Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 7, číslo 12/2005 **15. prosinec 2005**

12/2005

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. Soutěž v luštění 2005 – jak šly „dějiny“…

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

(25.9.2005) - SOUTĚŽ 2005 ZAČALA! Přeji všem soutěžícím hodně úspěchu a zábavy!

(25.9.2005) - Zveřejněny úlohy prvého kola!
(26.9.2005) - Soutěžící pod pseudonymem **Stanislaw** jako první vyřešil všechny úlohy prvého kola!
(27.9.2005) - V NEWS zveřejněna nápověda k úloze č.I/9
(28.9.2005) - V NEWS zveřejněna nápověda k úloze č.I/7
(29.9.2005) - V NEWS zveřejněna nápověda k úloze č.I/10
(30.9.2005) - V NEWS zveřejněna nápověda k úloze č.I/8

(8.10.2005) - V informacích zveřejněn odkaz na Absolutně bezpečný systém ...
(9.10.2005) - Zveřejněny úlohy druhého kola!
(9.10.2005) - V NEWS zveřejněna nápověda k úloze č.II/7 a č.II/8
(11.10.2005) - Soutěžící pod pseudonymem **vn** jako první vyřešil všechny úlohy druhého kola!
(13.10.2005) - V NEWS zveřejněna nápověda k úloze č.II/9
(17.10.2005) - V NEWS zveřejněna druhá nápověda a pomůcka k úloze č.II/7 a č.II/8
(18.10.2005) - V NEWS zveřejněna nápověda k úloze č.II/3
(25.10.2005) - V NEWS zveřejněna nápověda k úlohám druhého kola (hlášení špióna)
(28.10.2005) - V NEWS zveřejněna nápověda k úloze č.II/7 a č.II/8
(29.10.2005) - V NEWS zveřejněna nápověda k úloze č.II/9 (program pro dešifraci)

(30.10.2005) - V NEWS zveřejněna nápověda k úlohám třetího kola (!)
(1.11.2005 / 20:00) - Zveřejněny úlohy třetího (posledního) kola!
(2.11.2005 / 09:01) - Souěž 2005 má svého vítěze! (**misof**)
(2.11.2005) - Druhé a třetí místo bylo obsazeno ...(pierre 17:12, alchymista 17:46)
(2.11.2005 / 23:50) - V NEWS zveřejněna nápověda k úloze č.III/3 a č.III/5
(2.11.2005 / 09:01) - Souěž 2005 má svého vítěze! (misof)
(3.11.2005) - informace - v NEWS již nebudou zveřejněny další nápovědy ...

(27.11.2005 / 20:00) - Soutěž 2005 skončila ...
Závěrečná statistika : http://soutez2005.crypto-world.info/index.php?crypto=statistika

(27.11.2005 / 20:30) - Konečné výsledky soutěže 2005:
Pořadí na prvýcch třech místech:
- 1 misof (75 bodů, ukončil 02.11 / 09:01)
- 2 pierre (75 bodů, ukončil 02.11 / 17:12)
- 3 alchymista (75 bodů, ukončil 02.11 / 17:46)
Celkové pořadí viz : http://soutez2005.crypto-world.info/index.php?crypto=zebricek

Ceny dále získali tito vylosovaní řešitelé:
(Limit pro zařazení do losování splnilo 51 soutěžících)
- 36 Palivec (19 bodů)
- 20 Winetou (33 bodů)
- 10 MD5mir (71 bodů)

B. Soutěž v luštění 2005 – řešení úloh I. kola!

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

Šifry/Nešifry

Na konci díla poznáme, čím jsme měli začít. (Blaise Pascal)

Úlohy I.kola zveřejněny 25.9.2005

ÚLOHA I/1 - TRANSPOZICE Č. 1

BODY: 1
Úlohu vyřešilo: 136 soutěžících

Text úlohy:

```
INEZAV ICIZETUOS EMANICAZ OKAJ YDZV EVRPJEN IMLEV UOHCUDONDEJ
UOHOLU IZUOLS K UMOT ETSYBA IS ILESUOKZO KAJ ES ENVARPS AVADAZ
EVOCILK OVOLS ICIJUZAKOD EZ ETSJ UHOLU ILISERYV ETJEVADAZ OTYT
YKDELSYV YDZV IMYKLEV YNEMSIP A ZEB REZEM ETSUKZ IS OT AN
OTMOT ELSEH INELOVYV
```

Popis zašifrování: text jednotlivých slov psaný pozpátku
Otevřený text se přepíše do tvaru bez diakritiky (pomocí mezinárodní abecedy) a dále se vypíše odpředu, ale jednotlivá slova se vypisují pozpátku. Rozdělovat text do pětic není v tomto případě zvykem, neboť by příjemce mohl mít s dešifrací problém.

OTEVŘENÝ TEXT
VAZENI SOUTEZICI ZACINAME JAKO VŽDY NEJPRVE VELMI JEDNODUCHOU ULOHOU SLOUZI K TOMU ABYSTE SI OZKOUSELI JAK SE SPRAVNE ZADAVA KLICOVE SLOVO DOKAZUJICI ZE JSTE ULOHU VYRESILI ZADAVEJTE TYTO VYSLEDKY VZDY VELKYMI PISMENY A BEZ MEZER ZKUSTE SI TO NA TOMTO HESLE VYVOLENI

Heslo: VYVOLENI

ÚLOHA I/2 - TRANSPOZICE Č. 2

BODY: 1
Úlohu vyřešilo: 72 soutěžících

Text úlohy:

```
DUALH JOENT ASOII YTMAO TCYAE ZPEUE AUAOU AVRSN ZDJEI BOHRA
ITOEB ZEETM OCRKA AAELT SOAUE EEADO RVOEO UTNDZ MAPLE CAMVI
RIESL HVDAP OTDST ZMWHY IARNM LEINK IRZME TPESP NETRG BTEAI
EEYZK DKJDZ ZDREV ZNKIE PMESS CZPNR ATPEA OUHR
```

Popis zašifrování: zepředu/zezadu
Otevřený text se přepíše do tvaru bez diakritiky (pomocí mezinárodní abecedy) a dále se vypisuje střídavě vždy jedno písmeno otevřeného textu zepředu a druhé zezadu do připravené řádky pro šifrový text. Na závěr se text rozdělí do skupin znaků po pěti.

OTEVŘENÝ TEXT
DRUHA ULOHA JE OPET NA TRANSPOZICI SYSTEM MA POETICKY NAZEV ZEPREDU ZEZADU JAKO DUKAZ VYRESENI ZADEJTE BIGBROTHER NAPISTE OPET BEZ MEZER TIM KONCI REKLAMA NA REALITY SHOW A MUZETE SE DAT DO OPRAVDOVEHO LUSTENI DRZIM VAM PALCE

Heslo: BIGBROTHER

ÚLOHA I/3 - TRANSPOZICE Č. 3

BODY: 2
Úlohu vyřešilo: 64 soutěžících

Text úlohy:

```
TEART IOZUU LJOEH TAEUN ZTVOA SMYMS OTZEN MATBE UXDTE SDEEN
LEAJT PPROV TEIRZ OEZTD REOLC IHNUA PDRVI EPPOO MLION VAILN
OYNAS PKAYK SSYES NTAEL MIPCO HDALM EIPSL TOATZ UAAPL IESJE
EPZRD VENPI RCEAC SETJA ENNAR SOUZD DAIML IVSET PAIDS RTUEH
KALCI ACSPT RSOYL SNTUE TMIST EONTA OZSYL VOAVP ORTOO LTNIU
ZTCIH TAERX ATKUT
```

Popis zašifrování: prolnutí textu
Transpozice se vytváří tak, že nejprve se text rozdělí na dvě poloviny a potom se začne sestavovat šifrový text. Do vznikajícího šifrového textu se nejprve na liché pozice zapíší znaky prvé poloviny otevřeného textu a potom se šifrový text doplní na sudých pozicích druhou polovinou otevřeného textu. Obě poloviny otevřeného textu se zapisují zleva doprava.

OTEVŘENÝ TEXT
TATO ULOHA UZ VAM MOZNA BUDE DELAT POTIZE TROCHU PRIPOMINA LONSKY SYSTEM PODLE PLOTU ALE JE ZDE PRECE JEN ROZDIL VEPISTE KLIC PROLNUTI TOTO SLOVO TOTIZ CHARAKTERIZUJE TENTO SYSTEM TEXT SE NEJPRVE ROZDELI NA DVE POLOVINY A PAK SE NA LICHA MISTA ZAPISE PRVNI CAST A NA SUDA MISTA DRUHA CAST SYSTEM SE NAZYVA PROLNUTI TEXTU

Heslo : PROLNUTI

ÚLOHA I/4 - STEGANOGRAFIE Č. 1

BODY: 1
Úlohu vyřešilo: 75 soutěžících

Text úlohy:

```
KYQTT QATQE IQTJZ GQOEQ UZJQL HOXOQ OOZQH EXVDQ AYBQJ NYDEQ
EGQFQ NILNQ AWDYC QTXKO QZZTQ VVAAQ KLSQL BNQAE NQMOI QAKQC
WQEWB NQTYQ EPQXZ QTDLQ VHYQO XPRQT VSNLQ ELCQV CQWQR BQKSQ
EWBTU QNSQE MQPYF KPQOT QDCQO HQBWQ EVHQJ EORJQ EOURM QOBCP
QBIAQ AICQL DJQEG QNGTJ QPMEZ JQIFU KJQSH HQMGB AQERQ NEJQY
```

```
SJUFQ KIXPR QTPRQ EEIQJ QRLWC AQARN BQNCQ EYEYM QSUYT QOHQQ
UOROQ VXQID QSYAC BQIHD DQSBQ OZREQ TNMTQ EMQVV PEQRB QEBLM
HQNEN QYCJQ MUDNM QTWQW NQESE QXVZZ FQTKM QEVAN QMEBK CQRSY
QENDQ SAKTE QIWMR LQTEQ ESQLA QEECQ NMDYT QAMUE QPPQI UPRAQ
SLTFQ IARQK AQLCF QAFBF AQMCQ ALZQC MFZNQ SADQY ZGQSJ ETQTK
QEOQK QMCVW QJYRQ ESRGQ PTEQK QROQE NNQDM OQSHI FNQTK QATQV
LTQES ULQNN ZGQTO QANMQ KFRQA JDXBQ BIQYB ZVRQB JYQYW RVQLH
SKLQL FQECQ HKUQC UBDYQ ERYQL BQUPQ SYUIB QTEAT QIUNS HQTKQ
FOQEN QLBRQ NDQYS TQNAH DQERX QQBRY QOAWQ SHQNB QAFTT LQDMQ
NRQEB DHIQB WDHQY BEANQ LQ?XW
```

Popis zašifrování: Q-kód
V šifrovém textu jsou písmena otevřené zprávy uvedena jen po určitém domluveném písmeni. Například jako zde po písmenu Q (vhodnější je samozřejmě jiné méně „nápadné“ písmeno …).

OTEVŘENÝ TEXT
TATO ULOHA JE NA TZV KLAMACE TEXT V OTEVRENE PODOBE JE OBALEN PISMENY KTERA NESOUVISI S OTEVRENYM TEXTEM RESITELE NAPISI KLAMAC SYSTEM JE PREDSTAVEN TAK ABY BYL LEHCE LUSTITELNY NEBO SNAD NEBYL ?

Heslo: KLAMAC

ÚLOHA I/5 - STEGANOGRAFIE Č. 2

BODY: 2
Úlohu vyřešilo: 78 soutěžících

Text úlohy:
Potkan arest pan potrat spojit puska hryzavy vysledek tatinek kdekoli lama pepsin udrzba udiv aspirin svoloc Dominik lzice kunkat Ital buldok uroda panenka postava taktovka dloubat koudel moucha talar zbozny bahnice utulek mzdovy Kanadan ucebni listovi akacie vylodit stepni vyjmout posluha klokani louh lehky balit presun radnice exaktni usni hlasovy rypavy mnik laskani vymrely hledat bandita pratele hanba svisly pokojska kroutit uplata opic povalec sin skadlit topit mroz kostra celni slepit rada zinek briza limitni vymotat otisk myslet osteni kreol ohar malirka hvezda banker chatrat Petr Evropan jsem ustat stitek sopka mnozina dozadu lzi krcni dziny kovani hykat mrazivy vyzadat ledovec dneska krmitko kosikar nulovy klopny kovarna kdezto srdnaty emulace kokain cpavek fazole odvaha otyly utratit uderit dostih udel kanon zdimat kujny brevno pocasi zprahly zvyseny Popelec kotelna hrom Oswald zbourat ubrat nalehat dodavka

Popis zašifrování: agenturní systém, 3-tí písmeno
Systém lze zařadit mezi typické steganografické metody. Tento steganografický systém se v různých (dokonalejších) variantách v minulosti skutečně používal. Oblíbený byl na obou stranách železné opony v době studené války. V textu je na domluveném místě písmeno otevřeného textu (zde je písmeno otevřeného textu vždy na třetím místě každého slova) ve složitějších variantách se na domluvených místech uváděla např. místo písmena otevřeného textu souřadnice kódové tabulky, kterou obě strany používaly.

OTEVŘENÝ TEXT
TENTO SYSTEM PRIPOMINA LONSKOU ULOHU DNES ALE JSOU HLEDANA PISMENA NIKOLIV NA POSLEDNIM MISTE ALE NA TRETI POZICI V KAZDEM SLOVE DUKAZ VYRESENI JE CRYPTOWORLD

Heslo : CRYPTOWORLD

ÚLOHA I/6 - JEDNODUCHÁ ZÁMĚNA Č. 1

BODY: 1
Úlohu vyřešilo: 75 soutěžících

Text úlohy:
-/-./-.-//.../..-./-./...-/---/-..//.../../.-../.-./-..//.../.-/-./..-//.-/./.-/.././/.--./.-./---/...-/..-././--//-.../--.-/.-
././.../../-//---././/-/---//..../..-./-./-.../.-/.//.-/-./.--./---/-..././..-/-.//-.-//.-/-./.../..-././..-/-../---./../.-.-/.././/-
../..-./---/..--/.//..-/-../-.-/-./..--//-.../--.-/.-././..././.-/..//---././/..--/.-./.-.-/-./..-/..-././.-/.././/

Popis zašifrování: Morseovo kódování - zrcadlení značek v kódu
Obdobných šifer – nešifer, které jsou založeny na využití převodu otevřeného textu do Morseova kódu s využitím následného jednoduchého přešifrování je opravdu celá řada. Vzhledem k tomu, že tyto systémy nepoužívají klíč, lze se na ně dívat jako na příklad možného kódování otevřeného textu. Zde použitá šifra vychází z Morseova kódu a vznikne tak, že se jednotlivé znaky tohoto kódu přešifrují tak, že se zrcadlově zamění značky (tečky a čárky) v každém kódovém vyjádření písmene. Takže např. z (G) ---. vznikne .--- (U) , z (K) -.- vznikne opět stejný kód -.- (K) atd.

OTEVŘENÝ TEXT
TAK SLABOU SIFRU SNAD NENI PROBLEM VYRESIT JE TO HLAVNE NAPOVEDA K NASLEDUJICI ULOZE DUKAZ VYRESENI JE ZRCADLENI

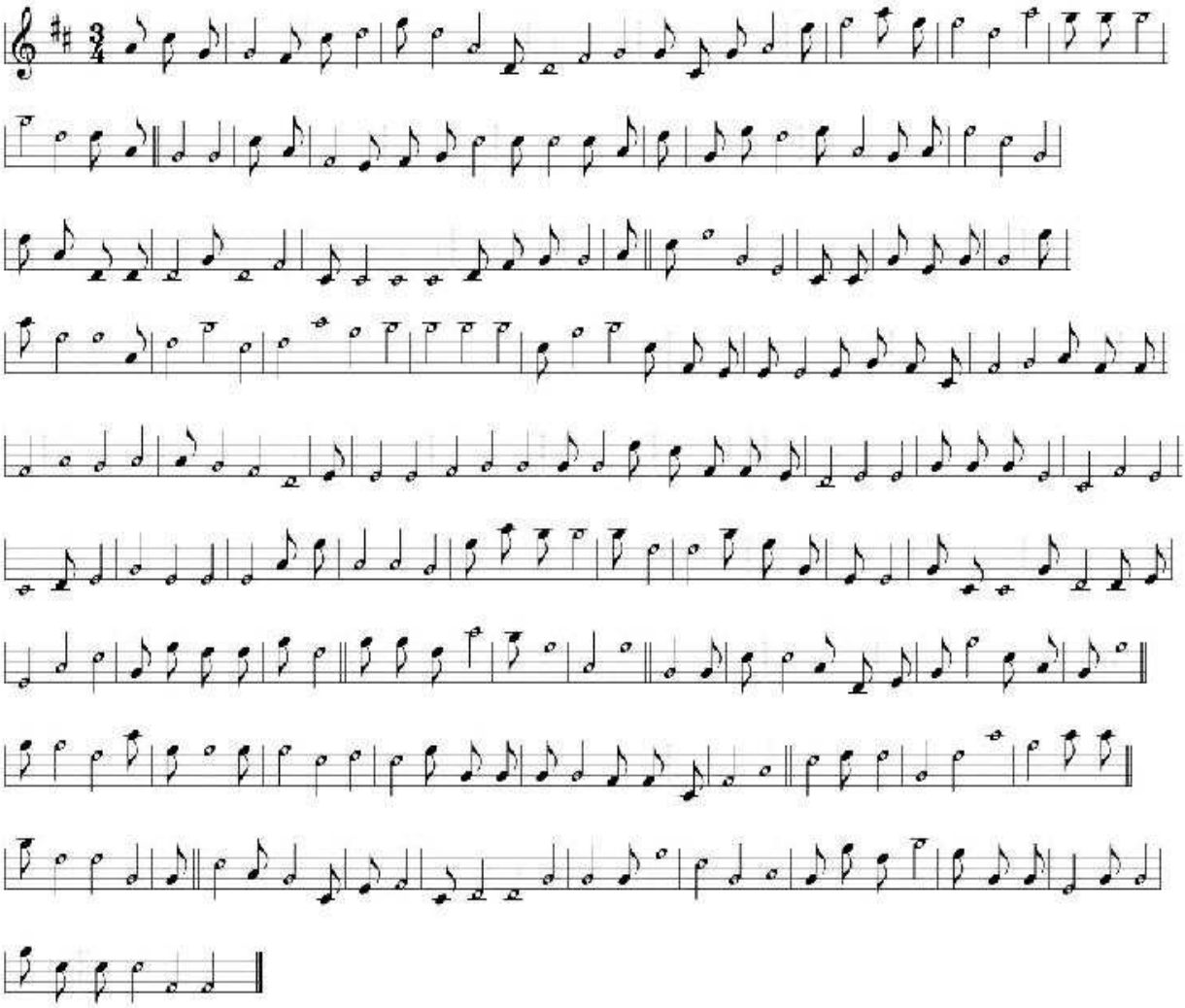
Heslo : ZRCADLENI

ÚLOHA I/7 - JEDNODUCHÁ ZÁMĚNA Č. 2 + STEGANOGRAFIE

BODY: 2
Úlohu vyřešilo: 59 soutěžících

Popis zašifrování: Morseovo kódování - kódování pomocí symbolů za účelem utajení
Systém je založen na převodu otevřeného textu do Morseova kódu a jeho následné překódování do grafické podoby. Mimo převodu kódu do této méně obvyklé formy je současně častou snahou šifrový text pomocí těchto symbolů ukrýt. Vybírány jsou tedy symboly, kde útočník při náhodném záchytu textu nemusí pojmout podezření, že zachytil šifrovou zprávu. Takovýchto systémů je možné vymyslet velkou řadu a závisí jen na nápaditosti těch, kteří se na systému domluví (plot z planěk o různé délce, zuby na pile atd.).
V naší ukázce je použit k utajení kódování notový zápis a je zvolen tento způsob kódování:
Čárka = celá nota
Tečka = všechny ostatní noty

Text úlohy:



OTEVŘENÝ TEXT
S NAPOVEDOU Z MINULE ULOHY JSTE JISTE POCHOPILI ZE TO JE MORSEOVO KODOVANI KOD JE CAJKOVSKIJ

Heslo : CAJKOVSKIJ

Nápověda: zveřejněna v NEWS 28.9.2005
(http://crypto-world.info/news/index.php?prispevek=2003)
Ode dneška si můžete stáhnout hudební part úlohy číslo sedm v lepší kvalitě.
(http://soutez2005.crypto-world.info/images/noty.jpg)
A teď ta nápověda, nepředbíhejte, vyluštěte si nejprve úlohu číslo šest ...

