2}NP^{-s2-2}P^{r2}MP^{-r2}P^{r1}M^{-1}P^{-r1}P^{s1+2}N^{-1}P^{-s1-2}$

Ke zkrácení rovnic označme písmenem Q_i následující výraz:

$Q_1 = MP^{-r1}P^{r2}M^{-1}P^{-r2}P^{s2}N^{-1}P^{-s2}B_1P^{s2}NP^{-s2}\ P^{r2}MP^{-r2}P^{r1}M^{-1}$
$Q_2 = MP^{-r1}P^{r2}M^{-1}P^{-r2}P^{s2+1}N^{-1}P^{-s2-1}B_1P^{s2+1}NP^{-s2-1}P^{r2}MP^{-r2}P^{r1}M^{-1}$
$Q_3 = MP^{-r1}P^{r2}M^{-1}P^{-r2}P^{s2+2}N^{-1}P^{-s2-2}B_1P^{s2+2}NP^{-s2-2}P^{r2}MP^{-r2}P^{r1}M^{-1}$

Nyní v předchozích rovnicích převedeme známé permutace nalevo. Použijeme zpřehlednění výrazů pomocí Q_i a vynásobíme upravené rovnice následovně:

$MP^{r2-r1}M^{-1}Q_1Q_2MP^{r1-r2}M^{-1} = P^{s1-r1}N^{-1}P^{-s1}A_1P^{s1}NP^{r1+1}N^{-1}P^{-s1-1}A_2P^{t1-1}NP^{-t1-1+r1}$
$MP^{r2-r1}M^{-1}Q_2Q_3MP^{r1-r2}M^{-1} = P^{s1-r1-1}N^{-1}P^{-s1-1}A_2P^{s1-1}NP^{r1+1}N^{-1}P^{-s1-2}A_3P^{t1-2}NP^{-t1-2+r1}$

Z těchto dvou rovnic můžeme opět spočítat $MP^{r2-r1}M^{-1}$ jako při odhalování propojení v pravém rotoru. Nyní počet řešení pro M závisí na rozdílu r_2-r_1. Označme si tento rozdíl písmenem v. Pokud je v=0, pak P^v je identita a není možné spočítati M. Také pokud v=13, pak P^v má cyklickou strukturu abecedy a máme 2^{13}x13! řešení pro M, což je značně nepraktické.

Uvažujme tedy nadále nadřazenou podmínku, že v není 0 nebo 13. Nyní když v je liché (neboli když NSD(v,26)=1), pak P^v má jeden cyklus délky 26 a máme 26 možností pro rotor M. Když v je sudé (neboli když GCD(v,26)=2), pak P^v má dva cykly délky 13 a máme $2x13^2$=338 možností pro M.

Jaká je pravděpodobnost, že budeme mít vhodná data? Předpokládejme, že nastavení rotorů bylo vybíráno nezávisle pro každý den a každá z 26ti počátečních pozic má stejnou pravděpodobnost.

Předpokládejme, že n je počet dní, ze kterých máme dostatek zpráv. Potom počet možností, jak bude v n dnech natočen levý rotor do jedné z 26 pozic, je 26^n. Budeme počítat počet nepříznivých případů: Nejprve rozdělme všechny případy do skupin, kde n dní je umístěno do n-j pozic, pro j=0,…,n-1. Potom pro každou skupinu (tedy každé j) máme $\binom{26}{n-j}$ možností, jak vybrat pozice, ve kterých je n dní umístěno. Nyní musíme pro každý výběr n-j pozic umístit n dní do těchto vybraných pozic.

