Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 9, číslo 12/2007 **15. prosinec 2007**

12/2007

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1232 registrovaných odběratelů)

Obsah :

Příloha: program na šifrování a dešifrování homofonních substitucí a nomenklátorů - nomenklator.exe (autor. J.Míka)

A. Soutěž v luštění 2007 – řešení úloh I. kola

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

Příklad: I/1

lehká úloha pátera Stansela pro zlobivé studenty

Systém: transpozice
Upřesnění: jednotlivá slova otevřeného textu psaná pozpátku

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Kdo?
Správná odpověď: BUH
Body: 1

Otevřený text:
Bůh učinil oblohu a oddělil vody pod oblohou od vod nad oblohou - a stalo se. Bůh nazval oblohu ‚nebe' a byl večer a bylo jitro, druhý den. Bůh řekl: "Ať se vody pod nebem shromáždí na jedno místo a ať se ukáže souš!" - a stalo se.

Zdroj otevřeného textu: http://www.nbk.cz/index2.html

Převod na mezinárodní abecedu:
BUH UCINIL OBLOHU A ODDELIL VODY POD OBLOHOU OD VOD NAD OBLOHOU A STALO SE BUH NAZVAL OBLOHU NEBE A BYL VECER A BYLO JITRO DRUHY DEN BUH REKL AT SE VODY POD NEBEM SHROMAZDI NA JEDNO MISTO A AT SE UKAZE SOUS A STALO SE

Šifrový text:
HUB LINICU UHOLBO A LILEDDO YDOV DOP UOHOLBO DO DOV DAN UOHOLBO A OLATS ES HUB LAVZAN UHOLBO EBEN A LYB RECEV A OLYB ORTIJ YHURD NED HUB LKER TA ES YDOV DOP MEBEN IDZAMORHS AN ONDEJ OTSIM A TA ES EZAKU SUOS A OLATS ES

Poznámky k luštění (markanty, nápovědy apod.) : ---------
Jedná se o velmi jednoduchou, testovací úlohu, kdy si řešitel má ozkoušet, že pochopil způsob zadávání správné odpovědi přes www rozhraní.

Příklad: I/2

těžší úloha patera Stansela pro zlobivé studenty

Systém: jednoduchá záměna
Upřesnění: Caesarova šifra

```
Caesarova převodová tabulka (posun o 3 znaky):
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:  D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Odkud ?
Správná odpověď: ALESIE
Body: 2

Otevřený text:

Vzhledem k vysokým ztrátám způsobeným římským obléháním a nedostatkem potravin, radil Vercingetorix svým vojákům, aby ho živého nebo mrtvého vydali vítězům a zajistili si tak lepší podmínky pro vyjednávání o kapitulaci. Podle legendy se Vercingetorix vzdal velkolepým způsobem. Údajně vyjel na koni z Alesie a objel římský tábor předtím, než složil zbraně k Caesarovým nohám. Přitom se měl svléknout a v kleče mávat na Caesara. Caesar ve svých Zápiscích o válce galské však v rozporu s touto legendou popisuje samotný akt Vercingetorikovy kapitulace mnohem střídměji.

Zdroj otevřeného textu: http://cs.wikipedia.org/wiki/Vercingetorix

Převod na mezinárodní abecedu:

```
VZHLEDEM K VYSOKYM ZTRATAM ZPUSOBENYM RIMSKYM OBLEHANIM A NEDOSTATKEM
POTRAVIN RADIL VERCINGETORIX SVYM VOJAKUM ABY HO ZIVEHO NEBO MRTVEHO VYDALI
VITEZUM A ZAJISTILI SI TAK LEPSI PODMINKY PRO VYJEDNAVANI O KAPITULACI
PODLE LEGENDY SE VERCINGETORIX VZDAL VELKOLEPYM ZPUSOBEM UDAJNE VYJEL NA
KONI Z ALESIE A OBJEL RIMSKY TABOR PREDTIM NEZ SLOZIL ZBRANE K CAESAROVYM
NOHAM PRITOM SE MEL SVLEKNOUT A VKLECE MAVAT NA CAESARA CAESAR VE SVYCH
ZAPISCICH O VALCE GALSKE VSAK V ROZPORU S TOUTO LEGENDOU POPISUJE SAMOTNY
AKT VERCINGETORIKOVY KAPITULACE MNOHEM STRIDMEJI
```

Šifrový text:

```
YCKOHGHP N YBVRNBP CWUDWDP CSXVREHQBP ULPVNBP REOHKDQLP D QHGRVWDWNHP
SRWUDYLQ UDGLO YHUFLQJHWRULA VYBP YRMDNXP DEB KR CLYHKR QHER PUWYHKR YBGDOL
YLWHCXP D CDMLVWLOL VL WDN OHSVL SRGPLQNB SUR YBMHGQDYDQL R NDSLWXODFL
SRGOH OHJHQGB VH YHUFLQJHWRULA YCGDO YHONROHSBP CSXVREHP XGDMQH YBMHO QD
NRQL C DOHVLH D REMHO ULPVNB WDERU SUHGWLP QHC VORCLO CEUDQH N FDHVDURYBP
QRKDP SULWRP VH PHO VYOHNQRXW D YNOHFH PDYDW QD FDHVDUD FDHVDU YH VYBFK
CDSLVFLFK R YDOFH JDOVNH YVDN Y URCSRUX V WRXWR OHJHQGRX SRSLVXMH VDPRWQB
DNW YHUFLQJHWRULNRYB NDSLWXODFH PQRKHP VWULGPHML
```

Rozpis na pětice:

```
YCKOH GHPNY BVRNB PCWUD WDPCS XVREH QBPUL PVNBP REOHK DQLPD QHGRV WDWNH
PSRWU DYLQU DGLOY HUFLQ JHWRU LAVYB PYRMD NXPDE BKRCL YHKRQ HERPU WYHKR
YBGDO LYLWH CXPDC DMLVW LOLVL WDNOH SVLSR GPLQN BSURY BMHGQ DYDQL RNDSL
WXODF LSRGO HOHJH QGBVH YHUFL QJHWR ULAYC GDOYH ONROH SBPCS XVREH PXGDM
QHYBM HOQDN RQLCD OHVLH DREMH OULPV NBWDE RUSUH GWLPQ HCVOR CLOCE UDQHN
FDHVD URYBP QRKDP SULWR PVHPH OVYOH NQRXW DYNOH FHPDY DWQDF DHVDU DFDHV
DUYHV YBFKC DSLVF LFKRY DOFHJ DOVNH YVDNY URCSR UXVWR XWROH JHQGR XSRSL
VXMHV DPRWQ BDNWY HUFLQ JHWRU LNRYB NDSLW XODFH PQRKH PVWUL GPHML
```

Poznámky k luštění (markanty, nápovědy apod.):
Luštitel byl upozorněn, že se jedná o klasickou šifru …
V jedné z nápověd přímo citována Caesarova a Augustova šifra…

Příklad: I/3

úloha patera Stansela sloužící k vysvětlení jednoho z klasických systémů

Systém: jednoduchá záměna
Upřesnění: Augustova šifra
Augustova převodová tabulka (posun o jeden znak)

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

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Kdo (4)?
Správná odpověď: DEUS
Body: 2

Otevřený text (v latině):
1. in principio creavit Deus caelum et terram
2. terra autem erat inanis et vacua et tenebrae super faciem abyssi et spiritus Dei ferebatur super aquas
3. dixitque Deus fiat lux et facta est lux
4. et vidit Deus lucem quod esset bona et divisit lucem ac tenebras
5. appellavitque lucem diem et tenebras noctem factumque est vespere et mane dies unus

Zdroj otevřeného textu: http://www.fourmilab.ch/etexts/www/Vulgate/Genesis.html

Převod na mezinárodní abecedu:
```
IN PRINCIPIO CREAVIT DEUS CAELUM ET TERRAM
TERRA AUTEM ERAT INANIS ET VACUA ET TENEBRAE SUPER FACIEM ABYSSI ET
SPIRITUS DEI FEREBATUR SUPER AQUAS
DIXITQUE DEUS FIAT LUX ET FACTA EST LUX
ET VIDIT DEUS LUCEM QUOD ESSET BONA ET DIVISIT LUCEM AC TENEBRAS
APPELLAVITQUE LUCEM DIEM ET TENEBRAS NOCTEM FACTUMQUE EST VESPERE
ET MANE DIES UNUS
```

Šifrový text:
```
JO QSJODJQJP DSFBWJU EFVT DBFMVN FU UFSSBN
UFSSB BVUFN FSBU JOBOJT FU WBDVB FU UFOFCSBF TVQFS GBDJFN BCZTTJ FU
TQJSJUVT EFJ GFSFCBUVS TVQFS BRVBT
EJYJURVF EFVT GJBU MVY FU GBDUB FTU MVY
FU WJEJU EFVT MVDFN RVPE FTTFU CPOB FU EJWJTJU MVDFN BD UFOFCSBT
BQQFMMBWJURVF MVDFN EJFN FU UFOFCSBT OPDUFN GBDUVNRVF FTU WFTQFSF FU NBOF
EJFT VOVT
```

Rozpis na pětice:
```
JOQSJ ODJQJ PDSFB WJUEF VTDBF MVNFU UFSSB NUFSS BBVUF NFSBU JOBOJ TFUWB
DVBFU UFOFC SBFTV QFSGB DJFNB CZTTJ FUTQJ SJUVT EFJGF SFCBU VSTVQ FSBRV
BTEJY JURVF EFVTG JBUMV YFUGB DUBFT UMVYF UWJEJ UEFVT MVDFN RVPEF TTFUC
POBFU EJWJT JUMVD FNBDU FOFCS BTBQQ FMMBW JURVF MVDFN EJFNF UUFOF CSBTO
PDUFN GBDUV NRVFF TUWFT QFSFF UNBOF EJFTV OVT
```

