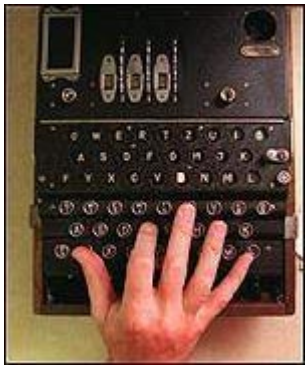
# Crypto-World

## Informační sešit GCUCMP

Ročník 2, číslo 12/2000 15.prosince 2000

# 12/2000

**Připravil : Mgr.Pavel Vondruška,**
**člen GCUCMP, BITIS, IACR, ISACA.**
**Sešit je rozesílán registrovaným čtenářům.**
**Starší sešity jsou dostupné na adresách**
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
**(>230 e-mail výtisků)**



**OBSAH :** **Str.**



**Příloha :** teze.zip - zkrácené verze prezentací ÚOOÚ použité při předložení tezí k Zákonu o elektronickém podpisu (§6, §17) dne 4.12.2000 a teze příslušné vyhlášky.

# A. Soutěž (průběžný stav, informace o 1.ceně)

**Mgr. Pavel Vondruška ( NBÚ )**

## 1. Pravidla soutěže

Naše soutěž probíhala ve čtyřech kolech. V sešitech 9/2000 až 12/2000 jsme postupně uveřejnili po jedné soutěžní úloze a současně uvedli doprovodný text k příslušné úloze. Řešitelé úloh I. až III., kteří zaslali správné řešení do data uvedeného u každé úlohy, byli slosováni a dva vybraní získali cenu kola (certikát k datům pro vytváření elektronického podpisu u poskytovatele certifikačních služeb I.CA resp. AEC ).

Čtvrté kolo bude ukončeno 19.12.2000 ve 20.00 hod. Úplným závěrem soutěže bude losování, které proběhne 21.12.2000. Z řešitelů, kteří vyřeší úlohu tohoto posledního kola, budou opět vylosováni dva výherci s možností získat zdarma certifikát u příslušných poskytovatelů certifikačních služeb a bude také vylosován celkový vítěz. **Celkovým vítězem se tedy může stát i ten soutěžící, který se zapojí do soutěže až nyní a řešení všech čtyřech úloh odešle najednou v časovém limitu do 19.12.2000 !**

Dne 22.12.2000 vyjde speciální číslo, ve kterém budou uvedena řešení úloh ze všech kol, vítězové posledního kola, jméno celkového vítěze , uveřejníme také menší statistiku k celé soutěži a představíme firmy PVT a.s. , AEC spol. s r.o. a Globe Internet s.r.o., které věnovaly ceny do naší soutěže.

Řešení úloh zasílejte pomocí komunikačního okna v oddílu - "SOUTĚŽ" na URL adrese http://www.mujweb.cz/veda/gcucmp/ . Vaše anonymita je zaručena. Uvedena budou pouze celá jména jednotlivých vítězů (nebo bude-li si to dotyčný přát, pak místo jména jeho e-mail adresa, případně pouze pseudonym).

## 2. Informace k cenám

Cenou v jednotlivých kolech je bezplatná registrace vašeho veřejného klíče u certifikační autority (1x u PVT , 1x u AEC). Jde o poskytnutí certifikátu s nejvyšším bezpečnostním stupněm ochrany na dobu 6 měsíců (cena cca 300,- Kč).

Hlavní cenou věnovanou společností Globe Internet, s.r.o., je registrace domény .CZ nebo .SK (podle místa bydliště žadatele) a provoz virtuálního serveru modelu LITE na dobu jednoho roku.

Informace o serveru najdete na adrese
http://servery.cz/index.php3?include=descmodel.inc&c_id=4 .

**Model: LITE server**

---

- 100 MB na disku, 15 e-mailových schránek
- neomezený přenos dat, neomezený přístup přes FTP nebo FrontPage Extensions
- profesionální virtuální obchod GESTO - ZDARMA
- Globe Internet HELPDESK
- pošta přes WWW rozhraní WEBMAIL

- neomezené nastavení aliasů, forward, automatická odpověď, SMS notifikace došlé pošty, doménový koš
- automatické kódování češtiny
- vaše stránky dle obsahu zdarma PC Globe Internet s.r.o. zanese do příslušných kategorií populárních českých a zahraničních vyhledávačů Internetu
- provoz PHP, ASP, PERL a dalších CGI scriptů.
- provoz databázových aplikací MySQL, SYBASE nebo jakýchkoli jiných databází využívajících ODBC rozhraní
- WWW rozhraní pro administraci databáze MySQL
- zjednodušení adresy tak, že není nutné psát "předponu" www .

## 3. Stav po III.kole

| Pseudonym | I.kolo datum /bodů | II.kolo datum /bodů | III.kolo datum/bodů | IV.kolo datum/bodů | CELKEM |
|---|---|---|---|---|---|
| Josef M. | 12.9 /10 ☒ | | 23.11/10 | | |
| Mirek Š. | 12.9 /10 | 17.10/10 | 17.11/10 | | |
| Petr T. | 12.9 /10 | 18.10/10 | | | |
| Bohumír Š. | 12.9 /10 | 18.10/10 | 22.11/10 | | |
| Martin K. | 12.9 /10 | | | | |
| František K. | 12.9 /10 | | | | |
| Tomáš V. | 13.9 /10 ⏢ | 31.10/10 | 26.11/10 | | |
| Jan J. | 13.9 /10 | 17.10/10 | 19.11/10 | | |
| Josef D. | 18.9 /10 | | | | |
| Honza K. | 18.9 /10 | | | | |
| Vašek V. | 2.10/10 | | 22.11/10 ⏢ | | |
| Michal B. | 4.10/10 | 18.10/10 ⏢ | 20.11/10 | | |
| Láďa R. | 4.10/10 | 24.10/10 ☒ | 24.11/10 | | |
| Martin V. | 18.10/10 | | | | |
| Karel Š. | | 24.10/10 | 29.11/10 | | |
| Ivan L. | | 19.10/10 | 17.11/10 | | |
| František P. | 29.11/10 | 23.11/10 | 18.11/10 ☒ | | |

Legenda : cena kola - certifikát u AEC ⏢
cena kola - certifikát u PVT ☒

Vítězové III.kola :
Vašek V. vasekv@hotmail.com
František P. ok1df@qsl.net

Metodiku k úloze čtvrtého kola a úlohu připravil můj bývalý kolega RNDr. Petr Tesař. Řešení této úlohy musíte zaslat do 19.12.2000 !

## Příjemnou zábavu !

# B. Část IV. -
# Substituce složitá periodické heslo, srovnaná abeceda
**RNDr. Petr Tesař (PVT a.s.)**

### 1. Zašifrování

se provádí sečtením hodnoty znaku otevřeného textu (OT) se znakem hesla (H) modulo 26. Výsledkem je znak šifrového textu (ŠT). Heslo je posloupnost kratší než-li OT a používá se periodicky znova. Historicky se šifrování provádělo pomocí čtvercové tabulky 26x26, kde řádky byly označeny A až Z (pro znaky OT) , sloupce také A až Z pro znaky hesla. Na příslušném průsečíku byl v tabulce znak ŠT. Používaly se tři různé tabulky (podle autorů) : Tritheimova, Vigenerova a Beaufortova .