ÚLOHA I/8 - JEDNODUCHÁ ZÁMĚNA Č. 3 + STEGANOGRAFIE

BODY: 2
Úlohu vyřešilo: 55 soutěžících

Text úlohy:
703 : 764 x 9659 x 9302 - 269 - 1548 + 0971 x 424 : 9 x 0 + 886 + 22 : 5906 + 539 : 6358 - 27 - 185 x 133 - 4227 + 81 : 6122 x 46 : 79 + 917 x 050 : 064 x 6 + 133 : 2687 : 541 x 605 x 3 x 27 + 185 x 8575 + 2 + 866 + 9 + 2 - 8313 - 0 x 340 + 10 + 25 : 229 + 0102 : 359 - 8226 - 49 x 369 - 971 : 328 - 375 x 4483 x 49 x 10 x 02 : 5 + 6 - 76 + 3 : 353 - 907 + 694 : 65 - 9 x 6 : 15 + 84 + 606 + 9 x 911 x 7038 x 81 x 256 : 745 x 7633 - 83 - 1 + 4 - 1016 x 103 + 5097 - 668 : 481 - 126 : 2 : 49 : 0324 + 02 - 1779 - 6 x 5698 + 06 + 480 : 4342 + 60 + 9050 x 2 x 7782 x 21 + 942 - 0 x 6915 + 9 : 4 - 2646 x 6 - 484 x 8304 - 199 : 55 : 25 + 1 + 8 : 19 + 83 + 3 + 68 - 703 : 87 =

Popis zašifrování: Morseovo kódování - kódování pomocí čísel
Opět jde o zakódování otevřeného textu pomocí Morseova kódu a následné vyjádření tohoto kódu jiným, netradičním způsobem. Tentokráte se místo znaků tečka a čárka použijí číslice. Zápis šifrového textu vypadá jako nějaký složitý početní příklad a tato jednoduchá steganografická metoda může zabránit tomu, aby se nepovolaná osoba zachyceným textem zabývala.
Konkrétní použité kódování:
Tečka = libovolná sudá číslice
Čárka = libovolná lichá číslice

OTEVŘENÝ TEXT
KDYZ UZ JSTE SI ZOPAKOVALI MORSEOVKU TAK JESTE JEDNA ULOHA KODOVANI TENTOKRATE MISTO CARKY A TECKY SUDE A LICHE CISLICE ZADEJTE HESLO MATEMATIKA

Heslo : MATEMATIKA

Nápověda: zveřejněna v NEWS 30.9.2005
(http://crypto-world.info/news/index.php?prispevek=2017)
Tentokráte je nápověda velmi jednoduchá - rada, kterou naleznete v otevřeném textu úlohy číslo šest platí i pro úlohu číslo sedm!
Ještě nic ?

ÚLOHA I/9 - JEDNODUCHÁ ZÁMĚNA Č. 4

BODY: 3
Úlohu vyřešilo: 56 soutěžících

Text úlohy:

Popis zašifrování: Kódování - klingonština

Pro šifrování lze v jednodušší formě opět použít obyčejné kódování, které je založeno na tom, že se za písmena otevřeného textu dosazují znaky z klingonštiny. Ve složitější formě „šifrování“ by bylo možná vkládat celá klingonská slova nebo fráze (např. We are Klingons! = tlhIngan maH!).
„Klingonsky“ se původně mluvilo jen v kultovním filmu Star Trek, ale mluvilo se v něm skutečně. Producent nechtěl jen pár „pazvuků“ pro diváky, a tak požádal filologa Dr. Marca Okranda, aby pro společnost Paramont Studios sestavil celou řeč. Okrand sestavil abecedu, slovník, gramatiku atd. K projektu se (zadarmo) připojili další nadšeni a vznikla skutečně kompletní umělá řeč. V současné době existuje i Klingonský jazykový institut, překlady Bible, Hamleta a vychází pravidelný časopis HolQeD.
Blíže ke klingonštině: http://www.kli.org

Vzhledem k možnostem přepisu českého textu do klingonštinu je potřeba otevřený text částečně upravit (tj. využít pouze Klingonské ekvivalenty)…

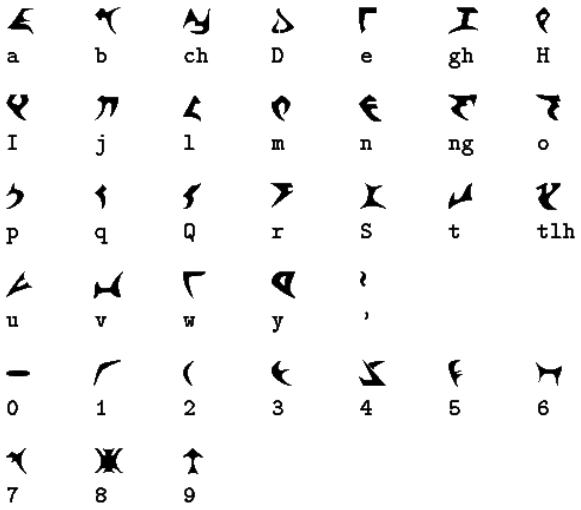
OTEVŘENÝ TEXT

tato abeceDa nenI moc vHoDna na prepIS ceSkeHo textu SnaD vam uloHa nebuDe Delat velke potIze jako Dukaz vyreSenI ukolu zaDejte kDo temIto pISmeny pISe

místo k/K=(gh) g

tato abeceDa nenI moc vHoDna na prepIS ceSgeHo textu SnaD vam uloHa nebuDe Delat velge potIze jago Dugaz vyreSenI ugolu zaDejte gDo temIto pISmeny pISe

místo z=(tlh) T



UPRAVENÝ OTEVŘENÝ TEXT

tato abeceDa nenI moc vHoDna na prepIS ceSgeHo textu SnaD vam uloHa nebuDe Delat velge potITe jago DugaT vyreSenI ugolu TaDejte gDo temIto pISmeny pISe

ŠIFROVÝ TEXT PO PŘEPISU DO KLINGONSKÝCH FONTU:

Heslo: KLINGONI

Nápověda: zveřejněna v NEWS 27.9.2005
(http://crypto-world.info/news/index.php?prispevek=1995)
I was born on August the 29th, 1971. This means that I was born four months after Igor Stravinsky died, but one month before Jimi Hendrix died. This also means I share a birthday with Michael Jackson (joy) and with Richard Gere (double joy), and my birthday falls on the

Feast Day of the Beheading of St John the Baptist (hold me back, I can hardly contain myself.)

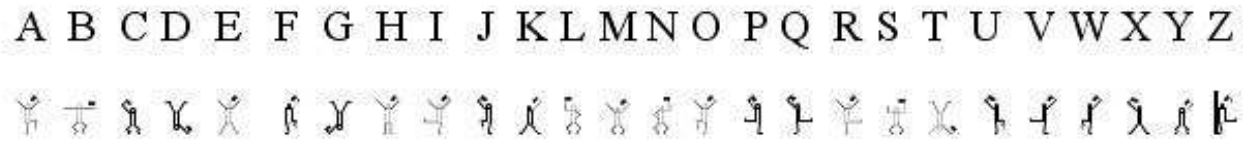
jIbogh qaSDI' DIS 1971, jar 8, jaj 29. vaj jIbogh qaSpu'DI' Igor Stravinsky Hegh loS jar, 'a qaSpa' Jimi Hendrix Hegh nungbogh wa' jar'e'. vaj qoS rap wIghaj je jIH, Michael Jackson je (Quchqu'lu'), Richard Gere je (Quchqu'lu'bej); 'ej quq qoSwIj'e', yo'a'neS quv nach teqlu' 'e' lopmeH jaj je (HIqop; jISeH'eghchoHlaHbe' jay'.)

ÚLOHA I/10 - JEDNODUCHÁ ZÁMĚNA Č. 5

BODY: 2
Úlohu vyřešilo: 56 soutěžících

Text úlohy:

Popis zašifrování: Kódování - Holmes
K laickému šifrování otevřeného textu pomocí jednoduché záměny je oblíbené použití některých převodových tabulek mezi šifrovou abecedou a znaky otevřeného textu, které byly publikovány v různých knihách. Typickým příkladem může být převodová tabulka z knihy Arthura Conana Doyleho - Návrat Sherlock Holmese, konkrétně z povídky Příběh tančících figurín (The Adventure of the Dancing Men)



OTEVŘENÝ TEXT
HESLO JE HOLMES NA ZAVER TETO SADY UKOLU JE TEXT NAPSANY POMOCI TANCICICH FIGURIN PRESNE TAK JAK JE POUZIL DOYLE V PRIBEHU THE ADVENTURE OF THE DANCING MEN KNIHA JE NATOLIK ZNAMA ZE SNAD ANI TATO ULOHA NEBUDE PRILIS TEZKA

Heslo: HOLMES

Nápověda: zveřejněna v NEWS 29.9.2005
(http://crypto-world.info/news/index.php?prispevek=2010)
Mezi mé záliby patří samozřejmě kryptografie, ale rád čtu i o různých záhadách a přímo miluji detektivky (chytré). Naposledy jsem si přečetl výbornou sbírku detektivních povídek od Arthura Conana Doyleho - The Return of Sherlock Holmes. Mimochodem nevíte náhodou, zda kniha vyšla i v češtině?

C. Soutěž v luštění 2005 – řešení úloh II. kola!

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

Klasické šifrové systémy

Je-li správná odpověď, kdopak se stará o to, je-li otázka špatná? (Norton Juster)

Úlohy II.kola zveřejněny 9.10.2005

Nápověda: zveřejněna v NEWS 28.10.2005
Soutěž 2005 - nápověda k úlohám druhého kola (hlášení špióna)...
(http://crypto-world.info/news/index.php?prispevek=2157)
Hlášení:
U zadrženého agenta byla nalezena slova uvedená v příloze k tomuto hlášení. Šetřením se zjistilo, že jde o slova z otevřených textů úloh Soutěž 2005 a to z jednotlivých úloh druhého kola. Naštěstí k velké kompromitaci nedošlo, neboť agent získal z každé úlohy pouze jedno slovo nebo krátkou frázi. Texty má navíc zapsány v jiném pořadí než je pořadí vyhlášených úloh.

Příloha :
... generál Model ...
... soukromou ...
... spáchání trestného činu ...
... křižník Potěmkin ...
... luštění ...
... schoval ...
... dokumentární film ...
... Trojdohoda ...
... operaci v Iráku ...

ÚLOHA č.II/1

Jednoduchá záměna (čeština, lehká)
Body : 2
Heslo: PARAGRAF
POZNÁMKA: Současně je heslo použito jako klíč pro sestavení tabulky pro PlayFair III/2 (PARGF)
Úlohu vyřešilo : 35 soutěžících
POPIS SYSTÉMU: Jednoduchá záměna - Crypto-World 10/2000, str. 2-4

OTEVŘENÝ TEXT (mezinárodní abeceda + doplněna soutěžní věta) :
PARAGRAF DVE STE PET OPATRENI A PRECHOVAVANI PRISTUPOVEHO ZARIZENI A HESLA K POCITACOVEMU SYSTEMU A JINYCH TAKOVYCH DAT KDO NEOPRAVNENE VYROBI UVEDE DO OBEHU DOVEZE VYVEZE PROVEZE NABIZI ZPROSTREDKUJE PRODA NEBO JINAK ZPRISTUPNI SOBE NEBO JINEMU OPATRI NEBO PRECHOVAVA ZARIZENI NEBO JEHO SOUCAST POSTUP NASTROJ NEBO JAKYKOLI JINY PROSTREDEK VCETNE POCITACOVEHO PROGRAMU VYTVORENY NEBO PRIZPUSOBENY K SPACHANI TRESTNEHO CINU NEOPRAVNENEHO PRISTUPU K POCITACOVEMU SYSTEMU A POSKOZENI A

ZNEUZITI ZAZNAMU V POCITACOVEM SYSTEMU A NA NOSICI INFORMACI PODLE PARAGRAFU DVE STE CTYRI NEBO TRESTNEHO CINU PORUSOVANI TAJEMSTVI DOPRAVOVANYCH ZPRAV PODLE PARAGRAFU STO PADESAT SEDM ODST JEDNA PISM B A C NEBO PRECHOVAVA POCITACOVE HESLO PRISTUPOVY KOD POSTUP NEBO PODOBNA DATA POMOCI NICHZ LZE ZISKAT PRISTUP K POCITACOVEHO SYSTEMU NEBO JEHO CASTI BUDE POTRESTAN ODNETIM SVOBODY AZ NA JEDEN ROK PROPADNUTIM VECI NEBO ZAKAZEM CINNOSTI ODNETIM SVOBODY AZ NA TRI LETA PROPADNUTIM VECI NEBO ZAKAZEM CINNOSTI BUDE PACHATEL POTRESTAN SPACHA LI CIN UVEDENY V ODSTAVCI JEDNA JAKO CLEN ORGANIZOVANE SKUPINY NEBO ZISKA LI TAKOVYM CINEM PRO SEBE NEBO PRO JINEHO ZNACNY PROSPECH JAKO DUKAZ UVEDTE PRVE SLOVO TOHOTO TEXTU

PŘEVODOVÁ TABULKA:
PLAIN TEXT ALPHABET: 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
CIPHER TEXT ALPHABET: E X F T R S N I Z A G K O C P U B L Y D H J M Q V W

ŠIFROVÝ TEXT :

```
U E L E N   L E S T J   R Y D R U   R D P U E   D L R C Z   E U L R F
I P J E J   E C Z U L   Z Y D H U   P J R I P   W E L Z W   R C Z E I
R Y K E G   U P F Z D   E F P J R   O H Y V Y   D R O H E   A Z C V F
I D E G P   J V F I T   E D G T P   C R P U L   E J C R C   R J V L P
X Z H J R   T R T P P   X R I H T   P J R W R   J V J R W   R U L P J
R W R C E   X Z W Z W   U L P Y D   L R T G H   A R U L P   T E C R X
P A Z C E   G W U L Z   Y D H U C   Z Y P X R   C R X P A   Z C R O H
P U E D L   Z C R X P   U L R F I   P J E J E   W E L Z W   R C Z C R
X P A R I   P Y P H F   E Y D U P   Y D H U C   E Y D L P   A C R X P
A E G V G   P K Z A Z   C V U L P   Y D L R T   R G J F R   D C R U P
F Z D E F   P J R I P   U L P N L   E O H J V   D J P L R   C V C R X
P U L Z W   U H Y P X   R C V G Y   U E F I E   C Z D L R   Y D C R I
P F Z C H   C R P U L   E J C R C   R I P U L   Z Y D H U   H G U P F
Z D E F P   J R O H Y   V Y D R O   H E U P Y   G P W R C   Z E W C R
H W Z D Z   W E W C E   O H J U P   F Z D E F   P J R O Y   V Y D R O
H E C E C   P Y Z F Z   Z C S P L   O E F Z U   P T K R U   E L E N L
E S H T J   R Y D R F   D V L Z C   R X P D L   R Y D C R   I P F Z C
H U P L H   Y P J E C   Z D E A R   O Y D J Z   T P U L E   J P J E C
V F I W U   L E J U P   T K R U E   L E N L E   S H Y D P   U E T R Y
E D Y R T   O P T Y D   A R T C E   U Z Y O X   E F C R X   P U L R F
I P J E J   E U P F Z   D E F P J   R I R Y K   P U L Z Y   D H U P J
V G P T U   P Y D H U   C R X P U   P T P X C   E T E D E   U P O P F
Z C Z F I   W K W R W   Z Y G E D   U L Z Y D   H U G U P   F Z D E F
P J R I P   Y V Y D R   O H C R X   P A R I P   F E Y D Z   X H T R U
P D L R Y   D E C P T   C R D Z O   Y J P X P   T V E W C   E A R T R
C L P G U   L P U E T   C H D Z O   J R F Z C   R X P W E   G E W R O
F Z C C P   Y D Z P T   C R D Z O   Y J P X P   T V E W C   E D L Z K
R D E U L   P U E T C   H D Z O J   R F Z C R   X P W E G   E W R O F
Z C C P Y   D Z X H T   R U E F I   E D R K U   P D L R Y   D E C Y U
E F I E K   Z F Z C H   J R T R C   V J P T Y   D E J F Z   A R T C E
A E G P F   K R C P L   N E C Z W   P J E C R   Y G H U Z   C V C R X
P W Z Y G   E K Z D E   G P J V O   F Z C R O   U L P Y R   X R C R X
P U L P A   Z C R I P   W C E F C   V U L P Y   U R F I A   E G P T H
G E W H J   R T D R U   L J R Y K   P J P D P   I P D P D   R Q D H X
(1020)
```

ÚLOHA č.II/2

Jednoduchá záměna (v OT nastavení Enigma)

Body : 3

Heslo: BRATISLAVA

POZNÁMKA: v OT nastavení Enigmy použité v úloze č. III/6

Úlohu vyřešilo : 23 soutěžících

POPIS SYSTÉMU: Jednoduchá záměna - Crypto-World 10/2000, str. 2-4

OTEVŘENÝ TEXT

BRITSTI CLENOVE DESIFROVACIHO TYMU V BLETCHEY PARKU STOJI V BREZNU ROKU JEDEN TISIC DEVET SET CTYRICET TRI TVARI V TVAR NEJHORSI NOCNI MURE NACISTICKE PONORKY NAHLE ZMENILY KOD A BITVA O ATLANTIK DOSTAVA NOVE ROZMERY VE SNAZE ZACHRANIT SITUACI POZADAJI O POMOC MATEMATICKEHO GENIA TOMA JERICHA JERICHO VSAK RESI I SVOU SOUKROMOU ZAHADU JEHO CLAIRE ZMIZELA PRAVE V OKAMZIKU KDY VLADNI ORGANY POJALY PODEZRENI ZE V PARKU JE SPION POMAHA MU JEJI NEJLEPSI PRITELKYNE

