Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 8, číslo 9/2006 **15. září 2006**

9/2006

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1141 registrovaných odběratelů)

Obsah :

A. Soutěž v luštění 2006 začala!

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

Vážení čtenáři, 15. 9. 2006 začala tradiční **podzimní soutěž v luštění jednoduchých šifrových textů o ceny – *Soutěž v luštění 2006***.

Úvodní informace k soutěži

Obdobné soutěže pořádal náš e-zin v letech 2000-2005. V roce 2000 byly úlohy zaměřeny na klasické šifrové systémy. V roce 2001 soutěž pokračovala řešením "modernějších" systémů. V letech 2003 až 2005 jsme předložili úlohy od hříček, přes jednoduché šifry až po klasické šifrové systémy (jednoduchá záměna, transpozice, periodické heslo) a šifry prvé a druhé světové války (ADFGX, ÜBCHI, Enigma).

V tomto roce se setkáte s obdobnými úkoly, které budou svojí obtížností lehčí než v roce minulém. Je tomu tak za dvou důvodů. Jednak řada z loňských luštitelů žádala předložit úkoly, které jsou určeny opravdovým začátečníkům a za druhé proto, že v tomto roce jsem se rozhodl využít úkoly, které budou otištěny jako příloha v mé knize *Kryptografie, šifrování a tajná písma*, která vyjde letos na podzim.

Toto „propojení“ soutěže s moji knihou má za následek několik změn proti posledním letům:

a) konec soutěže není dán přesným datem, ale datem, kdy kniha bude dána do prodeje (pravděpodobně 1. 11. 2006)
b) ve vyluštěném textu úlohy není přímo uvedeno, které "klíčové" slovo se má zadat přes www rozhraní jako důkaz, že úkol byl správně vyřešen a je proto potřeba zjistit (např. otestovat), které ze slov otevřeného textu to je
c) některé úlohy jsou velmi lehké
d) některé úlohy jsou určeny k dešifraci (nikoliv k luštění) a nelze je tedy bez dalších nápověd vyřešit (alespoň běžnými analytickými postupy)
e) ceny pro vítěze byly doplněny o tuto moji knihu.

V letošním roce budete luštit šifrové texty od velmi jednoduchých systémů přes úkoly, které lze luštit tradičními metodami, ale k řešení vede i chytrý nápad, postřeh nebo speciální znalost až po klasické šifrové systémy.

Pokud se chcete na soutěž připravit, doporučuji prolistovat stará čísla našich e-zinů (a to nejen věnovaných soutěži), určitě v nich naleznete něco pro inspiraci a úlohy se vám budou řešit snáze.

Starší články, které se věnují některým šifrovým systémům nebo řešení soutěžních úloh najdete v našem e-zinu Crypto-World v těchto číslech:

Řešení předložených soutěžních úloh

Soutěž 2005 : Crypto-World 12/2005, http://crypto-world.info/casop7/crypto12_05.pdf
Soutěž 2004 : Crypto-World 12/2004, http://crypto-world.info/casop6/crypto12_04.pdf
Soutěž 2003 : Crypto-World 12/2003, http://crypto-world.info/casop5/crypto12_03.pdf
Soutěž 2001 : Crypto-World 1/2002, str. 2-15, http://crypto-world.info/casop4/crypto01_02.pdf
Soutěž 2000 : Crypto-World Vánoce/2000, http://crypto-world.info/casop2/cryptova_00.pdf

Články v e-zinech Crypto-World věnované řešení různých šifrových systémů

Steganografie : Crypto-World 9/2000, str.2-5, http://crypto-world.info/casop2/crypto09_00.pdf
Jednoduchá záměna : Crypto-World 10/2000, str. 2-4,
http://crypto-world.info/casop2/crypto10_00.pdf
Jednoduchá transpozice : Crypto-World 11/2000, str. 2-6,
http://crypto-world.info/casop2/crypto11_00.pdf
Substituce složitá - periodické heslo, srovnaná abeceda : Crypto-World 12/2000, str. 4-10,
http://crypto-world.info/casop2/crypto12_00.pdf
Systém Gronsfeld : Crypto-World 9/2006, str. 11-14, http://crypto-world.info/casop8/crypto09_06.pdf
Kódová kniha : Crypto-World 9/2001, str. 2-7, http://crypto-world.info/casop3/crypto09_01.pdf
Jedno-dvoumístná záměna : Crypto-World 11/2004, str. 5-6,