Symbolicky:
Tabulka TRITHEIM ŠT= OT + H mod 26, A=1 , B=2, ……., Z=0
Tabulka VIGENERE ŠT= OT + H mod 26, A=0 , B=1, ……., Z=25
Tabulka BEAUFORT ŠT= OT - H mod 26, A=1 , B=2, ……., Z=0

Příklad :

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| OT : | V | E | S | E | L | E | V | E | L | I | K | O | N | O | C | E |
| HESLO: | R | O | K | R | O | K | R | O | K | R | O | K | R | O | K | R |
| ŠT: | N | T | D | W | A | P | N | T | W | A | Z | Z | F | D | N | W |

Použita tabulka TRITHEIM

### 2. Odšifrování
Odšifrování je inverzní proces, tedy OT = ŠT - H pro TRITHEIM a VIGENERE a
OT = ŠT + H pro BEAUFORT (samozřejmě vše modulo 26).

### 3. Charakter šifrového textu

Vyskytují se zpravidla všechna písmena abecedy. Výskyt písmen je rovnoměrnější než u OT, ale nerovnoměrnější vzhledem k náhodnému textu.
IC (viz PŘÍLOHA) ŠT se pohybuje (podle délky periodického hesla) cca mezi 0.041 - 0.049. V ŠT se mohou projevit i delší opakování, ve sloupcích jednotlivých písmen hesla jde v podstatě o jednoduchou záměnu podle srovnané abecedy navzájem posunuté.

## Luštit lze tento systém i bez znalosti příslušného jazyka!

Jediné co je potřeba znát - jsou frekvence jednotlivých znaků ve zdroji otevřených zpráv. Ze všech příkladů v této soutěži je luštění tohoto systému naprosto nejlehčí. Běžné PC (s vhodným softwarem) vyluští tento systém do jedné vteřiny !

**4. Vzorové luštění**

ZFFLN QATOO AVFTS GQKZN MUXXB FJVVZ FBEPO FQKTN ADTCB OFLEB
UQKZQ ATNKP HBGTV EQXNI GOTXB FFFLU UDDPP XZFAJ MEXGF
PFODB WQKPT LLHFN MOBKE MTXGF ELNEF OOHDU UTHFU QABNJ BPSOF
VJLEB HBCTP BSTGE AWRXJ YBMPN MUBVZ
(text v češtině bez mezerníku)
Počet znaků: 175

Vyhledání opakování trigramů (a delších) v ŠT:

| 7 | 15 | 2 | 5 | 9 | 18 | 6 | 5 | 1 | 5 | 6 | 7 | 6 | 9 | 10 | 9 | 8 | 1 | 3 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| TO | FJ | BO | TC | PO | **FL** | QK | BG | GO | VV | ZN | NQ | UX | QA | OA | OF | **AT** | XJ | CQ | OO |
| VF | EP | TP | DP | BU | LN | TV | FN | | ME | TN | **EB** | EX | **MU** | AV | HB | **KZ** | | OF | SG |
| DT | OF | | PP | QX | TS | OT | DU | | BP | ZQ | UU | OB | AD | FQ | PX | KT | | TG | NA |
| TN | UQ | | BW | XG | JV | FP | FU | | LE | PH | LH | TX | KP | FL | XZ | **KZ** | | | CB |
| JM | GT | | UU | MT | BE | FE | BC | | YB | PT | HF | PN | IG | TX | FO | **AT** | | | NK |
| BN | FF | | | LN | QK | EA | | | | EM | NE | UB | MO | DB | TL | XN | | | VE |
| WR | WQ | | | FO | LE | | | | | | **EB** | | EF | BK | SO | KP | | | XB |
| | KE | | | BH | FF | | | | | | | | JB | OH | BS | AB | | | LL |
| | NJ | | | AW | **FL** | | | | | | | | **MU** | HD | NM | | | | XG |
| | PS | | | | LU | | | | | | | | | FV | | | | | HF |
| | HB | | | | AJ | | | | | | | | | | | | | | PB |
| | CT | | | | PF | | | | | | | | | | | | | | GE |
| | ST | | | | OD | | | | | | | | | | | | | | |
| | MP | | | | NM | | | | | | | | | | | | | | |
| | VZ | | | | EL | | | | | | | | | | | | | | |
| | | | | | OO | | | | | | | | | | | | | | |
| | | | | | UQ | | | | | | | | | | | | | | |
| | | | | | VJ | | | | | | | | | | | | | | |

| 8 | 6 | 2 | 8 | 1 | 6 |
|---|---|---|---|---|---|
| U | V | W | X | Y | Z |
| XX | FT | QK | XB | BM | FF |
| QK | VZ | RX | **BF** | | NM |
| UD | ZF | | NI | | FB |
| DD | EQ | | **BF** | | QA |
| UT | JL | | ZF | | FA |
| TH | Z- | | **GF** | | -- |
| QA | | | **GF** | | |
| BV | | | JY | | |

**IC šifrového textu = 0.04683**

Opakování jsou vyznačena tučně a podtrženě. Zároveň jsme získali i četnosti jednotlivých znaků (vyznačena čísly nad písmeny).

**Zjištění délky periodického hesla**

Při ručním luštění využíváme opakování trigramů a delších. Vychází se z toho, že většina opakování koresponduje s opakováním v OT a vzdálenost těchto opakování je násobkem délky periody. Na počítači zjistíme délku hesla spočtením průměrného IC při rozpisech na různé délky periody. Pro správnou délku bude průměr IC v jednotlivých sloupcích korespondovat s IC u OT. Naopak pro špatné délky bude blízko IC šifrového textu.

| Opakování | pozice | | rozdíl | dělitelé | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1. | 2. | | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| FFL | 2 | 77 | 75 | - | / | - | / | - | - | - | - | - | - | - | - | - |
| LEB | 48 | 148 | 100 | / | - | / | / | - | - | - | - | / | - | - | - | - |
| NMU | 20 | 170 | 150 | / | / | - | / | / | - | - | - | / | - | - | - | - |
| QAT | 6 | 55 | 49 | - | - | - | - | - | / | - | - | - | - | - | - | - |
| QKZ | 17 | 52 | 35 | - | - | - | / | - | / | - | - | - | - | - | - | - |
| XBF | 24 | 74 | 50 | / | - | - | / | - | - | - | - | / | - | - | - | - |
| XGF | 93 | 118 | 25 | - | - | - | / | - | - | - | - | - | - | - | - | - |
| Počet dělitelů | | | | 3 | 2 | 1 | **6** | 1 | 2 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |
| Počet dělitelů*dělitel | | | | 6 | 6 | 4 | **30** | 6 | 14 | 0 | 0 | **30** | 0 | 0 | 0 | 0 |
| Délka opakování*dělitel | | | | 18 | 18 | 12 | **90** | 18 | 42 | 0 | 0 | **90** | 0 | 0 | 0 | 0 |

Označíme si maximální hodnoty heuristik (počet dělitelů, délka opakování*dělitel a suma počet dělitelů*dělitel). Nejpravděpodobnější bude ta perioda, která bude mezi těmi, které mají maximální hodnoty uvedených heuristik. Z tabulky pro náš příklad je vidět, že nejpravděpodobnější perioda hesla je 5. Konkuruje ji pouze její násobek, což je pochopitelné.