Nastavení pro Enigmu:

KOD REFLEKTOR SPACE B SPACE WHEELS SPACE III SPACE IV SPACE II SPACE RINGSTELLUNG SPACE S SPACE C SPACE A SPACE PLUG BOARD SPACE JP SPACE DY SPACE QS SPACE HL SPACE AE SPACE NW SPACE CU SPACE IK SPACE FX SPACE BR SPACE

Doplněna soutěžní věta:

TENTOKRATE SI SCHOVEJTE ZISKANY OTEVRENY TEXT BUDE SE VAM HODIT DUKAZ JE ZADANI NAZVU HLAVNIHO MESTA SLOVENSKE REPUBLIKY

PŘEVODOVÁ TABULKA:

```
PLAIN TEXT ALPHABET:  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
CIPHER TEXT ALPHABET: C L U F O X B K T H Q Z G P Y E N W D M V A J S I R
```

ŠIFROVÝ TEXT :

```
L W T M D   M T U Z O   P Y A O F   O D T X W   Y A C U T   K Y M I G
V A L Z O   M U K O I   E C W Q V   D M Y H T   A L W O R   P V W Y Q
V H O F O   P M T D T   U F O A O   M D O M U   M I W T U   O M M W T
M A C W T   A M A C W   P O H K Y   W D T P Y   U P T G V   W O P C U
T D M T U   Q O E Y P   Y W Q I P   C K Z O R   G O P T Z   I Q Y F C
L T M A C   Y C M Z C   P M T Q F   Y D M C A   C P Y A O   W Y R G O
W I A O D   P C R O R   C U K W C   P T M D T   M V C U T   E Y R C F
C H T Y E   Y G Y U G   C M O G C   M T U Q O   K Y B O P   T C M Y G
C H O W T   U K C H O   W T U K Y   A D C Q W   O D T T D   A Y V D Y
V Q W Y G   Y V R C K   C F V H O   K Y U Z C   T W O R G   T R O Z C
E W C A O   A Y Q C G   R T Q V Q   F I A Z C   F P T Y W   B C P I E
Y H C Z I   E Y F O R   W O P T R   O A E C W   Q V H O D   E T Y P E
Y G C K C   G V H O H   T P O H Z   O E D T E   W T M O Z   Q I P O R
C U K I U   O P I M O   S M V D E   T Y P C Q   Y F W O X   Z O Q M Y
W D E C U   O L D E C   U O J K O   O Z D D E   C U O T T   T D E C U
O T A D E   C U O T T   D E C U O   W T P B D   M O Z Z V   P B D E C
U O D D E   C U O U D   E C U O C   D E C U O   E Z V B L   Y C W F D
E C U O H   E D E C U   O F I D E   C U O N D   D E C U O   K Z D E C
U O C O D   E C U O P   J D E C U   O U V D E   C U O T Q   D E C U O
X S D E C   U O L W D   E C U O M   O P M Y Q   W C M O D   T D U K Y
A O H M O   R T D Q C   P I Y M O   A W O P I   M O S M L   V F O D O
A C G K Y   F T M F V   Q C R H O   R C F C P   T P C R A   V K Z C A
P T K Y G   O D M C D   Z Y A O P   D Q O W O   E V L Z T   Q I X X X(690)
```

ÚLOHA č.II/3

Jednoduchá záměna (slovenština ☺)

Body : 3

Heslo: SLOVENSKO

POZNÁMKA: heslo později použito jako druhý klíč v úloze III/3 (dvojitá transpozice)

POPIS SYSTÉMU: Jednoduchá záměna - Crypto-World 10/2000, str. 2-4

Úlohu vyřešilo : 25 soutěžících

Použit otevřený text z www stránky :
http://referaty.atlas.sk/vseobecne_humanitne/dejepis/5964/

OTEVŘENÝ TEXT (mezinárodní abeceda + doplněna soutěžní věta) :

NYNI BUDE KOD SLOVENSKO V PRVEJ SVETOVEJ VOJNE SE PO PRVYKRAT ROZSIRILO BOJISKO Z EUROPSKEHO PRIESTORU NA CELY SVET PROTI SEBE STALI MOCENSKE ZOSKUPENIA TROJSPOLOK A TROJDOHODA PRVA SVETOVA VOJNA DEMONSTROVALA HROZY MODERNEJ TECHNIKY ZAPOJENEJ DO STRATEGIE NICENIA NASADENIE NOVYCH ZBRANI TANKOV LIETADIEL AKO AJ CHEMICKYCH BOJOVYCH LATOK SI VYZIADALO ZIVOTY MILIONOV LUDI VOJNA SA DOTKLA VO ZVYSENEJ MIERE I CIVILNEHO OBYVATELSTVA NEDOSTATKOM POTRAVIN PRACOU ZIEN V ZBROJARSKOM PRIEMYSLE BOMBARDOVANIM MIEST PRINIESLA ZAVAZNE POLITICKE ZMENY POCAS VOJNY SA ROZPADLA POLITICKO SPOLOCENSKA STRUKTURA STAREJ EUROPY MONARCHIA NEMECKEJ RISE RAKUSKO UHORSKO A RUSKO SA ROZPADLI TAKISTO AKO OSMANSKA RISA OKTOBROVA REVOLUCIA V RUSKU PO PRVYKRAT V HISTORII PRESADILA SOCIALISTICKE PREDSTAVY DO PRAXE NEMECKO A NASTUPNICKE STATY HABSBURSKEJ MONARCHIE ZACALI PRECHADZAT K DEMOKRATICKYM REPUBLIKANSKYM STATNYM FORMAM VSTUP USA DO VOJNY PRESUNUL TAZISKO SVETOVEJ POLITIKY EUROPA STRATILA SVOJE HEGEMONNE POSTAVENIE USA SA STALI ROZHODUJUCOU HOSPODARSKOU A FINANCNOU VELMOCOU DOSLEDKAMI PRVEJ SVETOVEJ VOJNY BOLI OKREM INEHO AJ NEDOSTATOK POTRAVIN A ROZSIAHLA CHRIPKOVA EPIDEMIA EMANCIPACIA ZIEN ZACALI PRACOVAT TAM KDE PREDTYM MALI MONOPOL IBA MUZI A COSKORO ZISKALI AJ VOLEBNE PRAVO VOJNU FINANCOVALI EUROPSKE VLADY Z ROZSIAHLYCH POZICIEK TLACILI STALE VIAC PAPIEROVYCH PENAZI CO VIEDLO K INFLACI

PŘEVODOVÁ TABULKA:

```
Plain Text Alphabet:   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
Cipher Text Alphabet:  B S L O M N U X F G H Z K A C D E I J P Q R T V W Y
```

ŠIFROVÝ TEXT :

```
A W A F S   Q O M H C   O J Z C R   M A J H C   R D I R M   G J R M P
C R M G R   C G A M J   M D C D I   R W H I B   P I C Y J   F I F Z C
S C G F J   H C Y M Q   I C D J H   M X C D I   F M J P C   I Q A B L
M Z W J R   M P D I C   P F J M S   M J P B Z   F K C L M   A J H M Y
C J H Q D   M A F B P   I C G J D   C Z C H B   P I C G O   C X C O B
```

```
D I R B J   R M P C R   B R C G A   B O M K C   A J P I C   R B Z B X
I C Y W K   C O M I A   M G P M L   X A F H W   Y B D C G   M A M G O
C J P I B   P M U F M   A F L M A   F B A B J   B O M A F   M A C R W
L X Y S I   B A F P B   A H C R Z   F M P B O   F M Z B H   C B G L X
M K F L H   W L X S C   G C R W L   X Z B P C   H J F R W   Y F B O B
Z C Y F R   C P W K F   Z F C A C   R Z Q O F   R C G A B   J B O C P
H Z B R C   Y R W J M   A M G K F   M I M F L   F R F Z A   M X C C S
W R B P M   Z J P R B   A M O C J   P B P H C   K D C P I   B R F A D
I B L C Q   Y F M A R   Y S I C G   B I J H C   K D I F M   K W J Z M
S C K S B   I O C R B   A F K K F   M J P D I   F A F M J   Z B Y B R
B Y A M D   C Z F P F   L H M Y K   M A W D C   L B J R C   G A W J B
I C Y D B   O Z B D C   Z F P F L   H C J D C   Z C L M A   J H B J P
I Q H P Q   I B J P B   I M G M Q   I C D W K   C A B I L   X F B A M
K M L H M   G I F J M   I B H Q J   H C Q X C   I J H C B   I Q J H C
J B I C Y   D B O Z F   P B H F J   P C B H C   C J K B A   J H B I F
J B C H P   C S I C R   B I M R C   Z Q L F B   R I Q J H   Q D C D I
R W H I B   P R X F J   P C I F F   D I M J B   O F Z B J   C L F B Z
F J P F L   H M D I M   O J P B R   W O C D I   B V M A M   K M L H C
B A B J P   Q D A F L   H M J P B   P W X B S   J S Q I J   H M G K C
A B I L X   F M Y B L   B Z F D I   M L X B O   Y B P H O   M K C H I
B P F L H   W K I M D   Q S Z F H   B A J H W   K J P B P   A W K N C
I K B K R   J P Q D Q   J B O C R   C G A W D   I M J Q A   Q Z P B Y
F J H C J   R M P C R   M G D C Z   F P F H W   M Q I C D   B J P I B
P F Z B J   R C G M X   M U M K C   A A M D C   J P B R M   A F M Q J
B J B J P   B Z F I C   Y X C O Q   G Q L C Q   X C J D C   O B I J H
C Q B N F   A B A L A   C Q R M Z   K C L C Q   O C J Z M   O H B K F
D I R M G   J R M P C   R M G R C   G A W S C   Z F C H I   M K F A M
X C B G A   M O C J P   B P C H D   C P I B R   F A B I C   Y J F B X
Z B L X I   F D H C R   B M D F O   M K F B M   K B A L F   D B L F B
Y F M A Y   B L B Z F   D I B L C   R B P P B   K H O M D   I M O P W
K K B Z F   K C A C D   C Z F S B   K Q Y F B   L C J H C   I C Y F J
H B Z F B   G R C Z M   S A M D I   B R C R C   G A Q N F   A B A L C
R B Z F M   Q I C D J   H M R Z B   O W Y I C   Y J F B X   Z W L X D
C Y F L F   M H P Z B   L F Z F J   P B Z M R   F B L D B   D F M I C
R W L X D   M A B Y F   L C R F M   O Z C H F   A N Z B L   F X X X X
(1200)
```

Nápověda: zveřejněna v NEWS 18.10.2005
Soutěž 2005 - nápověda k úloze č.II/3
(http://crypto-world.info/news/index.php?prispevek=2119)

Už ste rozmýšľali prečo Vám robí práve táto jednoduchá substitúcia taký problém?
Želám veľa šťastia pri jej riešení.
Pavol

ÚLOHA č.II/4

Transpozice sloupcová úplná (lehká)

Body : 3

Heslo: CERNI BARONI

POZNÁMKA: heslo později použito jako první a druhý klíč v úloze III/4 (ÜBCHI)

POPIS SYSTÉMU: Jednoduchá transpozice - Crypto-World 11/2000, str. 2-6

Úlohu vyřešilo : 27 soutěžících

OTEVŘENÝ TEXT (ukázka z knihy ČERNÍ BARONI + doplněna soutěžní věta) :

GENERAL TAK JINAK SOUDRUHU PORUCIKU KDY A KYM BYL DAN POVEL K ZAHAJENI VELKE RIJNOVE REVOLUCE PORUCIK TRONIK SOUDRUHU GENERALE POVEL NA ZAHAJENI VELKE RIJNOVE REVOLUCE VYDAL PRECE SOUDRUH LENIN KTERY TAK ZMATL POLITICKY ZATUCHLY CARSKY REZIM PROTOZE TEN POVEL MISTO V RIJNU VYDAL AZ ZACATKEM LISTOPADU

GENERAL SOUDRUHU KAPITANE KTERA LOD ZAHAJILA PALBU NA ZIMNI PALAC KAPITAN ORECH TAK TO VIM OPET NAPROSTO PRESNE SUDRUHU GENERALE BYL TO KRIZNIK POTEMKIN A OD TE DOBY A NA JEHO POCEST SUDRUZI V SOVETSKEM SVAZU STAVI TAKZVANE POTEMKINOVY VESNICE

GENERAL ZDRCENE TO STACI SOUDRUZI NECEKAL JSEM ZAZRAKY ALE ALE IMPERIALISTE BY SE ZARADOVALI KDYBY VIDELI JAK MOHOU VYPADAT DUSTOJNICI LIDOVE DEMOKRATICKE ARMADY SPOLEHNETE SE ZE PODAM O VSEM CO JSME TADY ZAZILI PODROBNOU ZPRAVU ZADEJTE NAZEV KNIHY ZE KTERE JE TATO UKAZKA

Parametry sloupcové transpozice:

Tabulka : 18 x 39

Transpoziční klíč získán vyčíslením fráze : CERNIBARONITERAZKY.

Transpoziční klíč : 4-5-13-10-7-3-1-14-12-11-8-16-6-15-2-18-9-17

ŠIFROVÝ TEXT :

```
L O A L P   U Z V C Y   Z M S C E   N P A M E   L A C K A   I O K L Z
E D M O V   L A K X K   D Z V R A   V C H L C   T U S R O   I E R G I
Y U S K A   U A A L H   C K S M N   Z A X A P   D E E R A   O E R Y I
I A N A A   K I N Y N   O S V N T   E A E D T   E P O I Z   E X G D Y
J V K O E   D I I K O   A A K H P   A O R T J   S I V R Z   K T Y Y D
M P D P N   K E R M E   O S V R A   N T Y V L   D A A A K   P A E E O
T Y C I Y   E B P O A   O Y R I A   N U L N K   E N L R A   L Z J L U
A A O A H   Z O D Z E   E S M R V   M N I T J   O N E X R   U L V C D
N N R E K   Z M Z E T   L C V S B   I P T Z S   E C E S I   A D S M Z
U Z A J I   V I C E J   V U Z C T   R E S E U   A T R R E   S V O E C
S P D A O   A N C D T   E X O A H   R N E L V   E O R N Y   O H Z N H
S N P N I   A N Z R R   I K U L A   Z T U V O   X E H Y I   U U L J P
T C E L Z   G I I A O   E E K O E   K E N E L   Y V D E Y   A A V Y K
K C O R U   G A E O K   U O V K L   T B T E D   K T T S P   G A J M A
J T R H M   O J R X A   U P E R U   H R S A T   R O T A K   L I P U O
D S M E E   T L I R I   S K E E P   E E X N U   B N L O E   I L K I R
E A U P J   L T R L M   H V A V E   N A B Y A   V D D Z A   H Z T R N
K O H A E   E T A P T   A R E A P   O S T O E   E N C S A   E A L U O
L S I D T   X A K K O   T R I U U   T Y E N I   D L Z R P   U N B R U
M R O Z I   A O I C E   S B A T X   I K E J I   N E O D M   H O I M O
R N N N U   I D U A T   N I E E O   K J T E O   R E J X U   K A E I P
K Y N L S   P D P U A   I T T E O   A V V O D   U A S D V   I R E A Z
K U X S Y   A E O L E   E L P A E   V T U D M   C O E K A   Z T I L D
Z L I O I   E E E O E   T X (702)
```

ÚLOHA č.II/5

Fleissnerova mřížka (použita stejná jako v roce 2004 ! ☺)
Body : 2
Heslo: ALCHYMISTA
POPIS SYSTÉMU: Fleissnerova otočná mřížka - Crypto-World 11/2004, str. 7-8
Úlohu vyřešilo : 30 soutěžících

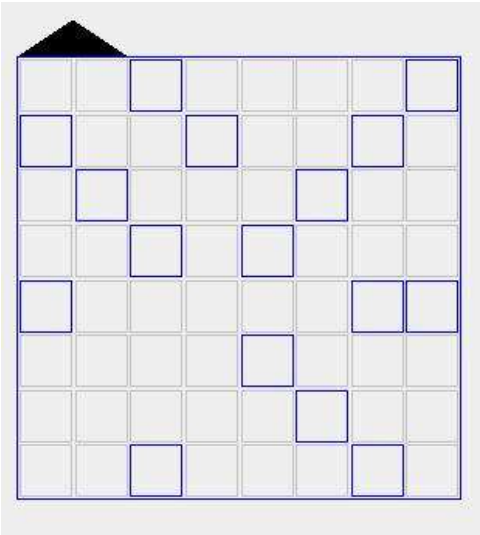
OTEVŘENÝ TEXT

Tak kdopak byl tak chytrý a schoval si loňskou tabulku ? Zapište ALCHYMISTA

Přepis do mezinárodní abecedy (bez mezer)
TAKKDOPAKBYLTAKCHYTRYASCHOVALSILONSKOUTABULKUZAPISTEALCHY
MISTAXX

Použitá mřížka (1 značí otvor), stejná jako v roce 2004:
(popis luštění viz řešení z roku 2004, Crypto-World 12/2004)

```
0 0 1 0 0 0 0 1
1 0 0 1 0 0 1 0
0 1 0 0 0 1 0 0
0 0 1 0 1 0 0 0
1 0 0 0 0 0 1 1
0 0 0 0 1 0 0 0
0 0 0 0 0 1 0 0
0 0 1 0 0 0 1 0
```



ŠIFROVÝ TEXT :

```
IOTHS NYAKT SKETD AROLK YPCAO UAHKY STBMC AHBYL IOUST VLTAK
ALUAS ZAXKI XPCL (64)
```

Vhodný software:
http://www.turning-grille.com/download.htm

ÚLOHA č.II/6

Periodický systém (systém Vigenére, heslo krátké = 5)

Body : 3

Heslo: CITADELA

POPIS SYSTÉMU: Substituce složitá - periodické heslo, srovnaná abeceda - Crypto-World 12/2000, str. 4-10

POZNÁMKA: heslo později použito jako klíč k úloze II/9 (Zlomkový systém Earle Chase)

Úlohu vyřešilo : 33 soutěžících

OTEVŘENÝ TEXT (mezinárodní abeceda + doplněna soutěžní věta) :