http://crypto-world.info/casop6/crypto11_04.pdf
Fleissnerova otočná mřížka : Crypto-World 11/2004, str. 7-8,
http://crypto-world.info/casop6/crypto11_04.pdf
Zlomkový šifrovací systém - Earle Chaseho : Crypto-World 9/2005, str. 4-5,
http://crypto-world.info/casop7/crypto09_05.pdf
Popis šifry PlayFair : Crypto-World 3/2005, str. 11-14,
http://crypto-world.info/casop7/crypto03_05.pdf
Popis šifry ÜBCHI : http://soutez2005.crypto-world.info/images/UBCHI.pdf
Popis šifry ADFGX : http://soutez2005.crypto-world.info/images/ADFGX.pdf
Dešifrace textu zašifrovaného Enigmou : Crypto-World 78/2005, příloha,
http://crypto-world.info/casop7/enigma.pdf
Absolutně bezpečný systém : Crypto-World 10/2001, str. 2-6,
http://crypto-world.info/casop3/crypto10_01.pdf

Pravidla

Soutěž začala 15. 9. 2006 rozesláním e-mailu s výzvou k soutěži všem odběratelům e-zinu Crypto-World a končí začátkem listopadu 2006 (přesný den bude uveden dodatečně a souvisí s tím, kdy bude dána do prodeje kniha *Kryptografie, šifrování a tajná písma*, ve které jsou tyto úlohy včetně jejich řešení uvedeny). Zúčastnit soutěže se může pouze odběratel e-zinu Crypto-World. Vstup na stránku soutěže bude přes domovskou stránku Crypto-Worldu - ikona **Soutěže** nebo přímým voláním soutěžní stránky (http://soutez2006.crypto-world.info).

Při registraci musí řešitel zadat *kód soutěže 2006*, který mu byl zaslán společně s výzvou k soutěži 15. 9. 2006 (Poznámka: Kód soutěže 2006 bude zaslán i všem nově registrovaným odběratelům e-zinu Crypto-World, kteří se během soutěže k jeho odběru přihlásí). Registrace k odběru e-zinu se provádí pomocí formuláře na http://crypto-world.info/dotaz/dotazy.php .

Soutěžící dále zadá své *uživatelské jméno a autentizační heslo* pro opětovné přihlášení a dále *e-mail, na který mu je zasílán e-zin Crypto-World*. Tento e-mail se dále na stránce nezobrazuje a je pro ostatní návštěvníky soutěže nedostupný. Slouží pouze k odesílání pokynů a informací soutěžícím a k ověření, že uživatel je registrovaným odběratelem e-zinu.

Mimo poslední soutěžní úlohy (číslo 31) jsou letos všechny úlohy zpřístupněny najednou a to v tomto e-zinu a na www stránce soutěže. K některým úlohám budou ještě zveřejněny dodatečné nápovědy, které umožní jejich vyluštění resp. jejich dešifraci. Nápovědy budou zveřejňovány v sekci Crypto-NEWS (http://crypto-world.info/news/index.php?sekce=c). Za vyřešení úlohy se připisují soutěžícímu body. Registrovaný řešitel zadává své odpovědi přes www rozhraní (vždy velkými písmeny)! Zadává se "klíčové" slovo z vyluštěného textu, detaily budou uvedeny v nápovědě, která bude zveřejněna v Crypto-NEWS a v e-zinu Crypto-World. Odpověď bude automaticky vyhodnocena a řešitel se ihned dozví, zda odpověděl správně nebo ne. Na rozdíl od minulých soutěží není v otevřeném textu uvedeno, které slovo má sloužit jako „klíčové“ a je potřeba do dovodit ze zveřejněných nápověd nebo otestováním všech slov otevřeného textu.