Poznámky k luštění (markanty, nápovědy apod.):
Luštitel byl v nápovědě upozorněn, že se jedná o klasickou šifru. Dodatečně byla zveřejněna informace, že jazyk otevřeného textu je latina …
V jedné z nápověd přímo citována Caesarova a Augustova šifra…

Příklad: I/4
šifrový text od Štěpána Schmidta pro přítele Josefa Steplinga

Systém: transpozice
Upřesnění: sloupcová transpozice, 7 sloupců,
transpoziční abecední heslo: SCHMIDT

heslo po vyčíslení: 6-1-3-5-4-2-7
délka otevřeného textu: 789 znaků
rozměr tabulky: 791=7*113
na úplnou tabulku doplněn otevřený text o 2 znaky X

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Než kdo?
Správná odpověď: MEDUSA
Body: 2

Otevřený text:
Ty však, kdokoli hledíš si trvale udržet dívku,
ponech jí domněnku tu, její žes krásou byl jat.
Bude-li oděna v nachu, ty pochvalíš nachová roucha,
bude-li v hedvábí kójském, hedváb že sluší jí, věř!
Bude-li zdobena zlatem, nechť zlato cennější je ti,
jestliže oblékne vlnu, i tuto vlnu jí chval;
v tunice před tebou stane: “Já od tebe shořím!” hned volej,
ale ať chladna se chrání, úzkostným hlasem jí pros!
Má-li snad pěšinku vábnou, chval pěšinku v účesu jejím;
ohněm si kadeří vlasy? Kadeř tu v oblibě měj!
Obdivuj paže, když tančí, a nad hlasem žasni, když zpívá;
potom, že skončila již, zármutek slovy jí sděl.
Velebit bude ti možno i náruč i blaženou rozkoš,
všeliké radosti noční za to pak odměnou měj;
i kdyby krutější byla než bývala Medúsa hrozná,
bude se k milenci svému vlídně a něžně pak mít.
Jenom se prozradit nesmíš, že přetvářka byla v těch slovech,
dbej, ať výraz tvé tváře nezboří to, co jsi řek.
Prospívá tajený úskok, však poznaný přináší hanbu,
a pak odejme právem důvěru pro všechen čas.

Zdroj otevřeného textu:
Ukázka : Pochlebování, Publius Ovidius Naso, Umění milovati
http://psaci.misto.cz/_MAIL_/texty/naso/pochlebovani.html

Převod na mezinárodní abecedu:
TY VSAK KDOKOLI HLEDIS SI TRVALE UDRZET DIVKU PONECH JI DOMNENKU TU JEJI ZES KRASOU BYL JAT BUDE LI ODENA V NACHU TY POCHVALIS NACHOVA ROUCHA BUDE LI V HEDVABI KOJSKEM HEDVAB ZE SLUSI JI VER BUDE LI ZDOBENA ZLATEM NECHT ZLATO CENNEJSI JE TI JESTLIZE OBLEKNE VLNU I TUTO VLNU JI CHVAL V TUNICE PRED TEBOU STANE JA OD TEBE SHORIM HNED VOLEJ ALE AT CHLADNA SE CHRANI UZKOSTNYM HLASEM JI PROS MA LI SNAD PESINKU VABNOU CHVAL PESINKU V UCESU JEJIM OHNEM SI KADERI VLASY KADER TU V OBLIBE MEJ OBDIVUJ PAZE KDYZ TANCI A NAD HLASEM ZASNI KDYZ ZPIVA POTOM ZE SKONCILA JIZ ZARMUTEK SLOVY JI SDEL VELEBIT BUDE TI MOZNO I NARUC I BLAZENOU ROZKOS VSELIKE RADOSTI NOCNI ZA TO PAK ODMENOU MEJ I KDYBY KRUTEJSI BYLA NEZ BYVALA MEDUSA HROZNA BUDE SE K MILENCI SVEMU VLIDNE A NEZNE PAK MIT JENOM SE PROZRADIT NESMIS ZE PRETVARKA BYLA V TECH SLOVECH DBEJ AT VYRAZ TVE TVARE NEZBORI TO CO JSI REK PROSPIVA TAJENY USKOK VSAK POZNANY PRINASI HANBU A PAK ODEJME PRAVEM DUVERU PRO VSECHEN CAS

Šifrový text:
YOERR KHEER LEATA HCLAK ASBDL COSEO VTITR UASNJ HEUYM MDUCS CISIA OEUDI
ANPON ZEJEU ZUEKI SIKUY EAASA KILEM MRSRA EEATE IISJO ORAKP UONKI SEDNO
TEUBD CCNRU EOESV LNMLN TIKIN ACENE IOANA SARSI NLUJN DSTBD ZADZY PSAMO
EIINL RSAOO EIRBB EOEEM EPERT ZAALB RVBOP AUANS AJEUC XVKDV ZUJNJ AJLVY
LOHIB EBIUO AHCIS BLOCU ESOHE ALCZM JAPVH IEMIV DBJJY ASIIM CZKIL DNCNO