Použit otevřený text z www stránky : http://nacismus.mysteria.cz/tanky.php

OHLEDNE OPERACE CITADELA JAK SE PLAN NA UTOK V KURSKEM VYBEZKU NAZYVAL ROZHODNE NEPANOVALA V NEMECKEM VRCHNIM VELENI SHODA K HLAVNIM ZASTANCUM OPERACE PATRIL ZPOCATKU ZEJMENA GENERAL ZEITZLER NACELNIK STABU OKH A GENERAL MODEL JEHOZ DEVATA ARMADA MELA HRALA V OPERARCI CITADELA HLAVNI ROLI GENERAL MANSTEIN VELITEL SKUPINY ARMAD JIH NAVRHOVAL DVE VARIANTY OPERACI NA LETO TISIC DEVET SET CTYRICET TRI BYL SI DOBRE VEDOM ZTRAT KTERE WEHRMACHT UTRPEL A SPATROVAL PROTO JEDINOU NADEJI V UDERECH LOKALNIHO CHARAKTERU KTERE POSTUPNE PODKOPOU BOJOVOU SILU RUSU
MODELEM PRO NEJ BYLA SAMOZREJME USPESNA PROTIOFENZIVA U CHARKOVA PRVNI MANSTEINEM NAVRHOVANA VARIANTA ZAHRNOVALA ROZSAHLY USTUP NA JIHU KTERY BY NASLEDOVAL DRTIVY PROTIUDER VEDENY PROTI ODKRYTEMU SEVERNIMU KRIDLU POSTUPUJICI RUDE ARMADY HITLER VSAK BYL ROZHODNE PROTI JAKYMKOLIV ZTRATAM UZEMI A TUDIZ TENTO PLAN NEPODPORIL DRUHA MANSTEINOVA VARIANTA ZAHRNOVALA UTOK NA KURSKY VYBEZEK KTERY MEL BYT VEDEN CO NEJDRIVE NEJLEPE DO KONCE KVETNA PAK BY ZBYVAL JESTE CAS ODRAZIT PREDPOKLADANOU SOVETSKOU OFENZIVU NA JIHU
JAKO RESENI VLOZTE NAZEV OPERACE A JSTE SOUCASNE PRIPRAVENI NA DESIFRACI POSLEDNI ULOHY DRUHEHO KOLA

Parametry pro Vigenérovu šifru:

Heslový klíč pro výběr abecedy: CITADELA

Postup při šifrování a dešifrování viz periodické heslo, srovnaná abeceda – Crypto-World 12/2000, str. 4-10

ŠIFROVÝ TEXT :

```
Q P E E G   R P O R M   K A F I N   I V I W E   O E U A M   A X P O E
Y N C C M   O N Z V U   T A D E P   Z J B G H   D U Q E K   Y X I E R
R D S O F   V X N H T   L N Q D T   L D Z Y E   O M V K H   Q G R E P
G I P Z P   L G V B S   K S O A M   P E A Y R   T M B I L   T D R N U
O W I E U   E N E R I   M R L P K   P Q K T T   N Y K E L   U X N D K
P N G Z T   L C I T T   B T X R Q   E N E N V   B K V X L   B W W D H
D K P N G   Z T L P S   O E N R X   H R D O E   X I M A D   V X A F I
F E O E S   R C T T V   R T P R C   Z V I F M   E A F M E   A K P L V
```

```
P Q K O O   M R E P M   K A O Q L   N U B X I   Q Z P L K   B X L V O
F P K V R   A U Q L D   L Q A N D   Z C H Q D   T L G Z P   V C Z B A
Q X J O R   M K A F M   Y A N M M   O W M D I   E L X V H   X D E V K
M Y U M N   E V B K I   E C W S K   L H B U I   G E F W F   Z W V L T
M B X R H   A P H T U   T C K X F   T T X X L   D W A A V   Z H V D P
A R Q B H   J H H T N   Q C G A G   I U I X C   W E U I N   H N W D A
O R T H Q   K A A U E   V T G Z N   K W I C E   R W L T X   T Y E R W
W K R T Z   U D W C O   Y S F S K   T N R X W   F M Q L X   L H Q A R
Q V X J E   C W A U I   F O C V P   J O M N S   S I D N C   X K O W M
Z F G V S   I Y E F C   J I K K R   Z L P T D   G I P E Y   S V M B N
H Q Y A X   Z A O Y E   Y A X I K   I D R E A   B I A R Q   S G A N I
K O C W L   H N G N S   W Y A N C   R B H X O   E E T G U   Y Q E D L
G L H V D   P O R V Q   O Y S V Z   T K C W E   U Z P D G   V R P U S
E I Q L D   R B X P M   W A X V H   V Y I O C   D R L H W   U R W L T
X T F J K   K B R X H   P A T U T   D B L T T   N M K V V   E V B A T
K O C L Z   D P M I R   R X T J C   S R M N S   W I X H M   R D X L M
W H X M L   E E U F Q   S T H R E   O R T T N   Q I A O F   X H R L P
O R W P T   M D R D T   G Q G O Y   E G A T Q   T N W E K   A J Z G O
Y E W A W   B H K Q E   V U T A D   Y Y C M E   B M D K W   I C Y O M
E B B X G   E F M G C   R R P J F   Z B V H R   P J N M I   E G S V O
P K X K Y   I E N C X   T K E C K   B A D T L   M I D T G   K T S R H
C A B Q M   P U I O P   Q S E A G   E Y O W A   H V H X D   K Q C H F
H R K I X   C G A M M   S U L I D   O U I D E   P Q O L R   D E E P I
S E Y S A   E T I V E   D N D T G   A H U F E   D N G X K   I S V L V
G V B N D   H P S K N   K A F M A   O U T X D   Q M F L Q   P R D U Y
S E J W D   O O E XX (1000)
```

ÚLOHA č.II/7 a II/8

Absolutně bezpečný systém (přičtené heslo u úlohy II/7 a II/8 je stejné)

Body : 4

Heslo: GEORGEWBUSH

POPIS SYSTÉMU: Absolutně bezpečný systém - Crypto-World 10/2001, str. 2-6

Úlohu vyřešilo : 14 soutěžících

ZAČÁTEK OTEVŘENÉHO TEXTU 1

PRAHA PATEK SEDMEHO RIJNA
VLOZENO ZACATEK ZADEJTE JMENO PREZIDENTA GEORGE W BUSH KONEC

ZAĆÁTEK OTEVŘENÉHO TEXTU 2

OPAKOVANI TELEGRAMU PRAHA SOBOTA OSMEHO RIJNA
VLOZENO ZACATEK ZADEJTE JMENO PREZIDENTA GEORGE W BUSH KONEC

NÁSLEDUJE SPOLEČNÝ STEJNÝ TEXT PRO OT1 A OT2:

Použit otevřený text z www stránky : http://www.novinky.cz/zahranicni/66849-bush-pry-rekl-sasovi--svrhnout-tyranii-v-iraku-mi-prikazal-buh.html

AMERICKY PREZIDENT GEORGE W BUSH PRED PALESTINSKYMI POLITIKY V CERVNU DVA TISICE TRI REKL ZE OPERACI V IRAKU MU PRIKAZAL BUH UVADI TO DOKUMENTARNI FILM BBC KTERY BUDE ODVYSILAN V PONDELI A CITUJE NEKDEJSIHO PALESTINSKEHO MINISTRA ZAHRANICI NABILA SASE TEN

PRO BBC REPRODUKUJE BUSHOVA SLOVA PODLE NICHZ SE MU ZJEVIL VSEMOHOUCI A REKL GEORGE JDI A UKONCI TYRANII V IRAKU

A NA ZÁVĚR OPĚT DOPLNĚNA SOUTĚŽNÍ VĚTA (STEJNÁ PRO OT1 A OT2):
ZADEJTE JMENO PREZIDENTA GEORGE W BUSH

OTEVŘENÝ TEXT 2/7 (mezinárodní abeceda + doplněna soutěžní věta) :
PRAHA PATEK SEDMEHO RIJNA
VLOZENO ZACATEK ZADEJTE JMENO PREZIDENTA GEORGE W BUSH KONEC AMERICKY PREZIDENT GEORGE W BUSH PRED PALESTINSKYMI POLITIKY V CERVNU DVA TISICE TRI REKL ZE OPERACI V IRAKU MU PRIKAZAL BUH UVADI TO DOKUMENTARNI FILM BBC KTERY BUDE ODVYSILAN V PONDELI A CITUJE NEKDEJSIHO PALESTINSKEHO MINISTRA ZAHRANICI NABILA SASE TEN PRO BBC REPRODUKUJE BUSHOVA SLOVA PODLE NICHZ SE MU ZJEVIL VSEMOHOUCI A REKL GEORGE JDI A UKONCI TYRANII V IRAKU
ZADEJTE JMENO PREZIDENTA GEORGE W BUSH

OTEVŘENÝ TEXT 2/8 (mezinárodní abeceda + doplněna soutěžní věta) :
OPAKOVANI TELEGRAMU PRAHA SOBOTA OSMEHO RIJNA
VLOZENO ZACATEK ZADEJTE JMENO PREZIDENTA GEORGE W BUSH KONEC AMERICKY PREZIDENT GEORGE W BUSH PRED PALESTINSKYMI POLITIKY V CERVNU DVA TISICE TRI REKL ZE OPERACI V IRAKU MU PRIKAZAL BUH UVADI TO DOKUMENTARNI FILM BBC KTERY BUDE ODVYSILAN V PONDELI A CITUJE NEKDEJSIHO PALESTINSKEHO MINISTRA ZAHRANICI NABILA SASE TEN PRO BBC REPRODUKUJE BUSHOVA SLOVA PODLE NICHZ SE MU ZJEVIL VSEMOHOUCI A REKL GEORGE JDI A UKONCI TYRANII V IRAKU
ZADEJTE JMENO PREZIDENTA GEORGE W BUSH

Převedeno do ASCII tvaru a rozděleno do pětic: II/7 (832)

```
80826 57265 80658 46975 83696 87769 72798 27374 78658 67679 90697 87990
65676 58469 75906 56869 74846 97477 69787 98082 69907 36869 78846 57169
79827 16987 66858 37275 79786 96765 77698 27367 75898 08269 90736 86978
84716 97982 71698 76685 83728 08269 68806 57669 83847 37883 75897 77380
79767 38473 75898 66769 82867 88568 86658 47383 73676 98482 73826 97576
90697 98069 82656 77386 73826 57585 77858 08273 75659 06576 66857 28586
65687 38479 68797 58577 69788 46582 78737 07376 77666 66775 84698 28966
85686 97968 86898 37376 65788 68079 78686 97673 65677 38485 74697 86975
68697 48373 72798 06576 69838 47378 83756 97279 77737 87383 84826 59065
72826 57873 67737 86566 73766 58365 83698 46978 80827 96666 67826 98082
79688 57585 74696 68583 72798 66583 76798 66580 79687 66978 73677 29083
69778 59074 69867 37686 83697 77972 79856 77365 82697 57671 69798 27169
74687 36585 75797 86773 84898 26578 73738 67382 65758 59065 68697 48469
74776 97879 80826 99073 68697 88465 71697 98271 69876 68583 72
```

Převedeno do ASCII tvaru a rozděleno do pětic: II/7 (872)

```
79806 57579 86657 87384 69766 97182 65778 58082 65726 58379 66798 46579
83776 97279 82737 47865 86767 99069 78799 06567 65846 97590 65686 97484
69747 76978 79808 26990 73686 97884 65716 97982 71698 76685 83727 57978
69676 57769 82736 77589 80826 99073 68697 88471 69798 27169 87668 58372
80826 96880 65766 98384 73788 37589 77738 07976 73847 37589 86676 98286
78856 88665 84738 37367 69848 27382 69757 69069 79806 98265 67738 67382
65758 57785 80827 37565 90657 66685 72858 66568 73847 96879 75857 76978
84658 27873 70737 67766 66677 58469 82896 68568 69796 88689 83737 66578
```

```
86807 97868 69767 36567 73848 57469 78697 56869 74837 37279 80657 66983
84737 88375 69727 97773 78738 38482 65906 57282 65787 36773 78656 67376
65836 58369 84697 88082 79666 66782 69808 27968 85758 57469 66858 37279
86658 37679 86658 07968 76697 87367 72908 36977 85907 46986 73768 68369
77797 27985 67736 58269 75767 16979 82716 97468 73658 57579 78677 38489
82657 87373 86738 26575 85906 56869 74846 97477 69787 98082 69907 36869
78846 57169 79827 16987 66858 37213 10
```

Heslo (náhodně vygenerované – délka 872):

```
72172 84180 12550 02458 49047 14411 75698 21962 37116 24924 11325 32251
31886 29322 22452 05234 15251 23615 74218 14646 12518 35711 12311 54229
23925 21978 16551 85388 29924 71542 33180 86859 00158 24519 73159 60220
16725 32501 74453 31981 61441 06123 36671 43196 23019 51965 12020 91660
01005 78425 20923 13633 12910 52237 56203 20019 38570 12131 59602 20167
25325 01741 47701 34894 25417 91041 69105 23153 12711 71121 21190 00294
31581 86134 21075 12184 21962 41351 10199 11065 23578 74236 73216 25025
50091 14245 09225 18521 21589 49498 07231 24327 12822 34710 12219 38215
23386 17417 87360 13616 81564 44216 32235 86170 11650 52081 86016 92080
04821 67321 33057 24412 70325 34216 46917 35911 81801 61119 14156 15685
21765 10424 20651 92166 16716 81061 35869 10310 15115 32062 09211 21121
13377 37113 55180 17015 65927 81602 51110 13725 42451 77138 66119 15713
11151 45725 50010 20073 95247 63173 57341 45091 14431 71211 66725 31592
31921 05126 13117 18612 23410 35184 50198 18822 86115 71905 81165 11411
92112 37130 66792 49235 91120 81982 16
```

Šifrový text II/7 (832) (vznikl sečtením z heslem od pozice 1)

```
52998 31345 92108 48323 22633 91170 47386 48236 05764 81593 01912 19141
96452 77781 97358 51093 89097 10082 33995 02628 71415 61570 80157 01388
92742 37855 72309 12553 98600 67207 00778 03116 75946 22778 63885 46198
90431 29483 45041 07566 44169 04382 94477 90755 06856 88748 87817 68940
70762 06898 95711 79392 94777 30795 32851 67392 01146 00513 22428 17633
15912 99700 29357 01170 98233 48526 36953 21326 87360 77697 87947 28770
96168 14503 89762 60651 80640 87833 88826 18331 90134 30901 57804 43981
35677 01103 85013 45897 86267 07467 75817 11990 77499 62195 86806 14180
81973 55780 59058 19182 40392 81584 15981 73349 88387 39364 60832 41045
76647 14194 90784 00978 43081 82571 29505 71889 61628 57775 71972 03667
90343 67909 94247 50649 88404 47544 01557 76890 84792 98930 72888 40104
72045 86187 14947 44691 48514 58574 20966 80080 24048 24709 25807 32872
85738 71200 25707 06746 79035 89641 20079 02373 79189 20276 24312 79951
05697 92995 93933 07685 81007 13549 21785 06093 45981 39488 53
```

Šifrový text II/7 (872) (vznikl sečtením z heslem od pozice 1)

```
41978 31659 98107 89732 08703 01593 30366 79944 92832 72293 77013 78720
14552 16591 04189 42099 91918 12674 42907 10103 77354 22201 77997 41603
82662 97846 85359 01278 92500 68326 98896 73731 71746 90194 56876 17198
75391 89260 56189 08460 41267 95196 94268 21567 82707 78024 99688 49932
81821 64205 85689 01917 85698 89716 23931 27985 01317 49610 35278 18343
93171 89306 21439 61151 84255 18323 28852 82112 81517 69386 88828 67576
96239 33819 01892 49649 11519 07936 82947 77523 96315 60005 48063 91993
34649 31018 79952 75287 87156 97857 89027 82885 71518 12399 95946 94783
09183 04275 46027 49173 54302 91675 00822 32939 85487 89250 66663 58963
88558 45696 92774 11185 48053 62698 01813 82193 46588 97882 82702 72951
86591 68783 04248 70148 85372 47743 94667 37278 90863 89421 65069 58390
99925 64782 31738 14973 31514 68969 23018 49692 27358 13014 39877 73072
88848 62600 17746 78232 60904 79042 39057 32459 87089 28780 34392 69971
13578 82499 99845 34187 08316 81943 24934 05299 45892 69987 40062 47270
60958 84299 35519 55112 57978 18195 26
```

Zveřejněné nápovědy:

Soutěž 2005 – nápověda k úloze na absolutně bezpečný systém (č.II/7 a č.II/8)
Nápověda č.1: zveřejněna v NEWS 9.10.2005
(http://crypto-world.info/news/index.php?prispevek=2057)

K vytvoření šifrového textu č.7 a č.8 byl použit tento postup:

- převod otevřeného textu do mezinárodní abecedy
- dekadické vyjádření ASCII znaků
- součet z heslem (bez přenosu)...

Příklad:

Otevřený text :	P	R	A	H	A
Převod na ASCII:	80	82	65	72	65
Heslo:	17	33	63	90	15
Součet:	97	15	28	62	70

Více o systému a o tom, kdy a za jakých okolností jej lze rozluštit viz článek Absolutně bezpečný systém v Crypto-Worldu 10/2001, str. 2-6 (http://crypto-world.info/casop3/crypto10_01.pdf)

Soutěž 2005 - druhá nápověda k úloze č.II/7 a č.II/8
Nápověda č.2: zveřejněna v NEWS 17.10.2005
(http://crypto-world.info/news/index.php?prispevek=2113)

Úloha, která nejvíce řešitelům odolává je zatím jednoznačně úloha druhého kola č.II/7 a č.II/8.
První nápovědu jsem zveřejnil již 9.10.2005.

Dnes zpřístupňuji pomůcku k luštění
http://soutez2005.crypto-world.info/images/vernam.exe) , kterou poskytl řešitel soutěžící pod pseudonymem room132.

Věnuje ji nezištně všem těm, kterým se ještě dvoj úlohu č. II/7 a č.II/8 nepodařilo pokořit....
Místo návodu se můžete podívat na tento obrázek
(http://soutez2005.crypto-world.info/images/vernam.jpg) - předpokládám, že z něj je použití jeho softwaru zcela jasné.

Přeji všem luštitelům příjemnou práci a úspěch ...

Soutěž 2005 – nápověda k úloze na absolutně bezpečný systém (č. II/7 a č . II/8)
Nápověda č.3: zveřejněna v NEWS 28.10.2005
(http://crypto-world.info/news/index.php?prispevek=2178)

Z hlášení špióna :

Zjistil jsem, ze při šifrování úloh II/7 a II/8 se dopustil autor chyby a k otevřeným textům těchto úloh omylem přičetl stejné heslo. Heslo je sice náhodné a stejně pravděpodobné, ale díky této chybě se z absolutně bezpečného systému stal snadno řešitelný problém....

Jeden z kryptologů mi vyzradil postup, jak lze v tomto případě šifru rozluštit ...