Umísťujeme tedy n rozlišitelných prvků do n-j rozlišitelných pozic. Počet takových způsobů umístění je tedy roven počtu surjektivních funkcí z množiny mohutnosti n do množiny mohutnosti n-j. Označme počet těchto funkcí jako $F_{n,n-j}$. Pomocí principu inkluze a exkluze lze ukázat, že:

$$F_{n,n-j} = \sum_{i=0}^{n-j} (-1)^{n-j-i} \binom{n-j}{i} i^n \qquad (2)$$

Které z těchto možností jsou nevhodné? Pokud j=0, tak máme pro každou pozici levého rotoru data pouze z jednoho dne, takže žádná z těchto možností není vhodná. Pokud j=1, máme pro jednu pozici levého rotoru data ze dvou dní, ale t=1/13 z těchto pozic je nevhodných, protože rozdíl pozic prostředního rotoru bude 0 nebo 13. Pokud j=2, pak máme buď dvě pozice levého rotoru s daty ze dvou dní, anebo jednu pozici rotoru s daty ze tří dní. V obou případech je poměr nepříznivých případů $t^2=(1/13)^2$. Obdobně můžeme pokračovat pro

j=3,…,n-1. Poměr nepříznivých případů bude t^j. To znamená, že pravděpodobnost, že máme vhodná data, spočítáme následovně:

$$p_n = \frac{\sum_{j=0}^{n-1} \binom{26}{n-j} \cdot F_{n,n-j} \cdot t^j}{26^n} \qquad (3)$$

Hodnota t=1/13 byla pro případ, kdy hledáme data, kde rozdíl pozic prostředního rotoru není 0 nebo 13. Pokud chceme pouze lichý rozdíl (kromě 13), je dostatečně přesné užít horní mez pro nepříznivé případy zvolením t=7/13.

V Tabulce 2 označuje hodnota $P_{1,n}$ pravděpodobnost, že máme vhodná data pro volbu t=1/13, hodnota $P_{2,n}$ je pravděpodobnost, že máme vhodná data pro volbu t=7/13. Hodnota $P_{1,n}$ je uvedena pouze pro n<21, protože pro větší n už dává zaokrouhlená hodnota 100 %.

n	$P_{1,n}$	$P_{2,n}$		n	$P_{1,n}$	$P_{2,n}$		n	$P_{2,n}$
2	3.55	1.78		12	93.30	68.56		22	97.92
3	10.39	5.23		13	96.08	74.41		23	98.53
4	19.90	10.17		14	97.83	79.49		24	98.97
5	31.22	16.34		15	98.87	83.81		25	99.29
6	43.35	23.44		16	99.45	87.41		26	99.51
7	55.31	31.15		17	99.75	90.36		27	99.67
8	66.29	39.13		18	99.89	92.71		28	99.78
9	75.73	47.10		19	99.96	94.57		29	99.85
10	83.36	54.79		20	99.98	96.01		30	99.90
11	89.15	61.99		21		97.10			

Tabulka 2: Pravděpodobnost, že máme vhodná data v závislosti na počtu dní, z kterých máme dostatek zpráv.

Několik poznámek

Pokud se znovu podíváme na postup výpočtu pravého rotoru, můžeme si všimnout, že U je již konjugováno s V pomocí NPN^{-1}, V je konjugováno s W pomocí NPN^{-1}, atd. Proč tedy ještě sousední permutace násobíme?

Tyto výše zmíněné permutace mají tvar abeced. To znamená, že kdybychom počítali NPN^{-1} již odsud, dostali bychom podle vzorečku (1): 2^{13}x13! možností z jedné rovnice. Pokud však přejdeme k systému rovnic pro součiny těchto abeced, místo konjugovaných abeced pracujeme s konjugovanými charakteristikami. Ukazuje se, že jejich cyklická struktura je daleko výhodnější.