```
KTZOM BJNLA BMSIZ ISAME BCCTV NTRPE KZINO RVVCA LSLTO DUZOT OAOSA BHKHE
IEEEZ NELEU LVITA TRVED ROLPI SBAKU HAARI BATAM DAELR LDBTI BUVRN TMJKI
ZMRDL ENEJP ISVLS DYTZC KVYSA AUEVR ESSOI AEPIK ISAIN PIVAV IMZJD BTTEJ
TLNVH NDTDO DLAHK HILEA VNSOK LELOP ZNEKV ZIASS EEOIO SEIAD EYSEA HUIVD
NTEDI TYHHV EEOEI NVNNB DAESA TDLTD VCNJK YDNUV CUEVS VURZZ ETJJE EUJVP
OJEHE CSINE SAKUE UJMRK VMVKC LSZTO ITYVB ORZZL ONAOD TLVUN ECVNK OZEPK
TVJZR RSOAK PPHAE DREKH IUIEM USBUE HHAOD DJDLE IANAE IZNTU LEBEB MLTAN
TSONN OPVEE EYUEI ENHAZ OKJUV LTMAA OEDCP NKUYY DZSNU AANON ERVOE AAOJR
TSKYI PMMPH X
```

Poznámky k luštění (markanty, nápovědy apod.) :
Statistický charakter otevřeného textu byl zachován, uživatel mohl předpokládat, že jde o transpozici, rozměr transpozičný tabulky volen tak, aby byl jednoznačný, jako padding (doplněk na celou tabulku) použita „klasická“ písmena X, která mohou popmoci při určení pozice sloupců, počet sloupců pouze 7

Příklad: I/5

Steplingův zašifrovaný text pro Štěpána Schmidta

Systém: jednoduchá záměna
Upřesnění: převodová tabulka vytvořena podle hesla NOSTRADAMUS

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

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Kdo?
Správná odpověď: NOSTRADAMUS
Body: 3

Otevřený text:

```
Nostradamova metoda
Pracoval v noci. V pracovně měl trojnožku vytvořenou podle vzoru svých
starořeckých předchůdkyň z Delf. Do stavu vytržení mu snad pomáhalo užívání
muškátového ořechu, to má být ve větším množství mírný halucinogen. Na
trojnožce visela mosazná nádoba naplněná vřící vodou a vonnými oleji.
Nostradamus sledoval odlesky ohně v její hladině. Předpisově seděl před
trojnožkou se vzpřímenou páteří. Prorocké schopnosti dle vlastního
vyjádření považoval jednak za vliv “nadpřirozeného světla“, které umožňuje
pochopit božské záměry z hvězd, zároveň za dar, jímž Bůh prorokovi umožňuje
účast na vlastním božství a také za projev intuice.
Nostradamovu slávu založilo následující proroctví:
Mladý lev přemůže lva staršího
na bitevním poli v jediné srážce
přes zlatou klec mu probodne oči
ze dvou ran jedna bude, poté zhyne krutou smrtí.
```

Zdroj otevřeného textu: http://psaci.misto.cz/_MAIL_/texty/koukolik/nostradamus.html

Převod na mezinárodní abecedu:

```
NOSTRADAMOVA METODA PRACOVAL V NOCI V PRACOVNE MEL TROJNOZKU VYTVORENOU
PODLE VZORU SVYCH STARORECKYCH PREDCHUDKYN Z DELF DO STAVU VYTRZENI MU SNAD
POMAHALO UZIVANI MUSKATOVEHO ORECHU TO MA BYT VE VETSIM MNOZSTVI MIRNY
HALUCINOGEN NA TROJNOZCE VISELA MOSAZNA NADOBA NAPLNENA VRICI VODOU A
VONNYMI OLEJI NOSTRADAMUS SLEDOVAL ODLESKY OHNE V JEJI HLADINE PREDPISOVE
SEDEL PRED TROJNOZKOU SE VZPRIMENOU PATERI PROROCKE SCHOPNOSTI DLE
VLASTNIHO VYJADRENI POVAZOVAL JEDNAK ZA VLIV NADPRIROZENEHO SVETLA KTERÉ
```

```
UMOZNUJE POCHOPIT BOZSKE ZAMERY Z HVEZD ZAROVEN ZA DAR JIMZ BUH PROROKOVI
UMOZNUJE UCAST NA VLASTNIM BOZSTVI A TAKE ZA PROJEV INTUICE NOSTRADAMOVU
SLAVU ZALOZILO NASLEDUJICI PROROCTVI MLADY LEV PREMUZE LVA STARSIHO NA
BITEVNIM POLI V JEDINE SRAZCE PRES ZLATOU KLEC MU PROBODNE OCI ZE DVOU RAN
JEDNA BUDE POTE ZHYNE KRUTOU SMRTI
```

Šifrový text:

```
GHLPK NTNFH VNFRP HTNIK NSHVN EVGHS UVIKN SHVGR FREPK HBGHZ CQVYP VHKRG
HQIHT ERVZH KQLVY SMLPN KHKRS CYSMI KRTSM QTCYG ZTREA THLPN VQVYP KZRGU
FQLGN TIHFN MNEHQ ZUVNG UFQLC NPHVR MHHKR SMQPH FNOYP VRVRP LUFFG HZLPV
UFUKG YMNEQ SUGHD RGGNP KHBGH ZSRVU LRENF HLNZG NGNTH ONGNI EGRGN VKUSU
VHTHQ NVHGG YFUHE RBUGH LPKNT NFQLL ERTHV NEHTE RLCYH MGRVB RBUME NTUGR
IKRTI ULHVR LRTRE IKRTP KHBGH ZCHQL RVZIK UFRGH QINPR KUIKH KHSCR LSMHI
GHLPU TERVE NLPGU MHVYB NTKRG UIHVN ZHVNE BRTGN CZNVE UVGNT IKUKH ZRGRM
HLVRP ENCPR KRQFH ZGQBR IHSMH IUPOH ZLCRZ NFRKY ZMVRZ TZNKH VRGZN TNKBU
FZOQM IKHKH CHVUQ FHZGQ BRQSN LPGNV ENLPG UFOHZ LPVUN PNCRZ NIKHB RVUGP
QUSRG HLPKN TNFHV QLENV QZNEH ZUEHG NLERT QBUSU IKHKH SPVUF ENTYE RVIKR
FQZRE VNLPN KLUMH GNOUP RVGUF IHEUV BRTUG RLKNZ SRIKR LZENP HQCER SFQIK
HOHTG RHSUZ RTVHQ KNGBR TGNOQ TRIHP RZMYG RCKQP HQLFK PU
```

Poznámky k luštění (markanty, nápovědy apod.):
Dostatečně dlouhý text, frekvenční statistiky pro češtinu vycházejí.

Dodatečně zveřejněna nápověda odhalující jednu samohlásku a několik méně četných znaků z konce převodové tabulky : A=N, ..., U=Q, V=V, W=W, X=X, Y=Y, Z=Z

Příklad: I/6
vlastní Schmidtova transpozice

Systém: transpozice
Upřesnění: otevřený text se rozdělí na skupiny po 6-ti znacích a šifrový text se získá vypsáním těchto znaků v pořadí dle numerického hesla: 631542
příklad: `MAM PRA` se zašifruje jako: `MAARP M`
Text doplněn tak, aby byl počet znaků dělitelný šesti a to pomocí X.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: O čem?
Správná odpověď: PRATELSTVI
Body: 3

Otevřený text:

```
Mám přátele! - musím si říct s údivem. A se stejným údivem - čím jsem si je
zasloužil? Snad proto, že sobě dobře činí, kdo činí dobře svým přátelům.
Přátelství činí naše štěstí zářivějším, zvyšuje jeho třpyt, neštěstí pak
činí snesitelnějším, poněvadž je sdílí a snáší s námi společně. Tvuj přítel
Štěpán.
```

Zdroj otevřeného textu:
upraveny a spojeny dva citáty o přátelství

Převod na mezinárodní abecedu:

```
MAM PRATELE MUSIM SI RICT S UDIVEM A SE STEJNYM UDIVEM CIM JSEM SI JE
ZASLOUZIL SNAD PROTO ZE  SOBE DOBRE CINI KDO CINI DOBRE  SVYM  PRATELUM
```

```
PRATELSTVI CINI NASE STESTI ZARIVEJSIM ZVYSUJE JEHO TRPYT NESTESTI PAK CINI
SNESITELNEJSIM PONEVADZ JE SDILI A SNASI S NAMI SPOLECNE TVUJ PRITEL STEPAN
```

Šifrový text:

```
MAARP MLUEM ETMRI ISSTD CUSIE SVAMI TNSJE EUVMI DYCJM MIEMJ EISSA OZLSE
INZSL UPTDO RAEBZ OSOOE DRBEN DIKIC IDCIN ORVBS EOPTM ARYUR LPMEE TTSLA
CIINI VSTAS ENTAS ZIEVS IJERZ SMYVI EHJEJ URTTY POSSE ETNPC IKATI ENNSI
TNILE SSPJM IEEDN AVOEI JDSZA AINSL SMIAN SPESL OIEUN VTCRE PTIJT ASPEL
XXXXX N
```

Poznámky k luštění (markanty, nápovědy apod.):
Luštitel byl postupně v nápovědách upozorněn, že se jedná o transpozici opakující se konstantní délky a později o tom, že se používá délka 6.
Také upozorněn, že obdobná šifra byla použita v úloze I/8. Pokud prolomil tuto lehčí šifru (délka hesla v této úloze pouze 4), pak mohl pochopit princip a vrátit se k řešení této úlohy.

Pro luštění bez nápovědy lze využít toho, že lustitel v šifrovém textu „uvidí“ zpřeházené slovo otevřeného textu a tím si může odvodit pravidlo pto transpozici konkrétní skupoiny, dále lze využít také závěrečné doplnění pomocí X (odhad délky transpozice a pravděpodobné „umístění“ jednoho znaku skupiny v otevřeném textu) ...

Příklad: I/7
Steplingova úloha pro Štěpána Schmidta

Systém: substituční záměna
Upřesnění: posun písmen postupně o,….
Příklad :
Zašifrováno jako :

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (6)
Správná odpověď: PITI
Body: 3

Otevřený text:

```
Pořád se mluví o nemístném pití, ale nikdy o veliké žízni. Milý Štěpáne,
víš že Staré víno je dobré jen proto, že je staré? Kdyby bylo bývalo dobré
samo o sobě, nikdo by je byl nenechal zestárnout.
```

Zdroj otevřeného textu:
upraveny a spojeny dva citáty o víně a pití

Převod na mezinárodní abecedu:

```
PORAD SE MLUVI O NEMISTNEM PITI ALE NIKDY O VELIKE ZIZNI MILY STEPANE VIS
ZE STARE VINO JE DOBRE JEN PROTO ZE JE STARE KDYBY BYLO BYVALO DOBRE SAMO O
SOBE NIKDO BY JE BYL NENECHAL ZESTARNOUT
```

Šifrový text:

```
PNPXZ NY FDLLX C AQXSBBUKR TLVJ AKC KEFXR G MUAWXQ KSIVP SNPB UUEOYKA QCL
RV IIOEQ GSWW QK ISETF JDL MNJNH RV ZT GGMCO TLFHD FBNP BXTXHJ XHTIU HOZA Z
CXJL TNOGQ CY IC YUG HXFVSWOY LPCCIYTTYW
```

Poznámky k luštění (markanty, nápovědy apod.):
v dodatečné nápovědě luštitel seznámen, že se jedná o a šifru, která je založena na "posuvné" záměně jednotlivých písmen

---

Příklad: I/8
Schmidtův dopis Klementině

Systém: transpozice
Upřesnění: vlastní Schmidtova transpozice
Systém již jednou použit a to v úloze I/6 (zde použita jiná délka dělby a jiné heslo).
Otevřený text se rozdělí na skupiny po 4 znacích a šifrový text se získá vypsáním těchto znaků v pořadí dle numerického hesla: 3142
příklad: `JSEM` se zašifruje jako: `SMJE`
Text doplněn tak, aby byl počet znaků dělitelný čtyřmi a to pomocí X.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Kdo jsem?
Správná odpověď: STUDENT
Body: 1

Otevřený text:
```
Jsem student, student láskou hořící
a ne básník, básně tvořící
a přesto jsem se pera chopil
a báseň o ni začal psát,
nepochopili byste, musíte ji znát.

Je krásná milá,
Oči její přímo hladí,
však to znáte,
byli jste přec také mladí.
```

Zdroj otevřeného textu: napsáno pro soutěž

Převod na mezinárodní abecedu:
```
JSEM STUDENT STUDENT LASKOU HORICI A NE BASNIK BASNE TVORICI A PRESTO JSEM
SE PERA CHOPIL A BASEN O NI ZACAL PSAT NEPOCHOPILI BYSTE MUSITE JI ZNAT JE
KRASNA MILA OCI JEJI PRIMO HLADI VSAK TO ZNATE BYLI JSTE PREC TAKE MLADI
```

Šifrový text:
```
SMJET DSUNS ETUET DTANL KUSOO IHRIN CABSE AIBNK SEANV RTOCA IIRSP EOSTJ
MEESE APRHP COLBI ASNAE NZOIC LAAST PAEON PHPCO LBIIS EYTUI MSEIT JNTZA
ERJKS AANIA MLCJO IJPEI IORML DHAVA ISTZK OAENT YIBLS EJTRC PEAET KLDMA
XXIX
```

Poznámky k luštění (markanty, nápovědy apod.):
Luštitel byl postupně v nápovědách upozorněn, že se jedná o transpozici obdobnou šifře I/6 a o tom, že se využívá klíč délky 4.
Pro luštění bez nápovědy lze využít toho, že lustitel v šifrovém textu „uvidí“ zpřeházené slovo otevřeného textu a odvodí si systém na jeho tvorbu a dále nevhodného doplnění závěru textu pomocí X (tím lze získat odhad délky transpozice a „umístění“ jednoho ze znaků skupiny).

Příklad: I/9

Klementin dopis

Systém: jednoduchá záměna
Upřesnění:
převodová tabulka vytvořena podle hesla SRDCE MÉ JE I TVÉ
(bez opakování hlásek: S R D C E M J I T V)
Výsledná 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: S R D C E M J I T V A B F G H K L N O P Q U W X Y Z
```

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Co opakuji?
Správná odpověď: JOSEF
Body: 2