ŠT .. šifrový text
OT .. otevřený text
H .. heslo

II/7 ŠT1= OT1+H
II/8 ŠT2= OT2+H

- spočítat ŠT1-ŠT2=OT1+H - OT2 - H = OT1-OT2
- z toho plyne: OT1=(ŠT1-ŠT2)+OT2

Nyní stačí "uhodnout OT2" a pokud se to podaří, pak se snadno dopočte odpovídající OT1. To samozřejmě platí i pro jednotlivé libovolně dlouhé úseky - tj. není třeba hádat celý text OT2 najednou (což by se asi nepodařilo :-), ale je možné zkoušet slova jejichž existenci v tomto textu předpokládáte a ty dosazovat na různé pozice textu. Dopočítáte, jaký text by tomu v OT1 odpovídal a pak je-li to čitelný text jste našli odpovídající úseky otevřeného textu OT1/OT2 (jinými slovy - předpokládané slovo se v OT2 vyskytuje a našli jste i jeho správné umístění v textu OT2 a jako "bonus" odpovídající část otevřeného textu v OT1 ...)

Získané úseky otevřeného textu rozšiřujete následně hádáním dalších slov na vlevo a na vpravo v OT1 resp. OT2 a získáváte tím další a další úseky hledaného textu v OT2 resp. OT1

Dále dodal, že společně s tím, co už mám k dispozici: program na výpočet OT1 při zadání OT2 a některá slova z otevřeného textu, by to neměl být žádný problém...

Jiný popis řešení (postup převzat z e-mailu jednoho z řešitelů):

Stanislaw Schmulinsky

Řešení úloh na téma „absolutně bezpečná šifra“ jsem začal prostudováním příslušného ezinu, kde je uvedeno, že systém je luštitelný pouze při porušení některého z pravidel bezpečného šifrování, tj:

1) prozrazení hesla
2) použití periodického hesla (pro úspěšné luštění stačí heslo 2x zopakovat)
3) použití stejného hesla na více zpráv

K mé lítosti autor úlohy heslo neposkytl ☺, takže jsem pokračoval zkoumáním hesla úlohy č.7. Poté, co jsem bez úspěchu překročil hodnotu 200 znaků, jsem začal mít podezření že to asi nebude správný způsob. Mé podezření posílil soutěžící vn, který zabodoval úlohou 7 a 8 naráz. Po zkusmém odečtení šifrových textů obou úloh se nevyskytly žádné anomálie,

(*nenalezení anomálie v tomto případě znamená, že se u ciferného rozdílu šifrových textů nevyskytují na první pozici číslice 4,5, nebo 6 – tím je s vysokou pravděpodobností dáno, že heslo či úsek hesla se pro danou část zprávy na dané pozici shodují. Je to vlastně určitá*

slabina šifrového systému, daná použitím „krátké“ sady znaků a současně sekvenčním ASCII kódováním.), přijal jsem tedy jako pracovní hypotézu že:

- heslo je skutečně pro obě zprávy stejné
- v obou případech je použito od první pozice textu

V další fázi luštění jsem se rozhodl zaútočit několika vytipovanými slovy (*tento, tato, toto, uloha, uvedte, zadejte, zapiste, dukaz, heslo, slovo, reseni, kod*. Jak je vidět na obrázku níže, tato taktika se vyplatila a po vyluštění slova „PREZIDENTA“ už šlo vše celkem snadno. I v této fázi luštění pomohl výskyt anomálií eliminovat některé varianty a navíc podstatná část obou zpráv byla shodná. Sice jsem vyzkoušel prezidenty všech geometrických, geopaleontologických a dalších společností, než mi došlo jak se věci mají (to jsem ještě netušil, že obě zprávy jsou o tomtéž), ale to byla už jen malá oklika.

Při luštění úloh, které řeším poprvé, často používám tabulkový procesor – umí potřebné funkce, výsledek je hned vidět, lze použít barvy a občas mě tento způsob přivede na nějaký nápad.

Na úpravu textu před zpracováním (odstranění mezer, uspořádání do n-tic atd.) používám jednoduchý program. Na následujícím obrázku je ukázka části tabulky po vložení slova „ZADEJTE“ na správnou pozici.

Š8	Š7	Š8-Š7	H8	H7		K8	O8	K7	O7		K8	O8	K7	O7
99	93	06	97	97		86	V	80	P		86	V	80	P
84	93	91	99	99		73	I	82	R		73	I	82	R
53	30	23	39	39		82	R	69	E		82	R	69	E
41	76	75	24	24		65	A	90	Z		65	A	90	Z
87	85	02	98	98		75	K	73	I		75	K	73	I
08	81	27	87	87		85	U	68	D		85	U	68	D
31	00	31	69	69		90	Z	69	E		90	Z	69	E
68	71	97	07	07		65	A	78	N		65	A	78	N
19	35	84	59	59		68	D	84	T		68	D	84	T
43	49	04	26	26		69	E	65	A		69	E	65	A
24	21	03	50	50		74	J	71	G		74	J	71	G
93	78	25	91	91		84	T	69	E		84	T	69	E
40	50	90	29	29		69	E	79	O		69	E	79	O

LEGENDA:

Š8, Š7	šifrový text úlohy
Š8-Š7	rozdíl šifrových textů
H8, H7	heslo
K8, K7	kód ASCII
O7, O8	otevřený text
černě	zadané hodnoty
červeně	vypočtené hodnoty
modře	kontrolní výpočty

vzorce:

O8 = (Š8 - Š7) + O7
O7 = O8 - (Š8 - Š7)

ÚLOHA č.II/9

Zlomkový systém Earle Chase

Body : 3

Heslo: DESIFRACE

POZNÁMKA: jako klíč pro sestavení tabulky použito heslo z úkolu II/6 (CITADELA)

POPIS SYSTÉMU: Zlomkový šifrovací systém - Earle Chaseho - Crypto-World 9/2005, str. 4-5

Úlohu vyřešilo : 19 soutěžících

OTEVŘENÝ TEXT 2/9 (mezinárodní abeceda + doplněna soutěžní věta) :

PRAVE JSTE SI OZKOUSELI CIM SE LISI LUSTENI OD DESIFRACE NAPISTE DESIFRACE

PARAMETRY ŠIFROVÉHO SYTSÉMU:
PŘEVODOVÁ TABULKA + NÁSOBENÍ 9
(PRO SESTAVENÍ TABULKY POUŽIT KLÍČ CITADELA)

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

Převod OTEVŘENÉHO TEXTU podle tabulky:
27 29 14 32 16 22 20 13 16 20 12 26 36 23 26 31 20 16 17 12 11 12 24 20 16
17 12 20 12 17 31 20 13 16 25 12 26 15 15 16 20 12 19 29 14 11 16 25 14 27
12 20 13 16 15 16 20 12 19 29 14 11 16

zlomek
2213122112123223211111221112113211212111211211121212111112112111
794262036026636106721240672027103652655602994165472036560299416

po vynásobení jmenovatele číslem 9 dostaneme tento zlomek:
1221312211212322321111122111211321121211121121112121211112112111
7148358324239724960491166048243932873900426947489248329042694744

Zlomky převedeme opět na řádkový zápis
17 21 24 18 33 15 28 23 12 14 22 13 29 37 22 24 39 26 10 14 19 11 11 26 26
10 14 18 22 14 13 39 23 12 18 27 13 29 10 10 14 22 16 19 24 17 14 18 29 12
24 18 23 12 19 10 14 22 16 19 24 17 14 14

Převedeme zpět na text podle stejné převodové tabulky (CITADELA)
L H M B W D Q K I A J T R = J M ! O G A F C C O O
G A B J A T ! K I B P T R G G A J E F M L A B R I
M B K I F G A J E F M L A A

Šifrový text (po zalomení do pětic):

LHMBW DQKIA JTR=J M!OGA FCCOO GABJA T!KIB PTRGG AJEFM LABRI
MBKIF GAJEF MLAA (64)

Nápověda č.1: zveřejněna v NEWS 13.10.2005
(http://crypto-world.info/news/index.php?prispevek=2092)
Před jejím řešením si ještě jednou pozorně přečtěte vyluštěné otevřené texty úloh druhého kola ....

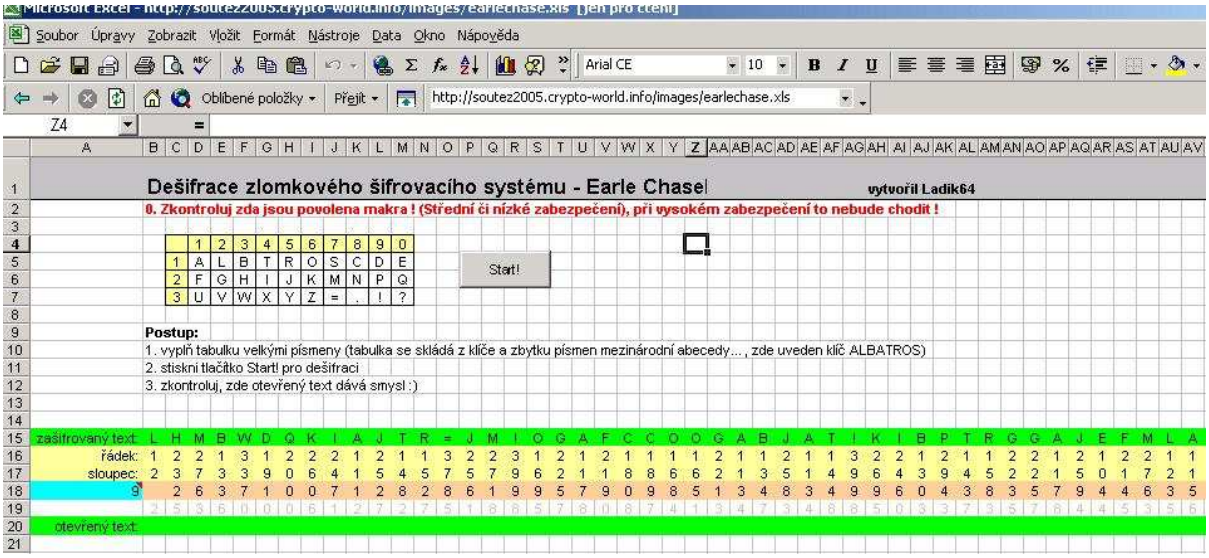
Nápověda č.2: zveřejněna v NEWS 29.10.2005
(http://crypto-world.info/news/index.php?prispevek=2179)

Vážení soutěžící,
váš soupeř a konkurent Ladik64 se rozhodl, že se s Vámi podělí o svůj program (http://soutez2005.crypto-world.info/images/earlechase.xls), který použil při dešifraci úlohy II/9.

K správné funkci musíte povolit v Excelu spouštění makra (nastavit střední či nízké zabezpečení).

Pro úplnost připomínám odkaz na zveřejněnou předchozí nápovědu k této úloze ze 13.10...

Přeji hezkou zábavu a ten správný nápad, jak najít klíč k této úloze (tj. jak správně sestavit převodovou tabulku..)



D. Soutěž v luštění 2005 – řešení úloh III. kola

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

Šifrové systémy prvé a druhé světové války

Nepozdvihne národ proti národu meče a nebudou se více učiti boji. (Bible)

Úlohy III.kola zveřejněny 1.11.2005

Přehled zveřejněných nápověd k úlohám třetího kola

Soutěž 2005 - nápověda k úlohám třetího kola (!)
Nápověda č.1: zveřejněna v NEWS 30.10.2005
http://crypto-world.info/news/index.php?prispevek=2180

Vážení soutěžící,
v nejbližší době budou zveřejněny úlohy třetího a posledního kola naší soutěže.
Nezapomeňte, že celkový vítěz bude ten, kdo nejen vyřeší všechny úlohy, ale vyřeší je jako první!
Informace z tohoto příspěvku je tedy možné využít k přípravě k řešení úloh třetího kola.

a. Přehled systémů, které budete ve třetím kole řešit:
III/1 Sloupcová transpozice (úplná tabulka)
III/2 Playfair
III/3 Dvojitá transpozice (úplná tabulka)
III/4 ÜBCHI
III/5 ADFGX
III/6 ENIGMA
III/7 ENIGMA

b. Popis systémů
Jednoduchá transpozice, Crypto-World 11/2000, str. 2-6
http://crypto-world.info/casop2/crypto11_00.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

c. Nápověda
Klasické luštění úloh tohoto kola by bylo velmi pracné. Z tohoto důvodu se ve vašem případě bude jednat spíše o řešení / dešifraci. Obdobně jako v úloze II/9. Předložené systémy mají jeden nebo dva klíče. Je možné, že jeden z klíčů (díky řešení předchozích úloh) již znáte a

teprve druhý budete muset získat (po tomto zjednodušení) vyluštěním.... V případě, že úloha má jeden klíč, je možné, že jej již také znáte ...
Dále vám prozradím, že úlohy již nepoužívají informace z řešení úkolů prvého kola. Na úkoly prvého kola můžete zcela zapomenout.

Soutěž 2005 - nápověda k úlohám č.III/3 a č. III/5
Nápověda č.2: zveřejněna v NEWS 2.11.2005
http://crypto-world.info/news/index.php?prispevek=2204

Zjištění špióna

a) zjistil jsem, že již třem lidem se podařilo vyřešit všechny šifrové depeše !

b) III/3 Dvojitá transpozice (úplná tabulka)
1. klíč : klíč (délky 12 - neznám)
2. klíč : délky jiné než 1. klíč (již znám)

c) III/5 ADFGX
První klíč tzv. substituční určuje obsah převodové tabulky, která má 25 znaků a neobsahuje W.
Permutační klíč: (jeho délka je větší než druhý klíč u III/3 a menší než první klíč u III/3 a již ho také znám)

ÚLOHA č. III/1
SLOUPCOVÁ TRANSPOZICE (ÚPLNÁ TABULKA)

Body: 3
Heslo: VZDYPRIPRAVEN
POPIS SYSTÉMU: Jednoduchá transpozice - Crypto-World 11/2000, str. 2-6
POZNÁMKA: Úloha byla zařazena především proto, aby luštitelé měli po jejím vyřešení jasné vodítko, jak postupovat při luštění úkolů tohoto kola.
Úlohu vyřešilo : 15 soutěžících

OTEVŘENÝ TEXT (mezinárodní abeceda + doplněna soutěžní věta) :
VAZENI SOUTEZICI ZACINA POSLEDNI KOLO NASI SOUTEZE VZHLEDEM K TOMU ZE BUDETE PRI RESENI TECHTO SIFROVYCH SYSTEMU POTREBOVAT DOBRE ZVLADNOUT TRANSPOZICI ZARADIL JSEM JAKO ROZCVICKU TUTO ULOHU PREDPOKLADAM ZE JSTE JI BEZ PROBLEMU VYRESILI A TAK JESTE DULEZITA RADA NA ZAVER V NASLEDUJICICH ULOHACH SYSTEMY CASTO VYUZIVAJI DVA KLICE JEDEN KLIC BUDE POUZITO NEJAKE HESLO Z ULOH DRUHEHO KOLA A TO ULOH JEDNA AZ PET A DRUHY KLIC ZNAT NEBUDETE ULOHY BUDOU TEDY JAKOUSI KOMBINACI DESIFRACE A LUSTENI DIKY TOMU JE VSAK MATE SANCI V ROZUMNEM CASE VYRESIT JAKO DUKAZ ZE SE VAM PODARILO TRANSPOZICI VYRESIT A VITE JAK NA NASLEDUJICI UKOLY NAPISTE VZDYPRIPRAVEN XXXXX

Parametry sloupcové transpozice:
Tabulka : 10 x 55
Transpoziční klíč získán vyčíslením fráze : PVONDRUSKA .
Transpoziční klíč : 6-10-5-4-2-7-9-8-3-1

Poznámka: problém řešitelům dělalo určení tabulky. K tomu je nutné provést výpočet poměru samohlásek a souhlásek v řádku (viz Crypto-World 11/2000).

ŠIFROVÝ TEXT

```
TNKUD BEOSR RTCSC UOSOS SAEJA CVCCT SUTAH NODOS SOAOE
KELIA NISPX NILAV OETOM AASAK UPABU TLNSH SVVEP ALKHT
CEDOA CDVNE SAONR JDYDN UIIOE ERTHT BUIJZ OPJRE ETVUH
YIIII ERANU TLEKE UTMRS ASIZT ACIIX ECSNE TTIRE VLNRA
KUDIM AUAAC YODDE JUOOE IDUKN AIEAN EKPAY EELZE ZIOOZ
KENFT OVAAJ CHAJE IDDNI STIED EZHLP LUBAI RNJSM RUMRV
TLOVV VEAOT EUSSY EETIE VLKTB ITRRI CAAEB OLHOA YEHYM
ITMTZ VOVOC VAUTR IZESZ MPEVU TDPDO TRMEV AEALU TYANO
KOOJA ZTOUC EISCM IZDSE AUNYX OCNSL ZIHCO OOZLO TDEPR
JIADO MZLLZ HDADR AUTID LYKVA JEROI NIPRX SADIH URCYP
DNOIR UEZZY KZZEL EUKKU EHLED NEUSI AKAIC TZAPS KJAPX
AZPLE MDEIS BZRZM IOLEL LEAVC HSJJU NOEUZ KBYJB FEUEU
YDATI ISKEA (550)
```

ÚLOHA č. III/2

PlayFair

BODY: 5

POPIS SYSTÉMU: Popis šifry PlayFair - Crypto-World 3/2005, str. 11-14

POZNÁMKA: klíč k sestavení tabulky bylo použito heslo II/1 PARGRAF

Heslo: BERCHTOLD

Úlohu vyřešilo : 13 soutěžících

OTEVŘENÝ TEXT (mezinárodní abeceda + doplněna soutěžní věta) :

Použit otevřený text z www stránky:

http://www.ceskenoviny.cz/prilohy/10_let_cn/zprava_stoleti/index.php?soubor=280714.html

VIDEN DVACATEHO OSMEHO CERVENCE PONEVADZ KRALOVSKA SRBSKA VLADA NEODPOVEDELA USPOKOJIVE NA NOTU KTEROU JI ODEVZDAL RAKOUSKO UHERSKY VYSLANEC V BELEHRADE DNE DVACATEHO TRETIHO CERVENCE ROKU TISIC DEVET SET CTRNACT JEST C A K VLADA NUCENA ABY PECOVALA SAMA O OCHRANU SVYCH PRAV A ZAJMU A ABY ZA TIMTO UCELEM APELOVALA NA MOC ZBRANI RAKOUSKOUHERSKO MA TUDIZ ZATO ZE JEST OD TOHOTO OKAMZIKU VE VALECNEM VZTAHU SE SRBSKEM RAKOUSKO UHERSKY MINISTR ZAHRANICNICH ZALEZITOSTI HR BERCHTOLD

Doplněna soutěžní věta:

DUKAZ JMENO MINISTRA

PARAMETRY SYSTÉMU:

Klíč: PARAGRAF – po vyčíslení PARGF (z úlohy II/1)

NULY: YQ

Tabulka (I/J):

P	**A**	**R**	**G**	**F**
B	**C**	**D**	**E**	**H**
I/J	**K**	**L**	**M**	**N**
O	**Q**	**S**	**T**	**U**
V	**W**	**X**	**Y**	**Z**