Při přesném výpočtu na počítači získáme následující průměrné hodnoty IC pro předpokládané délky hesla:

| Délka hesla | Průměrné IC |
|---|---|
| 1 | 0.04683 |
| 2 | 0.04507 |
| 3 | 0.04685 |
| 4 | 0.04172 |
| **5** | **0.05647** |
| 6 | 0.04860 |
| 7 | 0.04476 |
| 8 | 0.03772 |
| 9 | 0.04763 |
| 10 | 0.05253 |
| 11 | 0.04827 |
| 12 | 0.04560 |
| 13 | 0.04832 |
| 14 | 0.04462 |

Hodnota IC pro periodu 5 je nejblíže hodnotě IC zdroje otevřených zpráv (v daném případě **čeština bez mezerníku = 0.0577**).

V dalším budeme předpokládat délku periodického hesla d = 5. Provedeme rozpis ŠT na délku 5.

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | Z | F | F | L | N |
| 2 | Q | A | T | O | O |
| 3 | A | V | F | T | S |
| 4 | G | Q | K | Z | N |
| 5 | M | U | X | X | B |
| 6 | F | J | V | V | Z |
| 7 | F | B | E | P | O |
| 8 | F | Q | K | T | N |
| 9 | A | D | T | C | B |
| 10 | O | F | L | E | B |
| 11 | U | Q | K | Z | Q |
| 12 | A | T | A | K | P |
| 13 | H | B | G | T | V |
| 14 | E | Q | X | A | I |
| 15 | G | O | T | X | B |
| 16 | F | F | F | L | U |
| 17 | U | D | D | P | P |
| 18 | X | Z | F | A | J |
| 19 | M | E | X | G | F |
| 20 | P | F | O | D | B |
| 21 | W | Q | K | P | T |
| 22 | L | L | H | F | N |
| 23 | M | O | B | K | E |
| 84 | M | T | X | G | F |
| 25 | E | L | A | E | F |
| 26 | O | O | H | D | U |
| 27 | U | T | H | F | U |
| 28 | Q | A | B | A | J |
| 29 | B | P | S | O | F |
| 30 | V | J | L | E | B |
| 31 | H | B | C | T | P |
| 32 | B | S | T | G | E |
| 33 | A | W | R | X | J |
| 34 | Y | B | M | P | N |
| 35 | M | U | B | V | Z |

Četnosti ve sloupcích

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| A | 4 | 2 | 0 | 1 | 0 |
| B | 2 | 4 | 3 | 0 | 6 |
| C | 0 | 0 | 1 | 1 | 0 |
| D | 0 | 2 | 1 | 2 | 0 |
| E | 2 | 1 | 1 | 3 | 2 |
| F | 4 | 4 | 4 | 2 | 4 |
| G | 2 | 0 | 1 | 3 | 0 |
| H | 2 | 0 | 3 | 0 | 0 |
| I | 0 | 0 | 0 | 0 | 1 |
| J | 0 | 2 | 0 | 0 | 3 |
| K | 0 | 0 | 4 | 2 | 0 |
| L | 1 | 2 | 2 | 2 | 0 |
| M | 5 | 0 | 1 | 0 | 0 |
| N | 0 | 0 | 2 | 2 | 5 |
| O | 2 | 3 | 1 | 2 | 2 |
| P | 1 | 1 | 0 | 4 | 3 |
| Q | 2 | 5 | 0 | 0 | 1 |
| R | 0 | 0 | 1 | 0 | 0 |
| S | 0 | 1 | 1 | 0 | 1 |
| T | 0 | 3 | 4 | 4 | 1 |
| U | 3 | 2 | 0 | 0 | 3 |
| V | 1 | 1 | 1 | 2 | 1 |
| W | 1 | 1 | 0 | 0 | 0 |
| X | 1 | 0 | 4 | 3 | 0 |
| Y | 1 | 0 | 0 | 0 | 0 |
| Z | 1 | 1 | 0 | 2 | 2 |

Nyní budeme v každém sloupci zjišťovat "posun" abeced. Pro ruční luštění si vyrobíme proužek papíru, na který napíšeme abecedu dvakrát za sebou. Červeně si označíme 5 nejčetnějších písmen ve zdroji otevřených textů (pro češtinu bez mezerníku to jsou písmena E,A,O,I,N). Modře si označíme 5 nejméně četných písmen (pro češtinu bez mezerníku to jsou písmena G,F,W,X,Q). Přiložíme tuto šablonu na příslušný sloupec frekvencí ŠT a spočteme rozdíl četností mezi součtem na červených pozicích proti součtu na modrých. Potom šablonu o jedno písmeno posuneme a opět spočteme rozdíl. Při správném posunu bude rozdíl největší a bude odpovídat statisticky očekávanému.

V našem případě platí:
Pravděpodobnosti výskytu červených písmen ve zdroji OT jsou (pro Angličtinu bez mezerníku ve druhém sloupci)

| | |
|---|---|
| E = 0.1013 | E = 0.1260 |
| A = 0.0899 | T = 0.0904 |
| O = 0.0839 | R = 0.0826 |
| I = 0.0692 | I = 0.0757 |
| N = 0.0664 | N = 0.0756 |
| Celkem = 0.4107 | Celkem = 0.4503 |

Pro modré platí

| | |
|---|---|
| G = 0.0048 | X = 0.0047 |
| F = 0.0033 | K = 0.0035 |
| W = 0.0006 | Q = 0.0032 |
| X = 0.0004 | J = 0.0020 |
| Q = 0.0000 | Z = 0.0010 |
| Celkem = 0.0091 | Celkem = 0.0144 |

Pro rozdíl: červené - modré = 0.4107 - 0.0091 = 0.4016 ( 0.4359 pro angličtinu)

Protože v každém sloupci je přesně 35 písmen, měl by při správném posunu být rozdíl 35 * 0.4016 = 14.056

Pro náš příklad spočteme tuto tabulku:

Znak A v ŠT koresponduje v OT

| s písmenem: | Sloupec 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| A | -2 | -4 | -5 | 0 | 5 |
| B | -1 | -5 | 1 | -5 | -3 |
| C | 1 | -7 | 1 | -3 | -8 |
| D | 5 | 3 | 9 | 0 | 1 |
| E | 0 | -2 | -5 | 1 | -3 |
| F | -5 | -3 | -5 | 3 | 0 |
| G | -1 | -6 | -1 | -4 | 1 |
| H | 2 | -2 | **15** | 4 | -2 |
| I | 6 | 4 | 1 | -3 | -1 |
| J | 2 | 3 | -3 | 2 | 2 |
| K | -1 | 8 | -3 | -2 | 0 |
| L | -12 | -3 | 2 | 8 | -4 |
| M | -1 | 1 | -5 | -8 | 3 |
| N | 7 | -1 | -3 | -3 | 7 |
| O | **15** | 7 | -2 | 2 | 1 |
| P | -2 | -2 | -1 | **12** | -2 |
| Q | -7 | -4 | 6 | -1 | -1 |
| R | -8 | -6 | 1 | -8 | -3 |
| S | 0 | -1 | -6 | -7 | -10 |
| T | 0 | 3 | -3 | -2 | 0 |
| U | 0 | 3 | 5 | 6 | 6 |
| V | 0 | 3 | 3 | 1 | 7 |
| W | -2 | -8 | -3 | 0 | -8 |
| X | 0 | 1 | 3 | -3 | -6 |
| Y | 1 | 4 | 2 | 8 | 0 |
| Z | 3 | **14** | -1 | 2 | **18** |