Jak spočítat pravděpodobnost výskytu jednotlivých charakteristik? Předpokládejme, že všechny abecedy jsou stejně pravděpodobné. Nejprve udělejme kartézský součin množiny všech abeced se sebou samou. Každá uspořádaná dvojice abeced tak bude odpovídat nějaké charakteristice. Pravděpodobnost charakteristiky nějakého konkrétního typu t bude poměr uspořádaných dvojic abeced, které dostaneme rozkladem charakteristik toho typu, ku všem dvojicím abeced. Tedy:

$$P_t = \frac{A_t \cdot B_t}{C^2} \quad \text{, kde}$$

A_t = počet charakteristik typu t
B_t = počet párů abeced, které obdržíme rozkladem jedné z těchto charakteristik
C= počet abeced

Vzorečky pro výpočet těchto hodnot jsou následující, postup výpočtu popisuji blíže v mé diplomové práci (pro zápis typu permutace opět použijeme následující notaci - k_i značí počet cyklů délky i):

$$B_t = \prod_{i=1}^{13} l_i \qquad \text{, kde} \quad l_i = \frac{k_i ! \cdot i}{(k_i/2)! \cdot 2^{(k_i/2)}} \qquad \text{pro } k_i \neq 0 \text{, jinak } l_i = 1$$

$$A_t = \frac{26!}{\prod_{i=1}^{n} i^{k_i} \cdot k_i !}$$

$$C = \frac{26!}{2^{13} \cdot 13!}$$

V Tabulce 3 uvádím takto spočítanou pravděpodobnost $P_{1,t}$. Pro srovnání jsou uvedeny hodnoty $P_{2,t}$ zmíněné Turingem v [8] bez bližšího komentáře při popisu hypotetického odhalení propojení v rotorech za jím určených podmínek (jeho postup je myšlenkově totožný s Rejewským). Dále zde uvádím pravděpodobnosti výskytu konkrétních charakteristik AD, BE a CF, které byly používány v některých metodách pro odhalování denních klíčů. Hodnoty jsou pro dva skutečně používané reflektory, hodnota $P_{3,t}$ pro reflektor A, hodnota $P_{4,t}$ pro reflektor B (hodnoty jsou zaokrouhleny, v %).

Typ	$P_{1,t}$	$P_{2,t}$	$P_{3,t}$	$P_{4,t}$
13^2	24.82	25	25.10	25.22
$12^2 1^2$	13.44	13	13.07	13.31
$11^2 2^2$	7.33	7.3	7.51	7.50
$10^2 3^2$	5.38	5.4	5.56	5.55
$9^2 4^2$	4.48	4.5	4.52	4.55
$10^2 2^2 1^2$	4.03		4.05	4.03
$8^2 5^2$	4.03	4.0	4.02	4.03
$7^2 6^2$	3.84	3.9	3.85	3.88
$11^2 1^4$	3.68	3.7	3.53	3.52
$9^2 3^2 1^2$	2.99		2.98	2.93
$8^2 4^2 1^2$	2.52		2.43	2.48
$7^2 5^2 1^2$	2.30		2.33	2.19
$8^2 3^2 2^2$	1.68		1.64	1.69
$7^2 4^2 2^2$	1.44		1.51	1.42
$6^2 5^2 2^2$	1.34		1.32	1.38
$9^2 2^4$	1.12		1.13	1.11
$9^2 2^2 1^4$	1.12		1.15	1.09
$6^4 1^2$	1.12		1.14	1.05
$6^2 4^2 3^2$	1.12		1.12	1.13

Tabulka 3: Nejpravděpodobnější charakteristiky

Závěr

Bylo ukázáno, že propojení ve třetím rotoru lze vypočítat bez jakýchkoliv jiných dat. Zda skutečně Rejewski nějaký takový postup použil, nelze s určitostí říci, každopádně se však tato možnost nabízela.