Otevřený text, po úpravě J --> I:

VIDEN DVACATEHO OSMEHO CERVENCE PONEVADZ KRALOVSKA SRBSKA VLADA NEODPOVEDELA USPOKOIIVE NA NOTU KTEROU II ODEVZDAL RAKOUSKO UHERSKY VYSLANEC V BELEHRADE DNE DVACATEHO TRETIHO CERVENCE ROKU TISIC DEVET SET CTRNACT IEST C A K VLADA NUCENA ABY PECOVALA SAMA O OCHRANU SVYCH PRAV A ZAIMU A ABY ZA TIMTO UCELEM APELOVALA NA MOC ZBRANI RAKOUSKOUHERSKO MA TUDIZ ZATO ZE IEST OD TOHOTO OKAMZIKU VE VALECNEM VZTAHU SE SRBSKEM RAKOUSKO UHERSKY MINISTR ZAHRANICNICH ZALEZITOSTI HR BERCHTOLD DUKAZ IMENO MINISTRA

ŠIFROVÝ TEXT

```
POEHL HWPKC YMBUQ TTMBU DHPXH MDHBV MHWPH XLARK VPQLR
QPDQL PWKRC RMHSB BVYBE HKROT BVIQM VOPHM FKQUQ NYMPS
ONOVE HWVCR SDCQQ OQLQO BHDXM WWZXS FKHDP IDMHB GREHH
LHEWP KCYMB USGMY NBQBD GYBKH DGQIO ULOKB EHYBU TMYEQ
FLCKO MDTQE CQXIR CFKQH HMGWP CVGHD VPRKR QGKPQ QBDFF
KOTWZ DBAGP WFWPK NTCWP CZVGQ KNUQQ HDMMT RADMV PRKFK
GKQBV HGRIK GRIQO TIQZN DGQLT IGQSH NVWFU QYHMB TUSBU
QBUUQ QIGKV NNQYB WPMDH KMTWV QGNZT DXDDO MCLGC QQOQL
QOBHD XMWNK IKTUF XFCGR IKHKK BNFRK HYMOQ TOMDF CHADE
USIEX HSQCV NTMIU NKIKT UGR (428)
```

ÚLOHA č. III/3

Dvojitá transpozice (úplná tabulka)

Body: 4

Heslo: OBRANANARODA

POPIS SYSTÉMU: lze použít článek - Jednoduchá transpozice - Crypto-World 11/2000, str. 2-6

POZNÁMKA: pro jednoduchost jsou obě tabulky úplné

1.klíč : OBRANANARODA (nebyl znám)

2.klíč : SLOVENSKO (bylo použito heslo z úlohy II/3)

Úlohu vyřešilo : 8 soutěžících

OTEVŘENÝ TEXT (mezinárodní abeceda + doplněna soutěžní věta) :

DO PRAZSKE URADOVNY GESTAPA SE SNAZILI PRONIKNOUT NASI LIDE ZE ZPRAVODAJSKE SITE BYVALYCH PRISLUSNIKU PATRACI SEKCE DRUHEHO ODDELENI MAJORA FRANTISKA FARKA A STABNIHO KAPITANA ANTONINA LONGY RADA OSLOVENYCH CESKYCH POLICISTU ZARAZENYCH KE GESTAPU SPOLUPRACI S NASIMI CESKYMI ZPRAVODAJCI ODMITA NASLI SE VSAK NEKTERI KTERI DODAVAJI AKTUALNI ZPRAVY PRAVIDELNE I JEDNOU TYDNE JEDEN Z TAKOVYCH UREDNIKU DODAVA CESKYM ODBOJARUM Z OBRANY NARODA INFORMACE O VYSLESICH A CHOVANI OSOB ZATCENYCH GESTAPEM COZ VYZNAMNE PRISPIVA K PROVADENI OBRANNYCH OPATRENI NASIM ODBOJEM KE KRYTI SVYCH AKTIVIT A MNOHDY ZACHRANE SVYCH LIDI STEJNY UCEL MA CINNOST REGIONALNICH A MISTNICH VELITELSTVI OBRANY NARODA KTERE ZISKAVAJI ZDROJE MEZI POLICEJNIMI UREDNIKY V JEDNOTLIVYCH OBLASTECH DARI SE NAM TO ZEJMENA V BRNE NEBO OSTRAVE XX

ZADEJTE NAZEV ODBOJOVE ORGANIZACE KTERA ZA DRUHE SVETOVE VALKY PROVADELA A ORGANIZOVALA TUTO ZPRAVODAJSKOU CINNOSTX

PARAMETRY DVOJITÉ TRANSPOZICE

První transpozice:

Tabulka : 12 x 66

Transpoziční klíč získán vyčíslením fráze : OBRANANARODA .

Transpoziční klíč : 9-5-11-1-7-2-8-3-12-10-6-4

Druhá transpozice:
Tabulka : 9 x 88
Transpoziční klíč získán vyčíslením fráze SLOVENSKO' .
Transpoziční klíč : 7-3-5-9-1-4-8-2-6

Šifrový text po první transpozici (OBRANANARODA)

```
RNNNZ KCUEL AAIAL YZGPC ONEOL VOZDE UOOHT PNRNI MHHVN
OIVBT IOETT MRVAO EEONZ UZGZU ZSPAR NTTAO VHRSA SASTA
IDTAI KZAYV EMPVY AEKYC UTHLA RDINI COEXE GAOAZ RIKSL
NRTIR HMSBA GNOZA IYCIR APLDO UMBNL NYOID HIRIA LEEMT
YZOEK YDEEZ ONAEE VVNAA OLDVS SORAO ODCIC PSPMS EKYJE
HAOYM COEZV OTBSA ASCNN TOAEM EBSNS JJCHK OTJXO OEIDJ
LIKDF KAIOS TKLMA TKIUR DERAA ACAZT AKREJ YNEEN LCIAA
IUNAN VREVK SPGTK RPRIO YUIOO FHTAH CYSAZ DVTAV IJCDB
NRISG YIIAD ITRIA OTSRK MIJOI EOEOA ULAAA TAYAO EEHPD
ENSTL OCAER EDAKD NIUTN SMDVO CEEON NKADY YSCER EZLDL
ETNEZ RRTVI PCSEI TPIRT UIIAN NEPAT CKJLE VZEYK KYOIS
ANCRA CSKTZ HCRAI NERCI VHZNX VAZVD OANDD SNIAA NEDAR
KNAES HOIRI ARTPE DUVJN AHBSN ABROV MNTIA IVDVZ IDLEA
TTOEE YRUSU APSVB LCHJA INRCI NUNIO EKIAE EYODA OSOHV
PNPOT IHDMI SLASE NVHRM ODBZR AALDS PVSKE SYKCE RAPNS
KUEUI VANDA ANNEC RRECA AMPAN ECOSJ NNHOK JPROS ABANE
TVRAO OETIA AESAE AKNAY YLEPS MISIJ RNNVD ORFEI CZSEO
MYVCI LGIEN IJJYC AJBAD IDVLA OO
```

Šifrový text po druhé transpozici (SLOVENSKO)

```
ZAEOM TAGTS IVHOR RZLYL KEDDE MSAJO FMRKL NTIYI GIJLE
LKDKE ZEIKK AAZAN SPBNI EVRKO TSBVR IEPNA OAENC IYVUZ
VTVEE ZOTAE RESSY UDMEV SCJES EKDIK AJAEP FZDIT EAPAI
CYDTP NEIKE VDAIU AAEUC NEHDV AENNR EKNTK MDEIJ ONACD
RIMZA RDECN ORGRN RZOAA PAONN JITRZ EUSOA TRIKO YNENO
CTPTA ENHIV INANO DTAAI ONSMD KUAAS RVAYI FYIDK LOOHI
OZTAK YLEIH ADOEY EVCKC AECEK AARCV KOSJY AOAEO DVAZR
IAJYC INNEH ESTDY BCISI EZSAV CAHBO EPNZL CLNAO ENVRU
RSTMU IATNA LIONO OMOTT SXKKD TENPY HAITM AASDS NENCU
TYCCV DAARA VVOPI ODPLO SCENA JOREY JEVJI EGOPN TOSVA
YKDGL BCMHT ENOPE ZCBOJ OICYA VRHDB ASOTD EUEYL VIEVS
TRASR RVBIA SHUEV MHASS DECJE INIOO EBORL PZNOT NPHIV
YIANA IBIYZ ARSHV NSTLS UANIK ITVND REAER TESEI RPZAZ
CZNKI JRVTU JNYPI RLYKA COPTA ASRMN ACYLH HOEUA SZAAX
KMIOI EDVSI YOAMH IATAE IRROA CIOIA HCNOD LRTNL OSNXD
DODNI LRLIA OHNRK PARNO AEASV SGAAN INUIB VZNAA PTCZI
OPNAE ALOSY BOJOD LEANA GUCVS RIUOT AMNRE SICKR RHOAE
THMZE SNEAO ADPEU NMNSA SLRIC JD
```

ÚLOHA č. III/4

ÜBCHI (dvojitá transpozice + klamače)

Body: 5

Heslo: HAWKE

POPIS SYSTÉMU:

Popis šifry ÜBCHI http://soutez2005.crypto-world.info/images/UBCHI.pdf

POZNÁMKA: pro řešení je podstatné, že prvá transpoziční tabulka je úplná a heslo pro druhou transpozici (neúplná tabulka) se dalo otestovat z množiny hesel druhého kola, správné transpoziční heslo bylo heslo z úlohy II/4. O jaké heslo jde lze odvodit z nápovědy …

1.klíč : CERNI BARONI (úplná tabulka)
+2 klamače
2.klíč : CERNI BARONI (neúplná tabulka) (bylo použito heslo z úlohy II/4)

Úlohu vyřešilo : 11 soutěžících

Popis systému:

Jako hlavní německý polní šifrový systém za I.světové války (především na francouzsko-německé frontě) byla používána šifra ÜBCHI. Skládala se z dvojité sloupcové (neúplné) transpozice vylepšené o vložení několika klamačů mezi první a druhou transformaci. Počet klamačů byl určen počtem slov klíčové fráze. Francouzi šifru byli schopni luštit. Pomáhalo jim především využití tzv. předpokládaných slov.

Použitý postup:

- OT se přepíše do úplné tabulky
- provede se sloupcová transpozice podle prvého klíče CERNI BARONI
- získaný text se doplní o klamače (podle počtu slov prvého transpozičního klíče, dva)
- tento text se vepíše do tabulky (neúplné)
- provede se sloupcová transpozice podle vyčíslení druhého transpozičního klíče (CERNI BARONI)
- druhý transpoziční klíč (heslo z II/4) máme díky špiónáži k dispozici (viz OT úlohy III/1)

OTEVŘENÝ TEXT (mezinárodní abeceda + doplněna soutěžní věta) :

Použit otevřený text z www stránky : http://www.uboat.cz/historie/1sv.htm

PONORCE U DEVET SE PODARILO TORPEDOVAT KRIZNIK HAWKE TENTOKRAT BYL OBRNENEC POD HLADINOU ZA OSM MINUT ZA NECELY MESIC BYLA POPRVE NEMECKOU PONORKOU POTOPENA ANGLICKA OBCHODNI LOD BYLA TO GLYTRA VEZOUCI NAKLAD SICICH STROJU A WHISKY POTOPILA JI PONORKA USEDUMNACT BYLO TO PRESTOUPENI DOSAVADNICH ZVYKLOSTI A KAPITAN FELDKIRCHNER VELITEL USEDUMNACT SE VRACEL DO PRISTAVU S JISTYMI OBAVAMI MEL BY BYT POSTAVEN PRED VOJENSKY SOUD NIKDO MU VSAK JEHO POCIN NEVYCITAL PREPADAVANI NEVALECNYCH LODI PONORKAMI SE ZAHY STALO PRAVIDLEM NEMECKE PONORKY OBDRZELY TEZKE KULOMETY VYBUSNINY A SEZNAM ZBOZI URCENEHO K ZABAVENI TAK SE STALO POTOPENI GLYTRY VYZNAMNEJSI UDALOSTI NEZ VITEZSTVI NAD KRIZNIKY A DALO OD RIJNA PONORKOVE VALCE NOVY SMER COZ SE PROJEVILO I VE VEDENI NAMORNI VALKY
DUKAZEM RESENI JE NAZEV POTOPENEHO KRIZNIKU X (693)

PARAMETRY ÜBCHI
První transpozice:
Tabulka : 11 x 63 = 693
Transpoziční klíč získán vyčíslením fráze : CERNIBARONI
Transpoziční klíč : 3-4-10-7-5-2-1-11-9-8-6
Klamače: doplněny dva klamače QW (dva neboť klíč se skládá ze dvou slov)

```
EDDKK EINMP UTCLY NHSJE OEIIL EMEUA YRSVI PNLML NRTTA
IAEEZ ATROO NSIMU IONCO EIOND IYOOO IILIC IASLP NTEVU
CVBBP YUCLI HAAMO YEYZZ SPYDI KLNEZ OADNT ZPEOK EYOAN
BERAC LEDJT OAESY ICLSR TMTJI EYDEO AVKDK UANNO YEIVK
JEMJD VMZHO TTRTL DOEYM KAHAZ SUORC SAKTH UEIYE AEKHC
ACNHI ERUSM EIPTJ NIYNV EEEAR EORPP NTRAM LPKPL NGCIH
LUYUD SFRDA AOYNK MOANC KTENL MNOKK OVUVD AOCOL NYEOI
VLTKB PZACN ONBYV AOONN ROVPR ETPSI SONJV ALPZA CBEBN
EELLN TTIIV SOEIE AEXOE RZNBL MEACU GDOUC WIABO AONEE
RTIBE SOPTA YRSLO EOIBO ATYIZ ADPLC IIKSP REIAW TCUZI
ENEOB ALRPO MPDZA ITCOI MOVDK EPAIE REOKY ZCVAG MSSNR
OYRVN ZNNUD RVAAE OTSVO PADRK TYPUO IHKKI ADJAP DUANE
VDSPM YZVER ATIAO ZZDKV PERAE EKNSO IEOHS CLEON OTOIA
PKTTV LANSV SMLVN DOIVN OYDPZ LNZHT ORSEN AAARV NLEVK
UAOHR NNUER POKOT ASKID TNCAD LNLSV TEOSN REOIO EKEYS
UBSNN LEIOR OEVOK JPIQW (693+2)
```

A nyní provedeme novou sloupcovou transformaci : (CERNIBARONI) a to jako neúplnou tabulku.

PARAMETRY ÜBCHI
Druhá transpozice:
Neúplná tabulka : 11 x (63/64) =695
Transpoziční klíč získán vyčíslením fráze : CERNIBARONI
Transpoziční klíč : 3-4-10-7-5-2-1-11-9-8-6

```
ISULA OOLPY LEAYE AMTZU CPAML OEVIO ONBVR DNTOI CROEM
NSUPY ZNOVD NAHTL ESOEH EMZIY SBOKP RSIUE RAHAI EAHAT
UONRO EIEGO PBCTL CIGZT PAMZK ETNLA OODRB VETIV ANILV
ISAOJ RAEZY CARYP LSOOO BATPL EMIIL ZRNDD YOVDK EAEOI
VOREE DTKIQ DCIII SOIUH PDATT VIHMS EUNPN FAKLP OPZNA
EABOA EEZKZ YARIV TRHAS YSVRT EEOWK NMLEU IABMI ZEEJK
JTHTC EERIA KVECN SBIOU AOILW ATAAN OYJPO ELTVZ AAKAN
UEUES TOEIE LZOYD SOYME REEIR PDMNC KVELL ILWTS IPEPV
KRRAK NRPEO SNOLU IVEEI KYENE MDIVA DTBAT DKTAK HMETC
DCOYA NICTX COSOP ABIPV VETDS AECKL PNUOC SSOPO RTOOI
TCZZE ELEOV OOYIN OKUKM OTYRA EEBCR RYSIM OONDP HAEVI
TNVTN NKSOL PMEYR RCONU YEKLC DNDDU IHJEP YNLAL BPVEO
NUEYT KZOME SUOIU VKOOA IHVNS LINJD LLPAI NCCAY NNOMK
VOKAK SVNGR NKNZO SATEA BEEDI OAECR AKADI ASPMD EKPNO
YRNJA NTNOP YENOC IYNJL SENTR LUYND VNVJN SZOEA AIUPI
RSNVO DZDSN LOZRR ANONK (695)
```

ÚLOHA č. III/5

Šifra ADFGX

Body: 5

Heslo: HINDENBURGOVA

POPIS SYSTÉMU:

Popis šifry ADFGX http://soutez2005.crypto-world.info/images/ADFGX.pdf

POZNÁMKA: při sestavování šifry je nutné sestavit převodovou tabulku a dále provést jednoduchou transpozici určenou klíčem. Při luštění se provede nejprve zpětná transpozice (klíč se dál odvodit a následně se řeší získaný text jako jednoduchá záměna, kde znaky šifrové abecedy tvoří bigramy – souřadnice převodové tabulky …)

1.klíč : AŤ ŽIJE NAŠE REPUBLIKA ZVÍTĚZÍME (neznají)

2.klíč : BRATISLAVA

Úlohu vyřešilo : 10 soutěžících

Použitý postup:

Pomocí substitučního hesla se vytvoří převodová tabulka. Heslo se vepisuje do tabulky zleva doprava, pokud již nějaké písmeno hesla bylo do tabulky jednou vepsáno, tak se při dalších výskytech vynechá. Tabulka se doplní písmeny, které v hesle nejsou obsaženy. Zvolené substituční heslo vede na výše uvedenou převodovou tabulku.

Substituční klíč : AŤ ŽIJE NAŠE REPUBLIKA ZVÍTĚZÍME!