Tučně s podtržením jsou označeny maximální hodnoty, korespondující se správnými posuny. Průměrná hodnota těchto maxim je 14.8 , což velmi dobře souhlasí s teoretickou očekávanou hodnotou 14.056. Získáváme tak posun ve všech sloupcích:

| ŠT | OT | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| A | | O | Z | H | P | Z |
| B | | P | A | I | Q | A |
| C | | Q | B | J | R | B |
| D | | R | C | K | S | C |
| E | | S | D | L | T | D |
| F | | T | E | M | U | E |
| G | | U | F | N | V | F |
| H | | V | G | O | W | G |
| I | | W | H | P | X | H |
| J | | X | I | Q | Y | I |
| K | | Y | J | R | Z | J |
| L | | Z | K | S | A | K |
| M | | A | L | T | B | L |
| N | | B | M | U | C | M |
| O | | C | N | V | D | N |
| P | | D | O | W | E | O |
| Q | | E | P | X | F | P |
| R | | F | Q | Y | G | Q |
| S | | G | R | Z | H | R |
| T | | H | S | A | I | S |
| U | | I | T | B | J | T |
| V | | J | U | C | K | U |
| W | | K | V | D | L | V |
| X | | L | W | E | M | W |
| Y | | M | X | F | N | X |
| Z | | N | Y | G | O | Y |

Nyní již snadno získáme OT:
NEMAM EZADN OUMIR UPROM ATEMA TICKY TALEN TPRIM OCARA CESTA IPROP OSUZO VANIU SPECH UNAMA TEMAT ICKEO LYMPI ADEVE DEVSA KPRES ZKOUM ANIZD ASEVE SKUTE CNOST ISOUT EZICI POZDE JISTA VAJIO PRAVD OVYMI MATEM ATIKY

Při luštění pomocí počítače můžeme použít důmyslnější (a tím i výpočetně náročnější) statistiky jako korelace, PHI a KAPPA testy atp. Výhodou je naopak to, že luštíme i případy, kdy bylo periodické heslo použito méněkrát.

Poslední co zbývá zjistit, je zda použité heslo má sémanticky smysluplný význam při použití tabulek VIGENERE, TRITHEIM nebo BEAUFORT (jak bývá z důvodu zapamatování periodického hesla zvykem…).

Písmeno A v OT se šifruje v jednotlivých sloupcích na

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| M | B | T | L | B |

V případě použití VIGENERE je potom heslo: MBTLB.

V případě použití BEAUFORT je potom heslo: NYGOY.
V případě použití TRITHEIM je potom heslo: LASKA.
**Správné heslo je LASKA a byla použita tabulka TRITHEIM.**

# PŘÍLOHA

Index coincidence (dále jen IC) je pravděpodobnost výskytu dvojice stejných písmen ve dvou textech na stejných pozicích. Tato statistika se v klasické kryptoanalýze hojně používá. Hodnota IC pro různé jazyky (v mezinárodní abecedě, bez mezerníku):

| | |
|---|---|
| Angličtina | 0.0667 |
| Francouzština | 0.0778 |
| Němčina | 0.0762 |
| Italština | 0.0738 |
| Španělština | 0.0775 |
| Ruština | 0.0529 |
| Čeština | 0.0577 |
| Náhodný text | 0.0385 |

Četnosti písmen v angličtině ( podle S.Kullback: Statistical Methods In Cryptanalysis, Aegean Park Press, 1976):
A = 0.07189, B = 0.01146, C = 0.03345, D = 0.04029, E = 0.12604, F = 0.02994
G = 0.01795, H = 0.03287, I = 0.07572, J = 0.00198, K = 0.00353, L = 0.03549
M = 0.02534, N = 0.07558, O = 0.07408, P = 0.02661, Q = 0.00318, R = 0.08256
S = 0.05759, T = 0.09042, U = 0.02993, V = 0.01340, W = 0.01401, X = 0.00469
Y = 0.02099, Z = 0.00101

### Soutěžní příklad 4.kolo soutěže:

ZZLES FMDCU LQMEW SGWLM XHZUY ZRJKU SGKBM GNBEU VPJCT
VNGVW HPLOY VLBAM RIIZN UJVKH XADVV GBQWX OOTKM RSEMV
THMEU SNZMS FHPPB KTQKK IZVPU ABGVT CWXKE FZNLY YVINE
UTOGP MGCPM ESYBZ OAVHG QDYOD ITKBC SUGPH VDGVP QDVLB
NPFCP NYZQX QULBK GMIXI BVCHR FYYWD OPEGL EGVCA QWMUE
XBWXG KIIGH RTJIU WYYJB BSPPS VLTDO PLJNL DYODI TKBCS
UGPHV DGVPQ DVJYN PFVPN YZQXW EMGYO GEFCH CMOEI VLGQE
TWBWX GFANB RWECG KWLOK LRYGZ RHSKV EAVAB SVKLC XYWBA
JPARK ZRGEW MBRZE RAWJR AGTZZ SENRP

(Angličtina bez mezerníku)

Řešení této úlohy musíte zaslat do 19.12.2000 !

Řešení úlohy zašlete pomocí komunikačního okna v oddílu - "SOUTĚŽ" na URL adrese http://www.mujweb.cz/veda/gcucmp/ !

# C. CRYPTONESSIE

**Ing. Jaroslav Pinkava, CSc. (AEC spol. s r.o./ Norman Czech Republic)**

## Úvod

V první polovině letošního roku byl zahájen projekt NESSIE: *New European Schemes for Signatures, Integrity, and Encryption*. Cílem tohoto evropského projektu je přinést rozsáhlé portfolio tzv. kryptografických primitivů, které projdou procesem veřejné evaluace.

Do konce září 2000 bylo třeba podat jednotlivé návrhy a v návaznosti na to ve dnech 13-14. listopadu 2000 se konala první pracovní konference (workshop) této iniciativy (Leuven, Belgie).

Úkolem této stati je provést přehled podaných příspěvků spolu s jejich stručnými charakteristikami.

Přijaté návrhy

Přehled návrhů lze nalézt na adrese:
https://www.cosic.esat.kuleuven.ac.be/nessie/workshop/submissions.html
spolu s odkazy na stránky, kde jsou umístěny jednotlivé dokumenty.

## 64-bit blokové šifry

### A1.: CS-Cipher

Návrh přichází z CS Communication & Systèmes (Francie) a na jeho vývoji se podíleli dále Jacques Stern a Serge Vaudenay. Algoritmus vznikl v roce 1998. Druhý z autorů přednesl k danému algoritmu referáty na konferenci FSE (Fast Software Encryption) v letech 1998 a 1999 (specifikace algoritmu a bezpečnost algoritmu).

Algoritmus pracuje s délkou bloku 64 bitů a proměnlivou délkou klíče 40-128 bitů. Šifrování probíhá celkem v 8 iteracích a opírá se o použití rychlé Fourierovy transformace. Šifra je optimalizována pro hardwarové implementace.

### A2.: Hierocrypt-L1

S tímto algoritmem přichází známá japonská firma Toshiba (algoritmus vyvíjeli Kenji Ohkuma, Fumihiko Sano a Hirofumi Muratani).