Otevřený text:

```
Můj milovaný,
nikdy nezapomenu velebit tvého přítele Štěpána, že mne naučil hrát si se
slovy. Ale tobě jsem mnohem vděčnější, protože jsi mne naučil hrám
neskonale krásnějším. Každý den, kdy se máme setkat, nemohu dospat a má
ústa neslyšně opakují: „Josef... Josef Stepling.“
Navždy tvá Klementina
```

Převod na mezinárodní abecedu:

```
MUJ MILOVANY NIKDY NEZAPOMENU VELEBIT TVEHO PRITELE STEPANA ZE MNE NAUCIL
HRAT SI SE SLOVY ALE TOBE JSEM MNOHEM VDECNEJSI PROTOZE JSI MNE NAUCIL HRAM
NESKONALE KRASNEJSIM KAZDY DEN KDY SE MAME SETKAT NEMOHU DOSPAT A MA USTA
NESLYSNE OPAKUJI JOSEF JOSEF STEPLING NAVZDY TVA KLEMENTINA
```

Šifrový text:

```
FQVFT BHUSG YGTAC YGEZS KHFEG QUEBE RTPPU EIHKN TPEBE OPEKS GSZEF GEGSQ
DTBIN SPOTO EOBHU YSBEP HREVO EFFGH IEFUC EDGEV OTKNH PHZEV OTFGE GSQDT
BINSF GEOAH GSBEA NSOGE VOTFA SZCYC EGACY OEFSF EOEPA SPGEF HIQCH OKSPS
FSQOP SGEOB YOGEH KSAQV TVHOE MVHOE MOPEK BTGJG SUZCY PUSAB EFEGP TGS
```

Poznámky k luštění (markanty, nápovědy apod.):
Šifrový text je kratší, ale statistiky poměrně slušně vycházejí. Luštitel může s výhodou využít uhodnutí některého ze slov otevřeného textu (KLEMENTINA, MILOVANY, JOSEF STEPLING, apod.).
Pro ty, kteří si nedovedli s úlohou poradit, byla zveřejněna nápověda, že v převodové tabulce lze nalézt „SRDCE“.

B. Soutěž v luštění 2007 – řešení úloh II. kola

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

Příklad: II/1

Steplingův tajemný text

Systém: typ jednoduché záměny
Upřesnění: jedná se o záměnu samohlásek za jiná písmena, tato písmena se však mohou vyskytovat i v otevřeném textu, a proto při dešifraci mohou být drobné problémy s nejednoznačností ….
Použitá převodová tabulka:

A	E	I	O	U	Y
B	D	P	G	Q	C

Systém byl skutečně používán a to ve Vatikánu kolem roku 1332. Převodová tabulka je autentická.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Odkud?
Správná odpověď: LOYOLY
Body: 1

Otevřený text:
Každý, kdo chce hovořit s Bohem, nemůže bezstarostně klábosit s jinými lidmi. Neboť Boží tajemství nejsou určená uším všech. Jen zasvěcení mohou prožívat radost z vědění nejvyššího. Jsi na křižovatce. Pokud chceš být zasvěceným, staneš se poustevníkem vědění. Jestliže jsi k tomu připravený, navštiv kapli a hledej u obrazu svatého Ignáce z Loyoly.

Převod na mezinárodní abecedu:
KAZDY KDO CHCE HOVORIT S BOHEM NEMUZE BEZSTAROSTNE KLABOSIT S JINYMI LIDMI NEBOT BOZI TAJEMSTVI NEJSOU URCENA USIM VSECH JEN ZASVECENI MOHOU PROZIVAT RADOST Z VEDENI NEJVYSSIHO JSI NA KRIZOVATCE POKUD CHCES BYT ZASVECENYM STANES SE POUSTEVNIKEM VEDENI JESTLIZE JSI K TOMU PRIPRAVENY NAVSTIV KAPLI A HLEDEJ U OBRAZU SVATEHO IGNACE Z LOYOLY

Šifrový text:
KBZDC KDG CHCD HGVGRPT S BGHDM NDMQZD BDZSTBRGSTND KLBBGSPT S JPNCMP LPDMP NDBGT BGZP TBJDMSTVP NDJSGQ QRCDNB QSPM VSDCH JDN ZBSVDCDNP MGHGQ PRGZPVBT RBDGST Z VDDDNP NDJVCSSPHG JSP NB KRPZGVBTCD PGKQD CHCDS BCT ZBSVDCDNCM STBNDS SD PGQSTDVNPKDM VDDDNP JDSTLPZD JSP K TGMQ PRPPRBVDNC NBVSTPV KBPLP B HLDDDJ Q GBRBZQ SVBTDHG PGNBCD Z LGCGLC

Poznámky k luštění (markanty, nápovědy apod.):
Vzhledem k ponechané dělbě na slova se jedná o velmi jednoduchou úlohu, kterou lze řešit bez velkých problémů.