	A	D	F	G	X
A	a	t	z	i	j
D	e	n	s	r	p
F	u	b	l	k	v/ww
G	m	c	d	f	g
X	h	o	q	x	y

Druhý klíč tzv. permutační, určoval po permutačním vyčíslení příslušnou transpozici

Transpozice:

Tabulka : 10 x 130 = 1300

Transpoziční klíč získán vyčíslením fráze : BRATISLAVA

Transpoziční klíč : 4-7-1-9-5-8-6-2-10-3

OTEVŘENÝ TEXT (mezinárodní abeceda + doplněna soutěžní věta) :

Použit otevřený text z www stránky : http://www.payne.cz/2xS43907/valka1.htm

zadej nazev linie hlaseni zacatek usilovne utoky nemecke jez pronikly v breznu smerem k amiensu a v kvetnu az k rece marne nadeje v prulom nesplnily zatim general foch jmenovany take velitelem vojsk anglickych dusi jeho stabu byl general petain pripravil sam ofenzivu mel k ni zvlast po prichodu americanu nejen potrebnou zasobu rezerv ale i vyzbroj jeho byla zejmena uzitim velkeho poctu lehkych tanku dokonalejsi nez nemecka na marne kde pred ctyrmi lety francie prvy utok zachytila pocalo se ode dne osmnacteho cervence vitezstvi dohody a ustup nemcu nedavaje nepriteli oddychu a utoce na novych a novych usecich fronty vycerpal foch postupne energii a zasoby nemecke a prolomil strasna opevneni nemecka vcetne tzv linie hindenburgovy konec hlaseni zadej nazev linie x (650)

Substituční klíč : AŤ ŽIJE NAŠE REPUBLIKA ZVÍTĚZÍME!

```
     A  D  F  G  X
A    a  t  z  i  j
D    e  n  s  r  p
F    u  b  l  k v/ww
G    m  c  d  f  g
X    h  o  q  x  y
```

Šifrový text po substituci:

```
AFAAGFDAAXDDAAAFDAFXFFAGDDAGDAXAFFAADFDADDAGAFAAGDAAADDAFGFADFAGFFXDFXDDDAF
AADXDFGXXDDDAGADAGDFGDAAXDAAFDXDGXDDDAGFGFFXXFXFDDGDAAFDDFADFGADADGDAGAFGAA
GAAGDADDDFFAAAFXFGFXDAADDDFAAAAFFGDGDAGDDAGAAADGDDDADDAAGFDAAXDAFXDXDGFAFFX
DGADDDADFDXFFDDAGFFXXAFAAADAGGAGXDADDDADGAAFFGGXDGDXAAXGADADDXDFXAADDXXADAA
FGDAFXDAFFAGADDAFFDAGAFXXDAXDFFGAADDGXFFAGGDFGXXGDXAGFFADFAGAXDAXAXDDFADAAF
DFAFDXXFFGXDADDDADGAAFFDXDAADAAAGDDDXDGAGDXDGAAFXAGFFDFAAGAXDGGDADDAFAGFXFA
GADAFFFGDDAGAFFXFFAADFADDXXDDXDGAGGDXAXDGFFAAAGADADGAGGDAADDFADDDAAXDADDDXX
DADDGDAFDDDXDFAAFAADFXDFDFADGDAAFDADGFXAAFFDAAGFXXXAFFDDGXDAXAXDAXAXDFDXXFF
AAAFDAAXGADADDAAFAAFAGADAGGAFXDAFFFGDAXAXDDXXDGDADFAFFDAXAFGXXGDXAADAADDFGF
AGFXDFGXDDDAAFFDAAXDFAGDDDAAFDDDAGADAGDFGAADDAAGAAADGDDDAFGGFDADXDGDAGFGDAD
XXDGGAAGFFDAADXXGGDGAADDGDAGDADXDGFXXXFAADXDFGAFAAGDXAXXADAGFFAADXXDGDAAFFX
DDFDAXDGFDAGFDDDAXDDFGADDAAGDADDAXAXDGDDADGFXDADDGDDAFXAGADDAAFDFADFXAGGFXD
XAXDGFXXAAFADFADFADXDDDAGAGDFADDDAGFAAFXAAAXDADDDADXDGAGADDAFFAGXDGFGFXXGDX
AFAAAFAADXDGDDADDAADDXDFXXXGDXAAADDXDFXXXGDXAFADFDAGDAGGDXAGGDGXDDDADXXFXXX
GDDADGDXAAFFGGXDGDXADXXDDFADFADXDDDADADDDADGGXAGAGAAAFAADFXDFDXXDDDAGADAGDF
GDAAADXDGXDFFXDGAAGFFDFADDGAADFDDAAXDDXDAFXDDDADDAGDDDAGADAGDFGAAFXGDDAADDD
DAADAFFXFFAGDDAGDAXAAGDDGFDADDFDFADGGXXDFXXXFGXDDDDAGDXAFFAADFDADDAGAFAAGFD
AAXDDAAAFDAFXFFAGDDAGDAXG (1300)
```

Permutační klíč : BRATISLAVA (10)

Šifrový text po transpozici:

```
AAAFA AADXG AAFFD AAAFG DDFDF ADXDD DAFAG GDAFD ADFGA
DAAAF ADDFA DFFXX ADAFD FGFXA AGGFD DADDX XAFGX GGDAF
XDDDA DAGAA GFDXA DGXDD AXGDA ADDDG ADDFX GDGAD AAGFA
GDDAA GFAAG DGAAG FXAFF XAADD AFXXX FDAAF GXFGX GFDAA
AXDDD FFFXX XAAAD ADFAG AAGAD GGGXF DDFFA AGAFF XADAD
DFADD ADDGX XDDAG FAAFF DXDGD XAAXD FGXXA XXAAD AXDAX
DXFAA FXADD AGDDA AFXXA FAFFD GFDDX DGFAA DAXDA DAGAD
AADAF AFXAD GADFD ADDXD FGAAA GDADD AXXFD AXAXA AFAAX
DAGDX AAADG DAADD ADAAD FADDD AFDFG ADFXD ADDFD DDFDD
GFDAD DAFDA ADGGA FAGFA XAAXD DDAAD GADDG DFDDA FDADX
ADADX FXDFD DDADD XDADA GFAXD AXDAA XFDDA DFXFD XXFGD
GFDDD AFDDG DXDGF DAAFF DDAAA GADAA DFFDF DFDDG DFDDA
AFXDX GDGDX FDXDF FXFGA AAAXA FFDGA GDXDD DAXAF DAAFX
DXFDD DFAGG GXGFF XDXDD ADGDA GAGGD AXXXD XXDGX DXDDG
ADFXF DDAGD AAGDF XDDDA DDADA FXADD DFDGF DFFDD GDGFA
GAXXA DFAGX DXFDF ADFGF FFXXG AAAXX AFAAX AFGDG XAGAA
DADDG AGAXA AXDGG DDDAG XFGAD AGFGX AGGDF DGADA DDDFD
DFDFA FDDGX FAAFD FDFAD AFDGA ADXDG AAAFA AXAAG DDGAA
GGAGG AXDXA AXAAD AGFGF GADAF AGGGA AAGAD AXDGA AAAAG
XAAXD DFADA ADAGD AADDA XFXAD XDADD DFXXA ADAXA GDAAX
AGGDX AFAAG FFDAF AFADG XGGFA AXDGA AXDXX AGDDX XADDG
AADXA AGGDG FXXDA DADDF AAXXD AAGGD AAADF DGAFF AXDXG
XXDAF DADAG FDAFA GDADD AXAGX GDFAX ADGDF FAGDA FGFGG
ADAAG AAGFG DGAXD FGDAA GADGA DAFFF GADAD ADXAD FAAFG
DGXAF AFDGA GDXDA GXXDD FDDFX FDGDX FDAGA GDDGD AAFFD
DDDDX DFAAX GGDDA DXFAD AGDDG FXDGG AXDAD DDDAX DAFFD
AFDDG FFXGA XXADA DFAGD DDDDA DFAFA FDDFG ADFDD DDDDF
DADXD DDDFF DDFDF GAFXA FAXFD GDDDA FDDFA AGDDD XFFDX
ADFFD DGADF DXAXX AXFDA XGAXA ADDAD FXDXD AADFX (1300)
```

ÚLOHA č. III/6

Enigma (nastavení jako v ukázce)

BODY: 4

Heslo: LACHMAN

POPIS SYSTÉMU: Dešifrace textu zašifrovaného Enigmou - Crypto-World 78/2005, příloha (zde uveden vhodný emulátor)

POZNÁMKA: použité nastavení šifrovacího stroje Enigma je stejné jako v ukázce jak dešifrovat text zašifrovaný Enigmou … http://www.princ7.demon.co.uk/method.htm

Úlohu vyřešilo : 18 soutěžících

Nastavení v ukázce:

Action	The settings we used	Picture
Bring the lever forward so that the reflector disengages from the wheels	B	1
Select the three wheels for use	V IV I	2
Select each wheel in turn and set the ring setting" or to use the German term "Select each wheel in turn and set the Ringstellung".	S (19) C (3) A (1)	1
Re-plug the board with the new cable patches.	NT DY HL UF IS BG ZC EJ XK OR	3
Set the wheels to the first daily setting	NUP	4
Enter the first tri-graph	Type AYT, lamps QGQ light	5
Set the wheels to the Message Key QGQ		
Type the message		6
Open message		***6***

OTEVŘENÝ TEXT (mezinárodní abeceda + doplněna soutěžní věta) :

Použit text z knihy Robert Harris: Enigma, nakladatelství mustang, 1997

ADRESOVANO VRCHNIMU VELITELI NALEHAVE DVANACT KILOMETRU OD SMOLENSKA BYLY VCERA NALEZENY LIDSKE PZUSTATKY PATRNE VELKY HROMADNY HROB MOZNA TISICE LIDI CO MAM DELAT LACHMAN OBERST POLNI POLICIE NASLEDUJICI ZPRAVA BUDE ZASIFROVANA POMOCI KODU SUP URCENEHO PRO DRUHY BREZEN JEDEN TISIC DEVET SET CTYRICET TRI PROSIM ZADAT JMENO OBERSTA KTERY NAHLASIL NALEZ V KATYNSKEM LESE

Šifrový text (zašifrováno vhodným emulátorem a po doplnění hlavičky):

```
QRX QTC QTC = ENIGMA STN = NW QTC = CQ
CQ CQ DE CW2005 CW2005 CW2005 = ENIGMA MESSAGE =

0000 317 NUP AYT =
VZFOA UMZTT IDDIQ RVTOS BJWQQ DAWEQ UPMKA CDWHA MFOKV ZYHUF XNOCC SPSKH
VCKOQ DPGQV EGJCP ZMHSY FESPH NYLYL CQPYP UYXQC KZHTO YADKG LIXCQ EHUYG
WUTEJ XKTAI LXPDY CBDXF PMTSQ KWQPT MLIQT GTJFZ AFTBP SMQLR TJVME JZESN
NOKTO VMOSA FUVIA HOIAM VKQAD UYLAG KDVGB SGOYG LGYYH YFGEH IOGCH VOYGP
ZEVQA CDSON PSMGD RFUSD NZJPT WYNCL MKQKO DDZRJ JWVIC CCOZU QUKAF JJVZE
XIUSX HPJYB JCZWH QV+
= RPT =
```

```
VZFOA UMZTT IDDIQ RVTOS BJWQQ DAWEQ UPMKA CDWHA MFOKV ZYHUF XNOCC SPSKH
VCKOQ DPGQV EGJCP ZMHSY FESPH NYLYL CQPYP UYXQC KZHTO YADKG LIXCQ EHUYG
WUTEJ XKTAI LXPDY CBDXF PMTSQ KWQPT MLIQT GTJFZ AFTBP SMQLR TJVME JZESN
NOKTO VMOSA FUVIA HOIAM VKQAD UYLAG KDVGB SGOYG LGYYH YFGEH IOGCH VOYGP
ZEVQA CDSON PSMGD RFUSD NZJPT WYNCL MKQKO DDZRJ JWVIC CCOZU QUKAF JJVZE
XIUSX HPJYB JCZWH QV+
```

ÚLOHA č. III/7

Enigma

Body: 5

Heslo: CRYPTOWORLD

POPIS SYSTÉMU: Dešifrace textu zašifrovaného Enigmou - Crypto-World 78/2005, příloha

POZNÁMKA: použité nastavení šifrovacího stroje Enigma bylo uvedeno v otevřeném textu úlohy č. II/2). Toto nastavení je kód Sup z 2.března 1943:

III IV II LUK JP DY QS HL AE NW CU IK FX BR

Heslo pro důkaz vyřešení je voleno velmi slabé. Předpokládal jsem, že jej možná někdo otestuje a úlohu tím „vyřeší“….

Úlohu vyřešilo : 15 soutěžících

Action	The settings we used	Picture
Bring the lever forward so that the reflector disengages from the wheels	B	1
Select the three wheels for use	III IV II	2
Select each wheel in turn and set the ring setting" or to use the German term "Select each wheel in turn and set the Ringstellung".	S (19) C (3) A (01)	1
Re-plug the board with the new cable patches.	JP DY QS HL AE NW CU IK FX BR	3
Set the wheels to the first daily setting	LUK	4
Enter the first tri-graph	Type HAN, lamps JRY light	5
Set the wheels to the Message Key JRY		
Type the message		6
Open message		***6***

Část otevřeného text z úlohy II/2, kde jsou parametry popsány.

REFLEKTOR SPACE B SPACE WHEELS SPACE III SPACE IV SPACE II SPACE RINGSTELLUNG SPACE S SPACE C SPACE A SPACE PLUG BOARD SPACE JP SPACE DY SPACE QS SPACE HL SPACE AE SPACE NW SPACE CU SPACE IK SPACE FX SPACE BR SPACE

Chybí zde parametry pro tzv. Ringstellung. Toto nastavení je totožné s nastavením z předchozího příkladu….

OTEVŘENÝ TEXT (mezinárodní abeceda + doplněna soutěžní věta) :

Použit text z knihy Robert Harris: Enigma, nakladatelství mustang, 1997

ZA OBLEVY ZAHAJENY VCERA V OSM NULA NULA VYKOPOVE PRACE V KATYNSKEM LESE PROHLEDNUTY PADESAT DVE MRTVOLY OBJEVENO MNOZSTVI OSOBNICH DOPISU MEDAILI A POLSKE MENY TAKE PRAZDNE NABOJNICE RAZE SEDM SEDESAT PET OZNACENE CITUJI GECO D KONEC CITATU Z VYSLECHU MISTNICH OBYVATEL VYPLYNULO ZE POPRAVY PROVEDL NKVD BEHEM SOVETSKE OKUPACE V BREZNU A DUBNU TISIC DEVET SET CTIRICET CELKOVY POCET OBETI SE ODHADUJE NA DESET TISIC OPAKUJI DESET TISIC JAKO DUKAZ RESENI NAPIS NAZEV EZINU KTERÝ TUTO SOUTEZ USPORADAL

(Foto vlevo: Autor soutěže si hraje s historickým šifrátorem Enigma)

Šifrový text (zašifrováno vhodným emulátorem a po doplnění hlavičky):

```
QRX QTC QTC = ENIGMA STN = NW QTC = CQ
CQ CQ DE CW2005 CW2005 CW2005 = ENIGMA MESSAGE =

0000 420 LUK HAN =

QSGTQ UJIKK IVFZI APIHF WHFXX WKHNA PXWZJ HNAAC VAWZK IIEVV
VKIAS YUQKL IAWQO QJWFM JEOVF HSAHE SYCGH USFFT DQEND QSGDO
LVUFD CFGWM OYBSG JIZYV BXDGT DOLHV TFWZE AYNFG FIMNL ZRZZH
DTVJF TJRAQ ALHQK JJJVP XIILL RHYUR FQKNH XOAVF KIIYX AOOXF
ROPRL NOEQO YSPVD EDIHD TWSRJ TANEB BHCIA MDXRK VJHWJ GQFHM
DPRTB CCQAK ZDUIT ECHOS IXYBT JGKML GBKRN KAQKK PEVIZ OQVFD
AFLEV MQYDY MOONW TZUON UGRKS LUJCD BHKQQ HNIVV WMNOB YEQFO
WOYHL NBRRP YUYMX PSRIZ AJQBZ SNODI CPFVQ WDGFG YELCA ILJJI
ZNRPX XYMWM BVHKL QMJKJ
= RPT =
QSGTQ UJIKK IVFZI APIHF WHFXX WKHNA PXWZJ HNAAC VAWZK IIEVV
VKIAS YUQKL IAWQO QJWFM JEOVF HSAHE SYCGH USFFT DQEND QSGDO
LVUFD CFGWM OYBSG JIZYV BXDGT DOLHV TFWZE AYNFG FIMNL ZRZZH
DTVJF TJRAQ ALHQK JJJVP XIILL RHYUR FQKNH XOAVF KIIYX AOOXF
ROPRL NOEQO YSPVD EDIHD TWSRJ TANEB BHCIA MDXRK VJHWJ GQFHM
DPRTB CCQAK ZDUIT ECHOS IXYBT JGKML GBKRN KAQKK PEVIZ OQVFD
AFLEV MQYDY MOONW TZUON UGRKS LUJCD BHKQQ HNIVV WMNOB YEQFO
WOYHL NBRRP YUYMX PSRIZ AJQBZ SNODI CPFVQ WDGFG YELCA ILJJI
ZNRPX XYMWM BVHKL QMJKJ+
```

E. Soutěž v luštění 2005 – z poznámek soutěžících

Úloha I/9 (Noty)

Standa Tvrz
… správné řešení bylo to, které mne napadlo jako první, ale kvůli neviditelným trámcům jsem to vzdal.
Zkoušel jsem proto jiné možnosti, ale nevedli k cíli: zkoušel jsem řešit jako jednoduchou záměnu se znak = viditelný takt; znak = viditelný takt, nebo část taktu oddělená celou notou; znak = nota(podle výšky a délky). Kdybych zůstal u první možnosti a pokusil se restaurovat trámce, nemusel jsem být na té potupné 15 pozici : (
Těším se na další kola (kdy jej mohu čekat?).

Pubal Frantisek
… teda bylo mi jasny, ze kontrol. slovo bude ňákej známej fidlalista, tak jsem zkoušel Bach, Dvořák, Smetana, ale Čajkovskij...k tomu sem nedosel...

Úloha I/9 (Klingoni)

Stanislaw Schmulinsky
velmi jsem si užil úlohu č.9, potěšilo mě, že v době Harryho Pottera se ještě najdou příznivci poručíka Worfa :-).

Pavel Horal (Palko)
Vyluštil jsem úlohu číslo 9, ale stále mi není jasné jaké řešení mám zadat.
Jestli jsem to pochopil správně z textu úlohy ("tato abeceda neni moc vhodna na prepis ceskeho textu snad vam uloha nebude delat velke potize jako dukaz vyreseni ukolu zadejte kdo temito pismeny pise"), tak musím odpovědět kdo danou abecedou psal nebo píše. K tomu bych jí ale nejdříve musel poznat, což opravdu nedokážu....

Martin Suchan
… pisu Vam, protoze bych mel namitku vuci jedne uloze, konkretne uloze c.9.
Samotnou transpozici jsem mel hotovou behem pul hodinky, ale co prislo potom me docela sokovalo - klicove slovo neni v textu, je treba zjistit, kdo pouziva tuto abecedu. Priznam se, ze jsem ztravil asi 4 hodiny hledanim na google a ve Wikipedii, shledl jsem pres sto ruznych jazyku, abeced, fontu, pisem a run a zadny z nich se nepodoba tomu, co bylo pouzito v teto sifre. Take na strankach http://www.ancientscripts.com/ , kde je velmi dobře zpracovana databaze vetsiny pouzivanych pisem jsem na nic nenarazil. Prijde mi to ponekud nefer, protoze tuto soutez jsem vzdy povazoval za soutez v kryptoanalyze, ne v lingvistice. Je mi jasne, ze ted, kdyz uz tuto ulohu par jedincu nejak vyresilo je asi zbytecne o neco zadat, ale na druhou stranu, pripadna mensi napoveda by mohla nejenom me pomoci.