Příklad:
Řešitel vyluští zadanou úlohu a získá tento otevřený text:
KDE ZACNOU PALIT KNIHY TAM NAKONEC BUDOU LIDI UPALOVAT XX
(Kde začnou pálit knihy, tam nakonec budou lidi upalovat .)
Klíčovým slovem, kterým prokáže, že úlohu vyřešil může být libovolné slovo z otevřeného textu: např. PALIT, KNIHY nebo UPALOVAT atd.

Na stránce soutěže bude zveřejňován aktuální průběh soutěže. U každého řešitele bude v celkovém žebříčku uveden počet dosažených bodů a lze se podívat i na pořadí úloh, ve kterém je soutěžící vyřešil.

O pořadí soutěžících rozhoduje celkový počet dosažených bodů, v případě rovnosti bodů je rozhodující, kdo dosáhl tohoto počtu bodů dříve! V případě, že soutěžící ještě nezískali žádné body, jsou uvedeni podle pořadí registrace.

Pro určení celkového pořadí je rozhodující stav v době oficiálního ukončení soutěže (pravděpodobně 1. 11. 2006). První tři řešitelé získají cenu automaticky. Další ceny se vylosují mezi řešitele, kteří dosáhnou alespoň patnáct bodů.

Ceny

Pro vítěze celé soutěže je připravena již tradiční hlavní cena - bezplatná účast na mezinárodním kryptologickém workshopu **Mikulášská kryptobesídka 2006** (http://mkb.buslab.org/), který se koná 7. - 8. prosince v Praze. Pořadatel 6. ročníku TNS (Trusted Network Solutions, http://www.tns.cz/) a BUSLab (http://www.buslab.org/) hradí za vítěze registrační poplatek a zve jej srdečně na tuto akci.

První tři řešitelé získají knihu *Pavel Vondruška: Kryptografie, šifrování a tajná písma* (http://www.albatros.cz/klub/view.php?cisloclanku=2006081501), *repliku renesanční číše* (http://www.royal-glassworks.cz/detail.php?lang=E&pid=204) a dále dle svého výběru jednu z knih Google Hacking (http://www.zonerpress.cz/kniha-google-hacking.html) nebo Počítačové viry – analýza útoku a obrana (http://www.zonerpress.cz/kniha-pocitacove-viry-analyza-utoku-a-obrana.html).

Tyto ceny získají i další tři luštitelé, kteří budou vylosováni z těch soutěžících, kteří v době ukončení soutěže dosáhli alespoň patnáct bodů.

Děkuji touto cestou všem **sponzorům** soutěže:
TNS (Trusted Network Solutions), http://www.tns.cz
Albatros, http://www.albatros.cz
Zoner Press, http://www.zonerpress.cz/
Královská huť, s.r.o., http://www.qobchod.cz

Všem soutěžícím přeji úspěch v luštění a hodně zábavy !

B. Přehled úkolů „Soutěž v luštění 2006“

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

Tyto úlohy jsou od 15. 9. 2006 zveřejněny na stránce soutěže - ***Soutěž v luštění 2006*** http://soutez2006.crypto-world.info, zde také registrovaní řešitelé zadávají svá řešení (detaily viz předchozí článek, resp. pravidla soutěže).

1 Transpozice

`UMOK INEN YRUHS ONAD V ECYTAPA IPUOKEN`

Body: 1

2 Transpozice

`TSONN ICEJI NEDEV KATSE CANID EJ`

Body: 1

3 Transpozice

`VNCOE AEPJC OESOI IAMSJ PEKVL IIONK VLOI`

Body: 1

4 Jednoduchá záměna

.-.-/----/.-.././-.-/.-..//---/-//--./.-.-/--//-..-/-/.//-.--/-/.//----/-.--/--./-..-/-./.-.//./.../---/./--/----/.-/-//..--/-.//.--/-/.-///