Algoritmus pracuje s klíči v délce 128, 192 a 256 bitů v celkem 6 iteracích. Je formován tak, aby bylo jednoduché provést jeho programování v závislosti na hodnotách bajtů, tj. je využitelný i pro 8-bitové počítače.

### A3.: IDEA

Známý algoritmus, majitelem je firma Ascom (Švýcarsko). Jeden čas byl zvažován jako evropská norma. Algoritmus vznikl v roce 1991.

Pracuje s 64-bitovým blokem textu a používá 128 bitový klíč. Algoritmus pracuje v 8 iteracích.

### A4.: Khazad

Algoritmus předkládají Paulo Sérgio L.M. Barreto a Vincent Rijmen ( jeden z autorů algoritmu Rijndael, vítěze AES).

Je to opět 64 bitová šifra s délkou klíče 128 bitů. Algoritmus pracuje v 8 iteracích. Je navržen tak, aby s jeho pomocí bylo lze dosáhnout vysokých rychlostí šifrování na široké variabilitě platforem. Nevyžaduje přitom velké objemy paměti.

**A5.: MISTY1**

Mitsubishi Electric Corporation je majitelem patentu pro tento algoritmus (autorem je známý japonský kryptolog Mitsuru Matsui). Algoritmus byl poprvé opublikován v Japonsku v roce 1996 (a prezentován na FSE v roce 1997).

Algoritmus MISTY1 je 64 bitová šifra pracující s klíčem v délce 128 bitů. Počet iterací je volitelný, doporučováno je užití 8 iterací. Algoritmus lze implementovat i v prostředí s velmi malým objemem paměti RAM (např. 100 bajtů).

**A6.: Nimbus**

Algoritmus předkládá Alexis Warner Machado (Brazilie). Je to nový algoritmus.

Schéma algoritmu pracuje v 8 iteracích. Je to 64 bitová šifra s délkou klíče 128 bitů. Používá pouze tři typy operací: násobení (mod $2^{64}$), součet modulo dva a bitovou negaci.

## 128-bit blokové šifry

**B1.: Anubis**

Návrh předkládají (stejně jako algoritmus Khazad) Paulo Sérgio L.M. Barreto a Vincent Rijmen.

Je to 128 bitová šifra s variabilní délkou použitého klíče (počet bitů - 32N, $4 \leq N \leq 10$). Počet iterací algoritmu je roven 8 + N, kde N je počet 32 bitových slov klíče.

**B2.: Camellia**

Algoritmus předkládá Mitsubishi Electric Corporation. Autory jsou Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, Toshio Tokita. Jedná se o nový algoritmus.

Algoritmus pracuje s bloky textu v délce 128 bitů a s klíčem v délce 128, 192 a 256 bitů, tj. odpovídá podmínkám pro AES. Je to Feistelova šifra, která probíhá v 18 iteracích (128 bitový klíč), resp. v 24 iteracích (192 bitový a 256 bitový klíč).

**B3.: Grand Cru**

Návrh předkládá známý belgický odborník Johan Borst. Je to nový algoritmus, který svou konstrukcí se značně opírá o algoritmus Rijndael.

Algoritmus je koncipován pro délku textu 128 bitů a délku klíče rovněž 128 bitů. Pracuje ve čtyřech tzv. vrstvách (layer). Svojí architekturou je algoritmus primárně určen pro 8 bitové aplikace.

**B4.: Hierocrypt-3**

Algoritmus předkládá Toshiba. Autory jsou pánové Kenji Ohkuma, Fumihiko Sano, Hirofumi Muratani, Masahiko Motoyama a Shinichi Kawamura.

Algoritmus pracujes blokem textu v délce 128 bitů a s klíči v délce 128 (resp.192 a 256) bitů v celkem 6 (resp. 7, 8) iteracích. Je formován tak, aby bylo jednoduché provést jeho programování v závislosti na hodnotách bajtů, tj. je využitelný i pro 8-bitové počítače – stejně jako Hierocrypt L1.

**B5.: Noekeon**

Algoritmus předkládá Joan Daemen spolu s pány Gilles Van Assche a Vincent Rijmen.

Tato bloková šifra je určena k zašifrování 128 bitových bloků dat pomocí klíče v délce 128 bitů. Pracuje v 16 iteracích. Opět je určena především k implementacím na čipových kartách.

**B6.: Q**

Autorem návrhu je pan Leslie 'Mack' McBride z firmy Mack One Software.

Bloková šifra pracuje s bloky textu v délce 128 bitů. Dle autora umožňuje libovolnou délku „hesla“. Fakticky pracuje s klíčem v délce nejvýše 256 bitů. Počet iterací je 8 nebo 9. Design algoritmu má vycházet z lepších vlastností algoritmů Rijndael a Serpent.

**B7.: SC2000**

Algoritmus předkládá japonská firma Fujitsu. Jeho autory jsou Takeshi Shimoyama, Hitoshi Yanami, Kazuhiro Yokoyama, Masahiko Takenaka, Kouichi Itoh, Jun Yajima , Naoya Torii a Hidema Tanaka. Jedná se o nový algoritmus.

Bloková šifra SC2000 pracuje se 128 bity textu a lze používat klíče vdélce 128, 192 a 256 bitů. Počet iterací je pro 128 bitový klíč roven 14 iteracím tzv. I-funkce a 19 iteracím zpracovávajícím data. Při klíči v délce 192 a 256 bitů jsou tato čísla rovna 16 a 22.

## 160-bit blokové šifry

**C1.: SHACAL**

Předkladateli tohoto návrhu jsou Helena Handschuh a Daavid Naccache (Gemplus)

Návrh je založen na využití hashovací funkce SHA-1 v „šifrovacím módu“. K tomu využívá kompresní funkce algoritmu SHA-1. Klíč je v délce 512 bitů, přitom lze používat i kratší klíče, které jsou převáděny na 512 bitový klíč doplněním o nuly na příslušná místa. SHSACAL by však neměl používat klíče kratší než 128 bitů.

## Blokové šifry s proměnnou délkou bloku

**D1.: NUSH:**

Tento příspěvek pochází z Ruska. Jeho autory jsou Anatolij Lebeděv (firma LAN Crypto Int.) a Alexej Volčkov („RusCrypto“ Association). Nejedná se vlastně jen o jeden návrh, ale součástí je více algoritmů z různých kategorií : bloková šifra, dva typy hashovacích funkcí, MAC, asymetrické šifrování, pseudonáhodná funkce, samosynchronizující proudová šifra, synchronní proudová šifra a asymetrická šifra pro digitální podpis.

Bloková šifra je rozpracována přitom pro tři délky bloků: 64, 128 a 256 bitů. Počet iterací algoritmu je přitom adekvátně 9, 17 a 33. Všechny tři verze mohou přitom pracovat s klíči v délkách 128, 192 a 256 bitů. Proudové šifry jsou odvozeny z blokového algoritmu. Analogicky toto platí pro hashovací funkce, MAC a pseudonáhodnou funkci. Asymetrické primitivy kombinují zajímavým způsobem problematiku diskrétního logaritmu svyužitím algoritmu blokové šifry NUSH.

**D2.: RC6**

Tento algoritmus je znám již ze své přihlášky v rámci AES. Jeho autory jsou Ronald L. Rivest, Matthew J. B. Robshaw, Raymond M. Sidney a Yiquin Lisa Yin (RSA Security Inc.).