Ladislav Kvasnička
Jeste, co byl od Vas peknej podraz bylo reseni I/9 "kdo pise touto abecedou" - zahajil jsem obrovske patrani, ale nikdo to pismo neznal. Do googlu to neslo zadat :(. Po nekolika dnech jsem to nejak nasel. To nebylo vse, pak jsem zapasil co napsat, zkousel jsem nazvy ze www stranek - vse anglicky, zadal jsem kde co a nic. Az po dlouhe dobe jsem zkusil KLINGONI a ono to bylo ono.

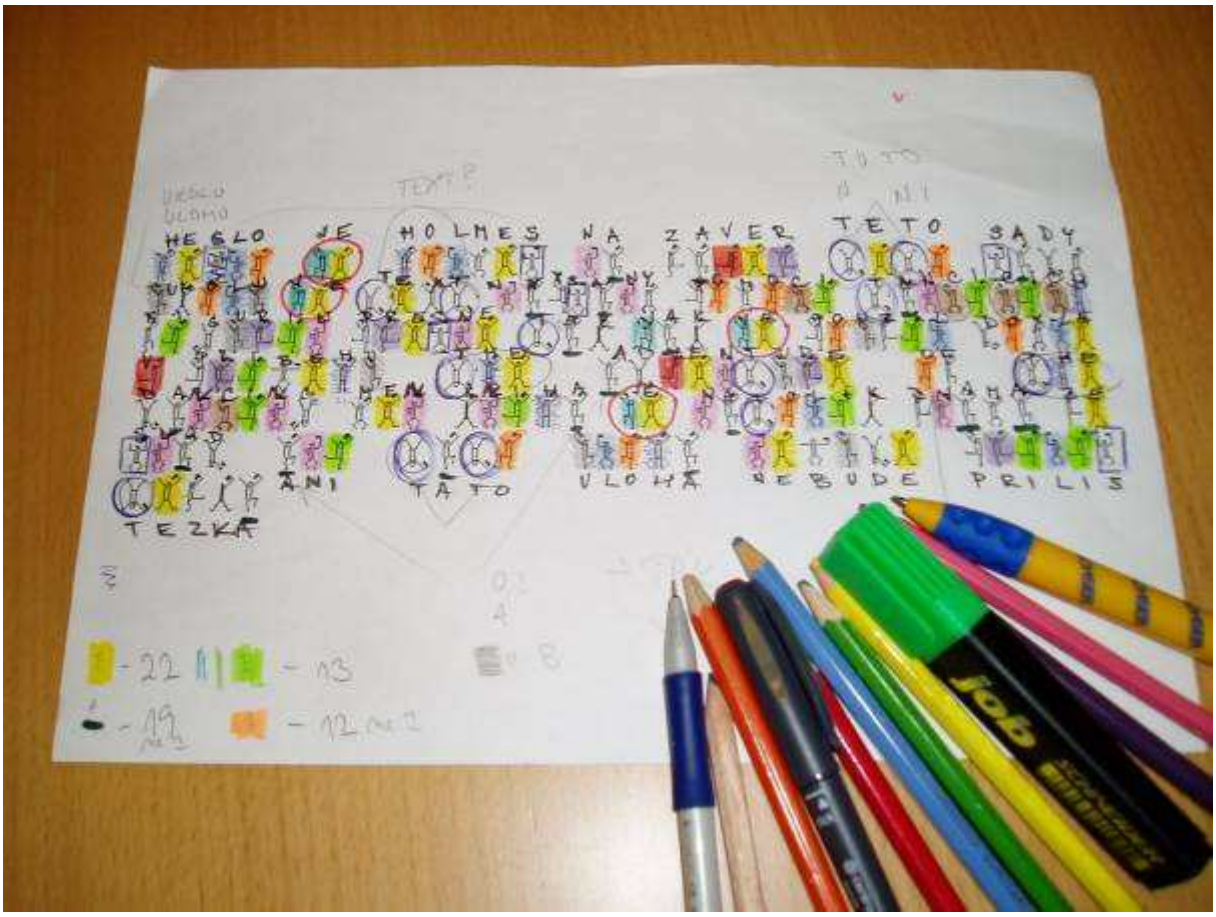
Josef Mika
Bohuzel me StarTrek trochu minul, ale uz se mi to podarilo desifrovat
viz http://ufp.wz.cz/Ste/Rasy/Klingon/Pismo.htm

Peta Polacek
…. ta byla drsna. Co ja prolezl stranek o ruznych archaickych pismech a ono to je z budoucnosti. Nakonec mi to prece docvaklo :-) Jestli tohle bylo v prvnim kole, tak co bude v daląich?

Necroman
Napoveda k 9. uloze je dle meho nazoru dobra, je videt, ze z "nejtezsi" ulohy, dle poctu reseni, se hnedka stala uloha "spise tezsi".
Ulohu 9 se mi nakonec podarilo vyresit, kdyz jsem po nekolikatem prochazeni odkazu z googlu narazil na stranky www.omniglot.com , které popisuji i nejznamejsi umele abecedy.

Úloha I/10 (Jednoduchá záměna)

Posilam Vam foto dokumentujici me lusteni posledni ulohy prvniho kola. Je to asi trochu ostuda, ze jsem neznala tu knizku a tak jsem musela lustit klasickym zpusobem, ale zase je to hezky barevne, ne? ;-)
Zuzana Rybarova



Úloha II/1-II/3 Jednoduchá záměna

Peter Gaži
Za zmienku mozno stoji ze som mal k dispozicii iba jeden cesky text - Capkovo R.U.R. z Projektu Guttenberg - ktory sa pre mna stal meradlom "ceskosti" textu pocas celej sutaze. Kedze viedol k vylusteniu vsetkych sifier svedci to o nadcasovosti Capkovho jazyka:))

Zuzana Rybarova
Take mi delala dlouho potize uloha II/2 (ani nevim proc), nad tou jsem stravila opravdu hodne casu - ale je fakt, ze jsem pak mela o to vetsi radost, kdyz jsem ji konecne vylustila.

František Půbal
… ale musim se priznat, ze i kdyz jsem vedel, ze II/3 je vo slovencine, vubec mi nanapadlo zadat kontr. slovo Slovensko!!
....po takovem uspechu s fidlalistou Cajkovskym...hamba hamba.

XXX
a jak se objevil první bigram PR !!! uz jsem začuchal!!! a pak už se po pár dalších písmenech ozval vitězný ryk !!!

Úloha II/4 (sloupcová transpozice – (úplná tabulka))

Ladislav Kvasnička

… ulohu II/4 jsem si "spravne" urcil velikost sloupce na 13 a pekne jsem si zakombinoval se sloupecky, bohuzel vysledek se nedostavil, se spravnou hodnotou (39) uz to pak byla hracka.

Úloha II/5 - - Fleissnerova mřížka

Alchymista
Jeste perlicka k uloze II/5 - Fleissnerova mrizka. Tuto ulohu jsem resil hrubou silou (nenapadlo me, ze bych mel zkusit nejdrive lonskou mrizku), a tak me zamrazilo, kdyz jsem si precetl:
TAK KDOPAK BYL TAK CHYTRY A SCHOVAL SI LONSKOU TABULKU ZAPISTE ALCHYMISTA
poprve me zamrazilo, kdyz jsem si precetl svuj login v otevrenem textu ;-), a podruhe, kdyz jsem si OT vylozil tak, ze ALCHYMISTA by mel byt tak chytry, ze si schoval tabulku z lonska, a pritom jsem ja, ALCHYMISTA, prave v tom naprosto selhal :-)). Kazdopadne si precist svuj login v OT je (i kdyz to byla patrne nahoda) dost zvlastni pocit.

Room132
Samozřejmě jsme použili silu, kvůli těm dvěma x na konci jsem to chtěl zkusit ručně, ale ten java script na to není vhodný. Lepší by byl ten program z loňska, ale nedokázal jsem tam změnit text.

Úloha II/6 (Periodické heslo – systém Vigenére)

Ladislav Kvasnička

Takova perlicka: vcera se mi podarilo zjistit heslo pro ulohu II/6 prakticky bez lušteni. Vydedukoval jsem, že by otevrena cast textu by mohla byt general Model, to jsem zadal do google a z textu se nabizeli dve hesla - STALINGRAD a CITADELA.
Kupodivu to druhe bylo spravne rešeni. To jsou zpusoby rešeni....

Úloha II/7 a II/8 (Absolutně bezpečný systém)

Zuzana Rybarova
… nejprve moc dekuji za usporadani souteze, je, stejne jako minuly rok, super!
Nejtezsi pro mne zatim byly ulohy II/7 a II/8 - vubec nevim, jak je nekdo mohl vylustit predtim, nez byl zadrzen spion s castmi otevrenych textu :-]

Petr Kocfelda (koc)
Nejdříve jsem si přečetl doporučované číslo e-zinu 10/2001 a řekl jsem si, že dva stejné typy úloh jsou v zadaní zřejmě z toho důvodu, že jsou obě úlohy podle Situace I. zašifrované stejným heslem. A tak jsem se soustředil pouze na navrhovaný způsob luštění.
V Excelu jsem si spočítal rozdíly mezi otevřenými texty (O1,O2) a připravil tabulku do které šlo zapisovat do jednoho sloupce první otevřený text a druhý se objevoval v druhém sloupci nebo do druhého sloupce druhý otevřený text a objevoval se první.
Dále jsem ve VisualBasicu napsal program, který pro zadaná slova prvního otevřeného textu vyzkoušel všechny pozice a do souboru zapsal slova (složená pouze z písmen) z druhého otevřeného textu (a samozřejmě naopak). Vložil jsem tedy slovo prvního otevřeného textu do vstupního souboru, spustil program a ve výstupním souboru jsem hledal srozumitelné slovo druhého otevřeného textu.
Nejprve jsem si slova vymýšlel a našel i několik vhodných, ale nikam to nevedlo. Tak jsem začal používat některá slova z frekvenčního slovníku s délkou nejdříve 10 a pak 12 písmen. A tak se mi podařilo pro slovo DOKUMENTARNI najit odpovídající význam PRIKAZALBUH.
Mysleli jsme (v tomto okamžiku se přidala i moje žena, které nešla vyluštit třetí jednoduchá slovenská záměna), že to bude o náboženství a tak jsme zkusili Google a hledali, co všechno "Přikázal Bůh". A tady jsme hned na začátku překvapivě narazili na příslušný projev G.Bushe, a protože jsme již měli v textu slovo GEORGE, začali jsme tušit, že luštíme dobře. V Excelu jsme pak dohledali zbytek textu. To už šlo víceméně samo, protože jsou oba otevřené texty stejné a pouze posunuté.

XXX
Pomohl mi az zverejneny lustici program a pritel google, ktery po zverejneni useku OT vyhledal zdroj OT:
http://www.google.com/search?hl=en&q=DOKUMENTARNI+FILM+BBC+KTERY+BUDE+ODVYSILAN+V+PONDELI&btnG=Google+Search

vita novy
Ze by ty dve ulohy mohly byt onim inzerovanym dvojitym pouzitim stejneho klice me napadlo celkem brzy. Udelal jsem tedy podle navodu rozdil zasifrovanych textu. Dost dlouho

mi pak trvalo, nez jsem si uvedomil specifika te rozdilove operace a jak musi vypadat tabulka kodovani pismen, aby mohla vzniknout vsechna cisla, ktera se v rozdilu vyskytuji.
Cili ze A je mezi 5 a 9 vcetne. Diky vyskytu cisel 31, 34, 35 a 79, ktera lze jako rozdil ziskat jen jedinym zpusobem, jsem usoudil, ze A = 5 nebo A = 9, ostatni pripady by vedly na prilis caste pouziti W a X nebo kombinaci malo frekventovanych pismen, coz jsem vyloucil. Diky temto cislum v rozdilu jsem taky mel na prislusnych pozicich hodnotu klice, takze jsem vyzkousel jestli klic neni prece jen kratky a pouzity vicektrat za sebou. To jsem vyloucil az do delky klice 100.
Pak uz me nic nenapadlo, tak jsem zkousel uhadnout nejake slovo a pouzival obe tabulky (A=5 a A=9). Moc to neslo, tak jsem jeste vytvoril ocekavane frekvence jednotlivych hodnot v rozdilu pro obe tabulky a porovnanim s frekvenci rozdilu realnych jsem se priklonil k A = 5 i kdyz to moc prukazne nebylo. Pak uz jsem hledal slova jen podle tabulky A = 5 a posleze jsem narazil na slovo PREZIDENT, ktere v druhem textu davalo OSMEHORIJNA. Zkusil jsem tedy i v prvnim textu najit nejake cislovky a mesice a nasel SEDMEHORIJNA, coz mi zase v druhem textu otevrelo vyraz OPAKOVANITELEGRAMU. Pak uz to bylo uplne jasne.

Úloha II/9 (zlomkový systém Early Chase)

Peter Gaži
Co sa tyka postupov riesenia, niektore sifry aj mimo prveho kola boli lahko riesitelne rucne (najviac ma potesil II/9 - Earle Chase system, kde som mal ziskany hint z predoslej sifry a len som si na papieri skusil ci sa neda vyuzit na skonstruovanie hesla presne rovnako ako v popise sifry a islo to:).

vita novy
Taky 2/9 je zajimava, napovedu z 2/6 jsem rychle zapomnel a kdyz posledni sifra odolavala vsem pokusum o moji amaterskou analyzu a na internetu taky nic, zacal jsem se pomalu chystat na generovani vsech moznych tabulek pomoci slovniku. A pak znenadani ve vane - heureka, jsem si vzpomnel, ze o posledni sifre uz byla zminka driv.

Úloha III/3 (Dvojitá transpozice)

… Byl to problem moji hlouposti - spatne naprogramovany algoritmus detranspozice podle zname permutace. Vsechno jsem psal v octave (free obdoba matlabu) a nejsem s tim jeste 100% kamarad.

… a ta dvojita transpozice uz byla moc , sice jsem lustil podle kodu "SLOVENSKO", ale zvolil jsem spatny rozmer, zkousel jsem 18 a 22 sloupcu. S napovedou to samozrejme pak byla sranda.

Mirka Kemenova
Tu som sa najprv pokusala riesit manualne - spravne som z hintu odvodila druhe heslo, po jeho aplikovani som sa skusala na text autisticky pozerat a najst spravnu permutaciu. To sa mi vsak nepodarilo, tak som si aj pri tejto ulohe trochu zaprogramovala.
Snad sa program bude hodit na buduci rok. ;)

Úloha III/6 a III/7 (Enigma)

Jeste bych rad nabidl odkaz na simulator Enigmy, ktery jsem uspesne pouzival, napsany v bash: http://www.forthrt.com/~dbarlow/

Pracovna jednoho z luštitelů, „samozřejmostí“ je i vybavení E-enigmou (viz šipka) (http://www.xat.nl/enigma-e)

Obecné komentáře

Tomas Sieger

prave jsem dolustil posledni ulohu ;-) a obsadil tak po tuhem bezesnem boji (spal jsem dve hodiny mezi pul patou a pul sedmou rano) 3. misto a rad bych Vam, krome opetovneho podekovani za to, ze takovou soutez organizujete, napsal par okamzitych postrehu (mozna zatizenych mym "vypnutym stavem").

… do posledni chvile nevedel, kdy budou zverejneny ulohy tretiho kola - kdybych to vedel dopredu, mohl jsem si lip rozplanovat cas - pro zenateho a zamestnaneho je sednout si nahle na celou noc k lusteni trochu komfort, ale natolik jsem chtel uspet, ze jsem si to nemohl odpustit ;-). V kontrastu s timto "tajnustkarstvim" mi pripadalo perfektni (nekdy se az mirne prehnane) naservirovavani informaci lustitelum pod nos: napriklad kdyz jste mi napsal, ze ve tretim kole se budou resit sifry 1. a 2. sv. valky, peclive jsem si postahoval oskenovane

clanky Dr. Klimy z CW s SW a pidil se v nich po danych sifrach, abych si mohl predem pripravit lustici programy, a pak jsem si jejich seznam precetl ve Vasi napovede :-).

Vyridte, prosim, moje podekovani taky panu Vodruskovi mladsimu - webove stranky jsou skvele (online zasilani dukazu o vyreseni, zebricek lustitelu, info o tom, kdo vylustil jake ulohy a v jakem poradi - to je mimochodem pekny postranni kanal - kdyz jsem byl na pochybach, jestli lze ulohu III/6 vylustit bez znalosti OT z ulohy III/3, tohle mi pomohlo ;-)).
Ladislav Kvasnička
… chci moc podekovat za peknou soutez. Sifry i samotna soutez je opravdu velmi pekne udelana…

Room132
"ocuchaval" jsem stranky souteze kazdych 10 min a pri zmene mi to poslalo SMS takze jsem vedel o zverejneni uloh jiz kolem 19:20. Co se tyce uloh jak mnozstvi , tak obtiznosti myslim, ze soucasny stav je super. Ja jsem se take tesil na predani cen , ale delat celou noc jsem nezvladl (musel jsem druhy den do prace) ….

Josef Mika
Na oplatku posilam tento odkaz. Je to super aplikace ale mozna o ni uz vite :-)
http://cisse.info/CISSE%20J/2002/spill.pdf

Stanislaw Schmulinsky
… tak to zase nebylo na bednu. Tedy myslím bednu jako stupně vítězů, ne bednu jako makovici, na tu to třetí kolo bylo až až. Na takové sprinty už jsem asi starý, ale i tak jsem si to užil.
…. a těším na příští rok na další soutěž ;-).

MIRKA KEMEN OVAXX
…dakujem za peknu sutaz. Najviac sa mi pacili asi ulohy druheho kola, pri rieseni niektorych som si vytvorila vlastne programy, na substitucne sifry som vyuzila program jedneho kamarata. Ulohy tretieho kola sa mi zdali lahsie. Dufala som, ze budu zverejnene neskor, takto som si kvoli pracovnym povinnostiam neuzila pravu sutazivu atmosferu :) V tomto kole mi zas pomohol kamarat Google, nasla som programy, ktore si poradili so vsetkymi siframi, okrem dvojitej transpozicnej..
Program, co bol pre mna pri rieseni vcelku uzitocny sa vola Cryptool, stiahnutelny z: http://www.cryptool.org/
Vitazov - Pierra a Misofa osobne poznam, su obaja z mojej fakulty, Pierre ma vlastne upozornil na tuto sutaz, a v stredu po zverejneni tretieho kola som s pobavenim sledovala, ako sa na jeho vkus nezvycajne skoro rano objavil Online. Z toho som vlastne usudila, ze asi boli zverejnene dalsie ulohy. ;)

F. O čem jsme psali v prosinci 1999 – 2004

Crypto-World 12/1999

Crypto-World 12/2000

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.

Crypto-World Vánoce/2000

Crypto-World 12/2001

Příloha: uloha7.wav

Crypto-World 12/2002

Příloha : EAL4.jpg
(certifikát operačního systému W2k podle CC na EAL4)

Crypto-World 12/2003

Příloha: pf_2004.jpg

Crypto-World 12/2004

Příloha : PF2005.jpg

G. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem 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@pvt.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/