Body: 1

5 Jednoduchá záměna

.../---/..../-./-/..//..././/-../.-.-/..//.--././.-/./..--/-../--//----/-../..-/..//-.-/.-/../..../-./--///

Body: 1

6 Jednoduchá záměna

IAky tT Qei jZ I Zj hO bozL x Dlq b YD WGQ qIl rW yCex OrZ uvA LStb Xe jO MK w Wb kY gzjD XhYM Prl sN vqlC qC W qks w uksO hyf pU Wc HeQw HzE rJt urM B PhIA IC Jo s Gtj MEZ hFUk xH C bAw f Jt ju HI

Body: 2

7 Jednoduchá záměna

6131 + 6 × 586 + 90 × 21 + 1368 – 14 : 8 + 0971 × 4241 × 4 – 3 – 864 + 26 + 9171 × 3876 : 48 – 2601 : 48 : 2384 : 26 + 9186 + 23 × 5696 × 98 – 64 – 5111 – 4372 × 335 – 6860 + 418 : 151 + 53 : 409 + 9856 × 0 × 18 + 7491 – 4820 + 4182 + 001 – 6352 + 29 + 101 =

Body: 2

8 Jednoduchá záměna

44 555 88 7 2 55 1 9999 2 1 7 33 222 444 1 7777 33 3 444 1 222 44 999 8 777 33 44 666 1 888 1 666 55 666 888 33 222 44 1 888 33 3 666 88

Body: 2

9 Jednoduchá záměna

⮡‐‹↙⇨↘ ◁ˇ⇦◢ ↔⇨↔‹ ↕◀◁‹△⇨◀ ⇦◁⇨▯⇨ ↔⇨↗↕↔⇨⬊↔‹ ↘↕▶⇦△↕ ▽◀↓⤓ ↔▯⇦△➔ ◁◢◀↗↔↕▶◀ ↘⇨◤⇨ ↔⇨↗↕↔⇨⬊↔‹↘▶ ↕↘◢↙▶↘̲

Body: 1

10 Steganografie

budoVa podpEra uvoDnik vOzka Malajsie krOkodyl uSpech oTep zarucnI skryVat naHy syseL vydAVat bahEni vyBetonovat artIkl obyDli Ales stoKA hoJit rybA pibonKa kObra oDenek krizovY stetKA jeV adResar padnoUt oKo barOkni kroUPy smIr hnoJiste kozA oKtava kurAtko

Body: 1

11 Steganografie

Okno udělal ponekud snadno. Pes ucesan doma. Buchar omlatil pistol. Udalost nemela vlastne na ctyri doby. Okraj odvaha sok andulka text pusa. Emise pijano ondulace pilot. Tchan oteze televize hnus rus ocet nikdy!

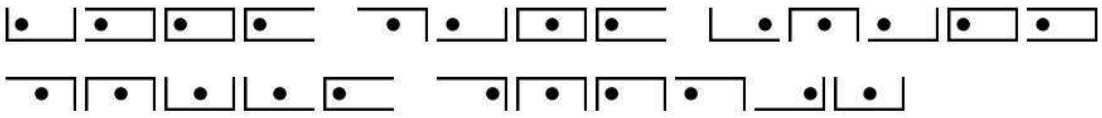
Body: 3

12 Steganografie

YQVVQ ECJEQ DNQAZ CIQJT QEXBH QZWOB QNIQE EEVQP LGYQR SXYQI
EQNGK FQAHL XQSWD YQICQ UYSRQ ZTQIS AAQTL QKTXN QUEQP JQOXQ
DXQOW QBSBI QAXQS PQEZQ LDQEX HYQKX PRQUV SNQJV QELCE QNCGW
QZBCK QNXQE BQLUK SQEMQ CGFKQ IXXSA