RC6 má jako proměnné parametry délku slova w (v bitech), počtu iterací r a délku klíče b (v bajtech). Autoři šifru pak označují RC6-w/r/b. Podrobnější popis algoritmu je již znám z AES.

**D3.: SAFER++:**

Tento algoritmus pochází ze známé firmy Cylink. Jeho autoři jsou James L. Massey (jméno velice známé z kryptologických konferencí), Gurgen H. Khachatrian a Melsik K. Kuregian. Algoritmus ve své koncepci vychází z předcházejících členů rodiny algoritmů SAFER.

Algoritmus je navržen v následujících variantách (délka bloku, délka klíče): (128,256), (128,128), (64,128). Jeho využití je již od osmibitových procesorů výše. Počet iterací je 7 při délce klíče 128 bitů, resp. 10 při délce klíče 256 bitů.

## Synchronní proudové šifry

**E1.: BMGL**

Daný příspěvek předkládá Johan Hastad (Švédsko). Algoritmus se opírá o teoretické výsledky pánů Blum, Micali, Goldreich a Levin. Základem je přitom bloková šifra Rijndael.

Konstrukce proudové šifry je přitom vytvářena tak, aby byla tzv. prokazatelně bezpečná. To odpovídá současným trendům kryptografie. Součástí návrhu jsou i výsledky statistických testů (Diehard, Maurerův univerzální test).

**E2.: Leviathan**

Cisco Systems Inc. přichází s dalším návrhem (autory algoritmu jsou pánové David A. McGrew a Scott R. Fluhrer.

Šifrování spočívá v přičítání jednotlivých bitů hesla k otevřenému textu. Délka klíče je 128 resp. 256 bitů. Vlastní heslo je vytvářeno na základě tzv. binárního stromu.

**E3.: LILI-128**

Předkladatelem je australský kryptolog E. Dawson, který je spoluautorem návrhu spány L. Simpson, J. Golič a W. Millan.

Algoritmus se opírá o použití lineárních registrů se zpětnou vazbou. délka klíče je 128 bitů – jak již napovídá název algoritmu.

**E4.: SNOW**

Autorem návrhu je Thomas Johansson, Lund University (Švédsko).

Šifra pracuje s 32-bitovými slovy, opírá se opět o použití lineárních registrů se zpětnou vazbou spolu v kombinaci s blokem FSM (Finite State Machine). Délka klíče může být 128 nebo 256 bitů.

**E5.: SOBER-t16**

Předkladatelem je pan Philip Hawkes (Qualcomm International – Austrálie). Je odvozen z algoritmu SOBER (1998).

Daný algoritmus je synchronní proudová šifra s délkou klíče maximálně 128 bitů. algoritmus je orientován na softwarové implementace (16-bitové). Ke konstrukci jsou rovněž použity lineární registry se zpětnou vazbou.

**E6.: SOBER-t32**

Varianta předešlého algoritmu umožňující používat klíče až do délky 256 bitů a pracující se slovy v délce 32 bitů.

## Autentizační kódy zpráv (MAC)

**F1.: Two-Track-MAC**

Předkladatelem je Bart Van Rompay, autorem Bert den Boer – oba pracují na univerzitě Leuven – Belgie.

V základu algoritmu je využití hashovací funkce RIPEMD-160. Algoritmus spočítá 160 bitovou hodnotu MAC a používá 160 bitový klíč.

**F2.: UMAC**

Intel přichází s tímto algoritmem, autory jsou John Black, Shai Halevi, Hugo Krawczyk, Ted Krovetz a Phillip Rogaway.

Algoritmus je MAC v duchu Wegman-Carterovy koncepce. Lze použít klíče v délce 128 a 256 bitů, výstupní délka je 32*N, $1 \leq N \leq 8$.

## Hashovací funkce rezistentní vůči kolizím a jednocestné hashovací funkce

**G1.: Whirlpool**

Algoritmus předkládají Paulo Sérgio L.M. Barreto a Vincent Rijmen.

Hashovací funkce má 512-bitový výstup. Je jednocestná a rezistentní vůči kolizím. Stejně jako KHAZAD a ANUBIS se opírá o použití konečných těles $GF(2^8)$.

Poznámka: Původně jsem se (dle přehledu na webovských stránkách NESSIE) domníval, že je to jediná hashovací funkce obsažená v přijatých návrzích. Ukázalo se, že další hashovací funkce jsou zahrnuty v rámci popisu jiných kryptografických primitivů.

## Asymetrická šifrovací schémata

**H1.: ACE Encrypt**

Autorem návrhu je Victor Shoup z IBM Zurich Research Laboratory spolu s Ronaldem Cramerem. Daný návrh je také součástí materiálů pracovní skupiny P1363 (Future Public Key Cryptography Study Group).

Podstatou algoritmů jsou tzv. prokazatelně bezpečná schémata. Návrh je pojat velice komplexně a dotažen až do podoby softwarové knihovny.

Poznámka: Nevýhodou koncepce je, že nebyla zatím dotažena i pro využití algoritmů na bázi eliptických křivek (např. P1363 obsahuje eliptické algoritmy jako jednu ze tří základních rodin systémů s veřejným klíčem). Bezpečná délka klíče RSA (a totéž platí pro diskrétní logaritmus) může být totiž již v některých aplikacích na obtíž. Stačí zmínit požadovanou délku klíče algoritmu RSA při výměně 256 bitových tajných klíčů pro symetrickou šifru. Některé odhady hovoří o nezbytnosti používat pro dosažení adekvátní bezpečnosti klíč RSA v délce cca 14 000 bitů atd.

**H2.: ECIES**

Návrh podává Certicom a obsahuje známá schemata ECIES a ECDSA z práce skupin SECG a P1363.

**H3.: EPOC**

Návrh podává Nippon Telegraph and Telephone Corporation (NTT). Autory jsou Eiichiro Fujisaki, Tetsutaro Kobayashi, Hikaru Morita, Hiroaki Oguro, Tatsuaki Okamoto, Satomi Okazaki, David Pointcheval a Shigenori Uchiyama .

Jedná se vlastně o tři návrhy (EPOC-1, EPOC-2 a EPOC-3) pravděpodobnostních systémů s veřejným klíčem. Schémata se opírají o koncepci prokazatelné bezpečnosti. Kryptografická odolnost schémat (totální zkoušky) je např. při délce klíče 1024 bitů srovnatelná s bezpečností RSA při téže délce klíče.

**H4.: PSEC**

Návrh podává rovněž Nippon Telegraph and Telephone Corporation (NTT). Autoři: Eiichiro Fujisaki, Tetsutaro Kobayashi, Hikaru Morita, Hiroaki Oguro, Tatsuaki Okamoto, Satomi Okazaki a David Pointcheval.

Konečně prokazatelně bezpečná schémata na bázi eliptických křivek. Jinak se jedná o eliptický analog předešlého návrhu (opět existují tři verze PSEC-1, Psec-2 a PSEC-3, atd.). Koho toto zajímá, nechť si prohlédne tabulku na straně 18 ukazující jednoznačné výhody eliptických kryptosystémů.

**H5.: RSA-OAEP**

Předkladatelem je ovšem RSA Security Inc. Autory OAEP jsou Mihir Bellare a Philip Rogaway, autory RSA Ronald Rivest, Adi Shamir a Leonard Adleman.

Specifikace OAEP je známá z dokumentu PKCS 1 v.2.0.