Rozluštění šifry Enigma však neznamenalo pouze zjištění vnitřního propojení, ale neustálé odhalování denních klíčů. Příběh Rejewského a jeho kolegů dál pokračoval. Polští matematici vyvinuli během třicátých let nejrůznější metody, které se střídavými úspěchy užívali. V některých obdobích dosahoval počet vyluštěných zpráv až 75%. Krátce před vypuknutím války došlo k setkání polských, francouzských a anglických kryptologů, kde polská strana ohromila své spojence znalostmi o Enigmě. Angličané tak získali zrekonstruované kopie přístroje a spoustu myšlenek, které poté angličtí kryptologové v čele s A. Turingem a G. Welchmanem dále zdokonalovali a rozvíjeli. Stejně tak byla ale zdokonalována i Enigma a šifrovací protokol. Přesto i úspěšné luštění jen části zpráv v části existujících sítí výrazně přispělo k porážce nacistických vojsk.

I po tolika letech jsou kolem Enigmy stále některé nevyjasněné skutečnosti. Hlavním důvodem je především nedostatek relevantních materiálů. Mnoho informací bylo po dlouhá léta utajováno a teprve v nedávných letech se dostaly na veřejnost (viz. např. [8]).

Enigma má ale význam nejen z historického hlediska. Používání a následné selhání Enigmy odhalilo mnoho problémů, s jakými se musíme potýkat i dnes při navrhování masově užívaného kryptosystému. Jedná se o obecné zásady, na jaké by neměl žádný kryptograf zapomenout, a potíže, se kterými se musí vyrovnat. Od založení bezpečnosti systému na klíči a ne na šifrovacím algoritmu, přes problém distribuce klíčů, použití lidí jako náhodných generátorů, návrh vhodného operačního protokolu, až po vytrvalost a odhodlanost nepřítele, který může disponovat netušenými prostředky.

Použitá literatura

[1] Orlowski A.,Gaj K.: *Facts and Myths of Enigma: Breaking Stereotypes, Appendix 1,* EUROCRYPT 2003

[2] Bauer F. L.:*Decrypted secrets: Methods and Maxims of Cryptology,* 2nd edition. Springer-Verlag, Berlin, 2000.

[3] Kozaczuk W.: *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two,* Edited and Translated by Christopher Kasparek. Frederick, Maryland: University Publications of America, Inc., 1984.

[4] Rejewski M.: *How the Polish Mathematicians Broke Enigma*. Přetištěno v [3], Appendix D, 1980.

[5] Rejewski M.: *An Application of The Theory of Permutations in Breaking The Enigma Cipher,* Applicationes Mathematicae 16, No. 4, Warsaw, 1980. Dostupné na http://mad.home.cern.ch/frode/crypto/rew80.pdf

[6] Rejewski M.: Enigma (1930-40), *Metoda i historia rozwiazania niemieckiego szyfru maszynowego*. Manuskript, ?1940. Dostupné na http://www.spybooks.pl/en/enigma.html

[7] Rejewski M: *Wspomnienia z mej pracy w Biurze Szyfr w Oddzia u II Sztabu Glownego w Latach 1930-1945*. Manuskript, 1967. Dostupné na http://www.spybooks.pl/en/enigma.html

[8] Turing Alan M.: *Turing's Treatise on Enigma*. NARA College Park, Maryland, Record Group 457, Historic Cryptographic Collection, Box 201, NR 964, 1940. Tento dokument je editován trojicí Frode Weirud, Ralph Erskine a Philip Marks pro publikování na webu Frode Weiruda. Několik kapitol bylo již publikováno na: http://frode.home.cern.ch/frode/crypto/Turing

D. O čem jsme psali v lednu 1999 – 2005

Crypto-World 1/2000

Crypto-World 1/2001

Příloha: trustcert.pdf (upoutávka na služby Certifikační Autority TrustCert)

Crypto-World 1/2002

Crypto-World 1/2003

Příloha : Crypto_p1.pdf CEN Workshop Agreements

Crypto-World 1/2004

Crypto-World 1/2005

Příloha : Speciál 2004 - přehled článků a prezentací členů redakce Crypto-World za rok 2004 (http://crypto-world.info/casop6/prehled_2004.pdf)

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/