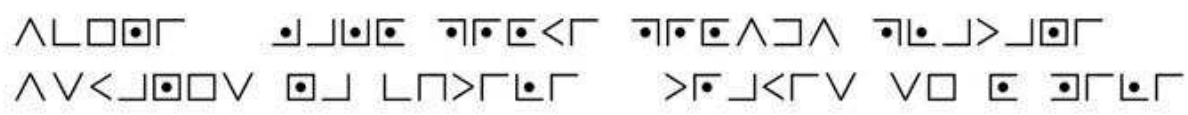
Body: 2

13 Jednoduchá záměna



Body: 2

14 Jednoduchá záměna



Body: 2

15 Transpozice

KNDEO MNUIZ KEDBY YNTEA BNYIL DDOIS TPEET LEYMM

Body: 3

16 Transpozice

KIPBO OIDLE UTZXO ICDOD XPSHE VEXRS AHPJX

Body: 3

17 Jednoduchá záměna

EVWVG QVFAM ZGPWB AMVXL ERHAV GLERH ZPWBA MVXLM VERHF AMZGA VGLMV ERH

Body: 2

18 Jednoduchá záměna

LJMEN QMBMR NWNFI WSENZ NEMXH MBTEA LJMRA ENBMQ JIWMX SNQYN JNFMR AOPNQ M

Body: 2

19 Jednoduchá záměna

WFEVT JOFMA FOBMP AJUOB ABEBT UPVTF NVTJN FABTO PVCJU

Body: 2

20 Jednoduchá záměna

OKDUL REYBN OHQHY HULPH DQLWH QNUDW NGBCP OXYLS UDYGX

Body: 2

21 Jednoduchá záměna

QVCLH ZGPCH OHTAV SUZLP DSUSB VFTNV

KPLDV UPIMV ODVZP QCQHF TCSFC SZLPO

HTGSN PBVBP OHIMV MHZPG PNCDH GY

Body: 3

22 Jednoduchá záměna

AKLSA KPVQU DUQDU VGUSS NXJQZ LOJFN
TENEL XUDUZ LAGPA SVCUA FTENO ANVQU
DLAFN DUYLV KCUAF TUYJD FDJAS LOUQZ
AOUZL APAFU GVSTU CNQNQ JAFLC UDOIS
VYVVF OEXUS PJTEJ OYVTL XDJFN DUAQZ
LTDP

Body: 3

23 Polyalfabetická substituce

BAEAK STFEK IQCNA KMDSS NQMWG VLODA
DUDNV MTATM GMZER UTGDQ LMMEC LGDWN
RQFQT WMZP

Body: 3

24 Polyalfabetická substituce

TREFT ZNYEP UFUFY IIOWA UJDTA PVPTF
PUCRB OHRNY EPWIV IP

Body: 4

25 Transpozice

NOOOT OJVNE XJADM EVHOE PEETE OLEOM
DJNAT THAHO EORID KENZS OZTOJ NIVHA
ZTEEE BEOTO NECNT TS

Body: 3

26 Transpozice

BNNEI OVKXE OOTED HEXCR JKTAA DAAER
TDKUE XEAEJ EVPIS NTNER EOVUC RDOHU
AVXUO IIKNN IRLNO IEAKD XVIBD LJDEX

Body: 3

27 Transpozice

EMMLS NYTUR ESMLI VEIIR LTITT OTEAX

JNTXA E

Body: 4

28 Playfair

ESLPY GOMLR STOBP GACOR OMYUL WGBSV

AVSAY GETQB DYEXE ZEZRG HN

Body: 5

29 BIFID

UPYML UZATM OWNLA AYXFU YZAQM IZYPN

WRYMA HUPYC LUZHH HAYXY HYEON AYDIZ

CVPYP MYPFA HQUAW PYAEM NAKU

Body: 5

30 ADFGX

XDGFX FAFDF XADFA FDGXA DXDGA AAXAD

AXADA AGDFG DDDDA DGGDD DDADG GAFAX

AXXGA DADXG FGFDG DDDDD GGDXA DGGXA

DDXDX FDFFD GAXFF DGFAA GXXDA GGXAF

AFDDX XAFAF GGDXF FFAFF DGAAF AFFXG

DAFFD ADGXA GDXAD DXD

Body: 5

31 závěrečná úloha (Chameleón)

(sledujte příslušnou www stránku)

Bude zveřejněna dodatečně !