## Asymetrická schémata pro digitální podpis

**I1.: ACE Sign**

viz ACE Encrypt.

**I2.: ECDSA**

viz ECIES

**I3.: ESIGN**

Předkládá opět Nippon Telegraph and Telephone Corporation (NTT). Autoři: Eiichiro Fujisaki, Tetsutaro Kobayashi, Hikaru Morita, Hiroaki Oguro, Tatsuaki Okamoto a Satomi Okazaki.

ESIGN je prokazatelně bezpečné schéma. Doporučená délka klíče je 1152, autoři však uvádí, že schéma je podstatně rychlejší než RSA či dokonce i eliptické křivky.

**I4.: FLASH**

Návrh předkládají francouzští kryptologové. Autory jsou Jacques Patarin, Louis Goubin a Nicolas Courtois.

Dle anotace se jedná o rychlé podpisové schéma pro cenově dostupné čipové karty. Schéma má být podstatně rychlejší než RSA avšak použitý veřejný klíč má větší délku – 18 kilobajtů, podpis má délku 296 bitů. Soukromý klíč v délce 2,75 kilobajtů je generován ze seedu v minimální délce 128 bitů.

**I5.: QUARTZ**

Titíž autoři jako u předešlého návrhu, tj. Jacques Patarin, Louis Goubin a Nicolas Courtois.

Dle anotace je schéma určeno k vytváření velmi krátkých podpisů (128 bitů). Délka veřejného klíče je 71 kilobajtů, soukromý klíč v délce 3 kilobajty je generován ze seedu 128 bitů. Předpokládá se implementace na PC.

**I6.: RSA-PSS**

RSA Laboratories předkládají schéma RSA-PSS. Autory PSS metody jsou Mihir Bellare a Phillip Rogaway. Schéma je součástí návrhů skupiny P1363.

Jedná se o kombinaci algoritmu RSA s metodou kódování označenou jako pravděpodobnostní podpisové schéma (EMSA-PSS).

**I7.: SFLASH**

Titíž autoři jako u návrhu algoritmů FLASH a QUARTZ, tj. Jacques Patarin, Louis Goubin a Nicolas Courtois.

Opět se jedná o rychlé podpisové schéma pro cenově dostupné čipové karty. Schéma má být podstatně rychlejší než RSA přitom použitý veřejný klíč má délku – 2,2 kilobajtů, podpis má délku 259 bitů. Soukromý klíč v délce 0,35 kilobajtů je generován ze seedu v minimální délce 128 bitů.

## Asymetrická identifikační schémata

**J.: GPS**

Předkládá France Télécom a La Poste. Autory návrhu jsou Marc Girault, Guillaume Poupard a Jacques Stern.

Jedná se o asymetrické identifikační schéma s nulovým předáním znalostí. Toto schéma kombinuje prokazatelnou bezpečnost založenou na složitosti obecné úlohy diskrétního logaritmu s krátkými klíči, krátkou dobou přenosu a minimálním on-line výpočty. Schéma je určeno k implementacím na cenově dostupných čipových kartách (bez kryptografického procesoru).

## K. Testovací metodologie

**K1.: Using the general next bit predictor like an evaluation criteria**

Autoři pochází ze Španělska: J.C. Hernández, J.M. Sierra, C. Mex-Perera, D. Borrajo, A. Ribagorda a P. Isasi.

Dokument popisuje prediktor dalšího bitu posloupnosti na základě principu samoučícího se stroje.

## Shrnutí

Zatím nebyl v historii kryptologie obdobný moment – předložení tak velkého počtu kryptografických primitivů k veřejnému projednání. První dojem také říká, že toto velké množství různorodých návrhů (díky zadání celého konkursu) je odlišné nejen svým zaměřením, ale asi i kvalitou. Některé návrhy jsou hluboce rozpracovány, jiné přináší nové myšlenky, některé však zase budí dojem, že by neškodila přiložená hlubší analýza. Některé sekce také trpí malou konkurencí návrhů. Je to ovšem teprve začátek a je pravděpodobné, že po první etapě projednávání předložených návrhů (spolu s vyřazením některých z nich) se celkový obraz změní.

# D. Kryptografie a normy

**Ing. Jaroslav Pinkava, CSc. (AEC spol. s r.o./ Norman Czech Republic)**

## Díl 4.
## Normy PKCS (Public-Key Cryptographic Standards) - PKCS #6, PKCS #7, PKCS #8

### Úvod

Dnešní část seriálu bude věnována hned třema titulům z řady PKCS. První z nich PKCS #6 je věnován rozšířením (extensions) certifikátů dle X. 509, druhý se zabývá syntaxí kryptografické zprávy (CMS – Cryptographic Message Syntax). Třetí PKCS#8 popisuje syntaxi pro informaci o obsahu soukromého klíče.

### PKCS #6

Všem třem normám se budeme věnovat jen velmi krátce. Jejich význam je totiž dnes již spíše jen historický, jsou dnes vlastně překonány a jejich obsah je výrazně podrobněji a moderněji rozpracován v následných normách.

První verze PKCS#6 vznikly v roce 1991, poslední aktualizovaná verze má číslo 1.5 a pochází z roku 1993.

Norma popisuje syntaxi tzv. rozšířených certifikátů. Tím je míněn klasický X.509 certifikát (v jedné z prvních verzí normy X.509) a obsahující navíc množinu atributů. Vše je spolu souhrnně podepsáno vydavatelem certifikátu X.509. Záměrem tohoto postupu bylo tehdy především umožnit zahrnout do certifikátu některé další informace jako je mailová adresa (použití v PEM – Privacy Enhanced Mail).

Uvedené postupy jsou dnes aplikovány samozřejmě ve výrazně širší podobě. Zahrnuje to především samo vydání nových verzí normy X.509 (v letošním roce se objevila zatím poslední z nich – výrazně se zabývá i podobou atributových certifikátů – draft revised ISO/IEC 9594-8). Dále je užitečné v této souvislosti poukázat na drafty a rfc skupiny IETF-pkix:

Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459) - rfc2459.txt
An Internet AttributeCertificate Profile for Authorization - draft-ietf-pkix-ac509prof-04.txt
Internet X.509 Public Key Infrastructure Certificate and CRL Profile – - draft-ietf-pkix-new-part1-02.txt

Protože se těmto normám budeme věnovat v rámci popisu výsledků práce dané skupiny – je tak možno lépe postihnout některé další souvislosti – obrátíme se na další normu v pořadí s číslem sedm popisované řady PKCS.

## PKCS #7

Opět první verze vznikly v roce 1991, poslední aktualizovaná verze má rovněž číslo 1.5 a pochází z roku 1993.

Norma popisuje syntaxi dat, která jsou následně šifrována – příkladem mohou být digitální podpisy a digitální obálky. Je zde povolena rekurze, tj. například jedna obálka může být umístěna v druhé obálce, nebo lze znovupodepisovat již dříve podepsaná data. Jsou povoleny různé atributy (např. časový okamžik podpisu), které lze podepsat spolu se zprávou.

Vzhledem opět k době vzniku normy je zde zvažována především kompatibilita s PEM v tom smyslu, že podepsaná data lze bez dalších kryptografických operací konvertovat na zprávy v podobě PEM (rfc1421-3).