Body: 6

Nápověda č.1

Znáte šifru CHAMELON ? Pokud zatím ne, zamyslete se, proč by se takový název pro nějakou šifru hodil a jak by mohla být realizována.

C. Systém Gronsfeld

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

Jedná se o jednoduchou polyalfaberickou šifru s periodickým heslem. Šifrový systém vznikl v 17. století, autorem byl němec Gaspar Schott. Místo Trithemiovy šifrovací tabulky *tabula recta*, která obsahuje 26 seřazených abeced, použil zjednodušenou tabulku pouze o deseti abecedách. Ke konkrétnímu výběru abecedy se používá číselný klíč, který se opakovaně (periodicky) nadepíše nad otevřený text.

Gronsfeldova převodová tabulka:

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

K samotnému šifrování se používají dvě (navzájem inverzní) verze Gronsfeldova systému.
V prvé se šifrový text určí obdobně jako ve Vigenérově systému. Nejprve se nad otevřený text opakovaně napíše domluvené číselné heslo (v našem případě 52973). Klíč určí řádek šifrové abecedy v tabulce a sloupek určí znak otevřeného textu, který se vyhledá v prvém řádku tabulky. Odpovídající šifrový znak je v určeném průsečíku. V našem příkladu to znamená, že šifrant vezme prvý znak otevřeného textu (D) a ten vyhledá v prvém řádku (d). Nyní prochází sloupkem, který je pod tímto znakem a v abecedě, která je určena prvým znakem klíče (5), získá prvý znak šifrového textu. Tím znakem je písmeno I. Vezme další otevřený znak N a ve sloupci (n) vyhledá ve druhé abecedě (2 je druhý znak klíče) šifrový znak P. Takto postupuje dále, až získá celý šifrový text.

```
Klíč:                5297 35297352
Otevřený text:       DNES NEPRIJDU
Šifrový text:        IPNZ QJRAPMIW
```

Při dešifrování příjemce postupuje „opačně“. Nejprve nad šifrový text opakovaně napíše domluvené číselné heslo (v našem případě 52973). Potom postupně vyhledává znaky

šifrového textu v abecedě (řádku), která je určena heslem zapsaným nad šifrovým textem. Hledaný znak otevřeného textu nalezne v prvém řádku tabulky nad šifrovým znakem. V našem příkladě vyhledá v páté abecedě šifrový znak I a k němu v prvém řádku vyhledá písmeno d (D). Takto opět postupuje tak dlouho, až celý text dešifruje.

```
Klíč:                5297 35297352
Šifrový text:        IPNZ QJRAPMIW
Otevřený text:       DNES NEPRIJDU
```

Druhá verze Gronsfeldova systému zaměňuje oproti předchozímu systému postup při šifrování a dešifrování.

Takto modifikovaný postup pak vypadá následovně. Klíč určí řádek šifrové abecedy, v něm se vyhledá znak otevřeného textu a odpovídající šifrový znak se nalezne ve stejném sloupku, ale v prvém řádku. V našem příkladu to znamená, že šifrant vezme pátou abecedu (určena prvou číslicí klíče) a v něm vyhledá znak D a ve stejném sloupku, ale v prvém řádku nalezne odpovídající šifrový znak y (Y). Otevřený znak N vyhledá ve druhé abecedě a nad ním nalezne odpovídající šifrový znak l (L). Takto postupuje dále, až získá celý šifrový text.

```
Klíč:                5297 35297352
Otevřený text:       DNES NEPRIJDU
Šifrový text:        YLVL KZNIBGYS
```

Při dešifrování příjemce nejprve nad šifrový text opakovaně napíše domluvené číselné heslo .

```
Klíč:                5297 35297352
Šifrový text:        YLVL KZNIBGYS
Otevřený text:       DNES NEPRIJDU
```

Hledaný znak otevřeného textu nalezne v průsečíku sloupce určeného šifrovým znakem a řádkem s abecedou, která je určena klíčem. V našem příkladě vyhledá v prvém řádku šifrový znak Y (y) a v průsečíku tohoto sloupce s pátou abecedou nalezne prvý znak otevřeného textu D. Dále vezme sloupec určený šifrovým znakem L (l) a v průsečíku s druhou abecedou (2) nalezne odpovídající otevřený znak N. Takto opět postupuje tak dlouho, až celý text dešifruje

Gronsfeldův systém byl oblíbeným systémem, který byl používán ještě koncem 20. století. Zvláště oblíbený byl mezi vězni a galerkou. Jeho obliba plynula z toho, že šifrování i dešifrování je rychlejší než při použití plné tabulky, jako v systému Vigenére. Systém (tak jako všechny obdobné polyalfabetické systémy) měl pověst bezpečného systému. Ve skutečnosti je velmi lehce řešitelný, a to pomocí principu, který publikoval roku 1883 Wilhelm Kasiski.

D. Mikulášská kryptobesídka - MKB 2006

Call for Paper

Daniel Cvrček, FIT VUT Brno, předseda programového výboru MKB
http://mkb.buslab.org

Základní informace

Mikulášská kryptobesídka, 6. ročník českého a slovenského workshopu, se koná letos 7. – 8. prosince 2006 v Praze. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Mikulášskou kryptobesídku pořádá TNS, a.s. a BUSLab.

Workshop se skládá z

(a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek 7. prosince 2006 a

(b) půldne prezentací příspěvků a diskusí v pátek 8. prosince 2006.

Součástí workshopu budou opět zvané přednášky. V současné době jsou domluveni následující hosté:

- **Alex Biryukov** (University of Luxembourg)
- **Riccard Focardi** (Universitá Ca' Foscari di Venezia)

a tři významní odborníci z České republiky

- **Petr Hanáček** (Vysoké učení technické v Brně) – Bezpečnost IS a chyby při návrhu
- **Vlastimil Klíma** (nezávislý kryptolog) – Hašovací funkce nové generace
- **Pavel Vondruška** (Telefónica O2) – Přehled a historie polyalfabetických šifer

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: http://mkb.buslab.org/ .

Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. Návrhy příspěvků (5-15 stran A4) by měly být připravené pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím vyplňte při registraci v našem konferenčním systému.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://mkb.buslab.org/ . Příspěvky mohou být napsané v češtině, slovenštině nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu PDF nebo PS přes registrační stránky MKB2006 a to nejpozději **do 2. října 2006**!

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do 23. října. Upravený příspěvek pro sborník workshopu pak musí být dodán, společně s krátkým životopisem (50-100 slov), do 20. listopadu.

Zasílání příspěvků

Letos opět používáme konferenční systém.

Pro odevzdání příspěvku je třeba se zaregistrovat na ConfTool MKB2006

Důležité termíny

Podání návrhů příspěvků:	2. října 2006
Oznámení o přijetí/odmítnutí:	23. října 2006
Příspěvky pro sborník:	20. listopadu 2006
Konání MKB 2005:	7. – 8. prosince 2006

Programový výbor

Dan Cvrček, FIT VUT v Brně – předseda

Antonín Beneš, SAP ČR

Vašek Matyáš, FI MU Brno

Daniel Olejár, FMFI UK Bratislava

Tomáš Rosa, eBanka

Zdeněk Říha, FI MU Brno

Martin Stanek, FMFI UK Bratislava

Jan Staudek, FI MU Brno

Pavel Vondruška, Telefónica O2

Mediální partneři

E. O čem jsme psali v září 1999 – 2005

Crypto-World 9/1999

Crypto-World 9/2000

+ příloha : gold_bug.rtf

Dnešní přílohou je klasická povídka The Gold Bug od Edgara Allana Poea (další informace k příloze viz závěr článku "Část I.- Začínáme steganografií" , str.10) .

Crypto-World 9/2001

Crypto-World 9/2002

Crypto-World 9/2003

Crypto-World 9/2004

Crypto-World 9/2005

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

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

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS (výběr příspěvků, komentáře a vkládání na web)	Vlastimil Klíma Jaroslav Pinkava Tomáš Rosa 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/