Materiál popisuje v definicích několik tzv. typů, identifikátory objektů a obecnou syntaxi. Syntaxe podporuje celou řadu typů obsahu, jmenovitě následujících šest:

data,
signed data,
enveloped data,
signed-and-enveloped data,
digested data,
encrypted data.

Podrobněji se k těmto definicím vrátíme při popisu současných norem z této oblasti jako je Cryptographic Message Syntax (RFC 2630) zpracovaný skupinou IETF-S/MIME Mail Security a některé doplňující drafty popisující použití konkrétních algoritmů (např. RSA-OAEP) v návaznosti na CMS.

## PKCS #8

Norma nese název Private-Key Information Syntax Standard (Syntaxe informace o soukromém klíči) a její první verze se objevila rovněž v roce 1991. Poslední je verze 1.2 z roku 1993.

Norma je velice stručná a v podstatě říká, že informace o soukromém klíči (vzhledem k nějakému kryptografickému algoritmu s veřejným klíčem) obsahuje tento soukromý klíč a určitou množinu atributů. K zašifrování této informace lze použít šifrovací algoritmus založený na použití hesla (např. popsaný v PKCS#5). Smyslem atributů je připravit jednoduchou cestou ustavení určité důvěry užitím informace jako jsou DN (distinguished name) anebo veřejný klíč CA. Seznam takovýchto atributů je pak obsažen např. v PKCS#9.

Tato norma svým způsobem není v současnosti příliš užitečná. K ochraně soukromého klíče se přistupuje dnes celou řadou způsobů. K problematice se vrátíme při popisu PKCS#12.

# E. **Letem šifrovým světem**

Informace pro odběratele e-zinu. Prosím nepřehlédněte změnu e-mail spojení. Od 1.12.2000 jsem nastoupil na ÚOOÚ do Odboru elektronického podpisu. Moje nová e-mail adresa bude vondruskap@uoou.cz (bude však zprovozněna v nejbližších dnech, zatím lze využívat adresu bosakovad@uoou.cz nebo stedronb@uoou.cz ).
Adresa pavel.vondruska@post.cz je stále platná.

1. Úřad pro ochranu osobních údajů (dále jen "Úřad") zveřejnil na adrese http://www.e-podpis.cz tzv. teze k Zákonu č. 227/2000 Sb., o elektronickém podpisu. Teze připravil kolektiv pracovníků Úřadu a odborné pracovní skupiny jmenované předsedou Úřadu RNDr. Karlem Neuwirtem. (jmenovité složení komise je dostupné na adrese http://www.uoou.cz/ep_skupina.html ) . Na této adrese "e-podpis" je také otevřena oficiální veřejná diskuse k jednotlivým tezím vyhlášky. Příspěvky v této diskusi Úřad využije ke své další práci nad tezemi vyhlášek.… Úřad nemá v současné době v provozu vlastní server a využil tedy možnosti použít bezplatně, bez smluvních závazků, do doby uvedení funkčního serveru Úřadu do provozu, prostor serveru e-podpis. Teze Úřad podstoupil i jiným serverům, ale oficiální diskuse je vedena jen na tomto serveru. Úřad 4.12.2000 také seznámil s obsahem tezí 25 subjektů, které přislíbily zaslat své písemné vyjádření do 15.12.2000. Na 20.12.2000 se na Úřadě připravuje setkání pracovníků Úřadu, členů odborné skupiny a těchto subjektů. Na tomto setkání se budou hodnotit jednotlivé připomínky k tezím. Jména subjektů (případně jejich písemná stanoviska) Úřad vhodným způsobem zveřejní. Výsledky těchto akcí budou následně během ledna 2001 zapracovány do připravovaných tezí. Termíny jsou opravdu vražedné, ale vycházejí z požadavků, které jsou na Úřad kladeny. Všem, kteří se zapojili nebo zapojí do diskuse touto cestou děkuji. Dnešní příloha - teze vyhlášky a doprovodné prezentace - vám mají umožnit lepší orientaci v této problematice.

2. Schválení zákona o elektronickém podpisu mělo dle odhadu odborníků podpořit rozvíjející se elektronický obchod na Internetu v USA. Skutečnost však je zcela opačná. Oslnivý nástup amerických firem obchodujících po Internetu letos skončil. Dokonce kolem 130 firem muselo ukončit svoji činnost a propustit kolem osmi tisíc zaměstnanců. Z těchto 130 firem se 60% zabývalo přímo elektronickým obchodem a přibližně 20% nabízelo různé servisní služby podnikatelské sféře. http://www.webmergers.com

3. "Bankovní institut vysoká škola a.s." pořádal 7.12.2000 jednodenní seminář s názvem "Elektronický podpis - využití v bankovnictví". Jako lektoři byli pozváni Ing.Jaroslav Pinkava a Mgr.Pavel Vondruška. Seminář se skládal ze sedmi samostatných lekcí. Oba dva lektoři slíbili zveřejnit své prezentace . Mimo sedmdesáti posluchačů semináře se tak s nimi můžete seznámit i vy a stáhnout si je z našeho webu: http://www.mujweb.cz/veda/gcucmp/ sekce BANKA.

4. Hackerům pravděpodobně vyhovují dlouhé zimní večery a předvánoční období. Tak jako loni i letos jsme již mohli zaznamenat řadu "úspěšných" útoků na stránky různých subjektů (KSČM, Ministerstvo vnitra, Český rozhlas). Postižen byl i můj bývalý kolega, kterému někdo přes Internet smazal obsah jednoho z logických disků. Současně byl útočník tak "slušný", že se omluvil a uložil na disk návod jak se podobným útokům bránit. V textu píše, že takto provádí konzultační služby zdarma a současně vede boj proti počítačové globalizaci. Jeho podpis byl Binary Divison Hacker Agency Unlimited Consulting Dastych Group Company.

5. O čem jsme psali před rokem ?
   **Crypto-World 12/99 http://www.mujweb.cz/veda/gcucmp/casopis/crypto12_99.html**
   A.Microsoft nás zbavil další iluze! (P.Vondruška)
   B.Matematické principy informační bezpečnosti (Dr. J. Souček)
   C.Pod stromeček nové síťové karty (P.Vondruška)
   D.Konec filatelie (J.Němejc)
   E.Y2K (Problém roku 2000) (P.Vondruška)
   F.Patálie se systémem Mickeysoft fritéza CE (Cyberspace.cz) **(doporučuji přečíst!)**

# F. Závěrečné informace

## 1. Sešit

Crypto-World je oficiální informační sešit primárně určený pro členy "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní 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 (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

**http://www.mujweb.cz/veda/gcucmp** .

Pokud se zajímáte pouze o sešit Crypto-World, můžete použít lépe dostupnou adresu:

**http://cryptoworld.certifikuj.cz**

## 2. Registrace / zrušení registrace

Pokud máte zájem o zasílání tohoto sešitu, může se zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.cz (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://www.mujweb.cz/veda/gcucmp/ . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@post.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

## 3. Spojení

běžná komunikace, zasílání příspěvků

| | | |
|---|---|---|
| **p.vondruska@nbu.cz** | - | do 30.11.2000 |
| **vondruskap@uoou.cz** | - | od 15.12.2000 (?) |
| **bosakovad@uoou.cz** | - | náhradní spojení do konce roku 2000 |
| **pavel.vondruska@post.cz** | - | osobní poštovní adresa, registrace odběratelů |
| **pavel.vondruska@sms.paegas.cz** | - | zasílání SMS |