Příklad: II/2
text ze starého foliantu

Systém: polyalfabetická substituce, Beaufortova šifra

Upřesnění: použito periodické heslo MATOUS (délka 6).
Způsob skládání hesla a otevřeného textu Beaufort :

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (4)
Správná odpověď: ZKOUSKU
Body: 3

Otevřený text:
```
Až složíš závěrečnou zkoušku, požádej Pátera Stansela, aby tě poslal
k lidem, kteří tvé umění ocení. Už si s tím poradí. A hodně zdaru, ať
zkoušku složíš na výbornou. BIK
```

Převod na mezinárodní abecedu:
```
AZ SLOZIS ZAVERECNOU ZKOUSKU POZADEJ PATERA STANSELA ABY TE POSLAL K LIDEM
KTERI TVE UMENI OCENI UZ SI S TIM PORADI A HODNE ZDARU AT ZKOUSKU SLOZIS NA
VYBORNOU BIK
```

Šifrový text:
```
MBBDG TEIUO ZOVWR BGYNQ FUCIS LFPUP IREOB OVABV UFUWI OUROH PZGAB AIEJK
JWHEB OVSAT QYAWG GGQIN LUVAE IAGID YJTLM SFMQB QTJAC UUZNQ FUCIS IIAVK
UNTTW RYJGA AREQ
```

Poznámky k luštění (markanty, nápovědy apod.):
Z textu se dalo odhadnout, že je použit podpis BIK. I při délce tohoto textu perioda vychází.
V nápovědě byl pak systém upřesněn (Beaufort) a to včetně délky periodického klíče (6).

Příklad: II/3
zašifrovaný text z císařské kanceláře

Systém: homofonní substituce
Upřesnění:
Převodová tabulka je tvořena jednoduchou záměnu doplněnou o homofony pro četná písmena a to konkrétně pro samohlásky A,E,I,O a dvě četné souhlásky S,T.
Použité heslo pro sestavení tabulky jednoduché záměny bylo: MARS A VENUSE

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

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Hrabě?
Správná odpověď: MORGESTERN
Body: 5

Otevřený text:
Udělejte všechno, aby jeho milost saský kurfiřt uznal nástupnické právo dcery našeho císaře Marie Terezie. Naznačte, že císař je za to ochotný uznat vše, co mu přednesl saský vyslanec hrabě Morgestern. Můžete naznačit, že jste do věci zcela zasvěcen. V této věci neštřte časem ani penězi. Vše důležité mi dejte ihned vědět. Spoléhám na Vás. BIK.

Převod na mezinárodní abecedu:
UDELEJTE VSECHNO ABY JEHO MILOST SASKY KURFIRT UZNAL NASTUPNICKE PRAVO DCERY NASEHO CISARE MARIE TEREZIE NAZNACTE ZE CISAR JE ZA TO OCHOTNY UZNAT VSE CO MU PREDNESL SASKY VYSLANEC HRABE MORGESTERN MUZETE NAZNACIT ZE JSTE DO VECI ZCELA ZASVECEN V TETO VECI NESTRTE CASEM ANI PENEZI VSE DULEZITE MI DEJTE IHNED VEDET SPOLEHAM NA VAS BIK

Šifrový text:
KS*Y* P1VLI 4RUCD MAWPV U3BZY 3IJ5M 5QWQK HE2HJ KXC-Y C-I1K FCZRQ VFHML
DSR*H WCM5* UDRZI -H4BM H2VJV H*X24 CMXCM RJVX* RZI-H PVX-1 D3RUD JCWKX
CMJLI 4RDBK FHVSC *5YIM IQWLW IYMCV RUH-A 4BDHN V514H CBKXV JVCMX CMR21
X*PIJ 4S3L4 RZXRV Y-XMI L*RVC LJ4JD L*RZC V51HJ 4RMIV B-C2F VC4X2 LI*SK
Y*XZ1 VBZSV P142U C*SLV SVJ5F 3Y4U- BCMLM 5AZQ

Šifrový text, druhá verze, desátá nápověda:
KS4YV PJ4L5 *RUC3 -AWPV UDBZY D51I- 5QWQK HE2H1 KXC-Y C-IJK FC2RQ VFHML
3SRVH WC-I4 UDR25 -HVB- HZ*J4 HVX2* CMXCM RJ4X* R2IMH PVXM1 33RUD JCWKX
CMJLI *R3BK FHVSC 45Y5M IQWLW IY-C4 RUH-A 4B3HN V5JVH CBKX* J4CMX CMR21
X4P5J 4S3L4 RZXR4 Y-XMI LVR4C L1*13 L*R2C VIJH1 *RM5V B-CZF *C*XZ LIVSK
Y*X21 4B2S4 PJ4ZU C4SLV S415F 3Y*U- BC-L- 5AZQ

Poznámka k luštění (markanty, nápovědy apod.):
Bylo použito jen velmi málo homofonnů. Lze „odhalit“, že číslice a znaky -* jsou homofony a vzhledem k počtu znaků šifrové abecedy lze předpokládat, že jiné homofony zde nebudou… Při luštění pomůže uhádnutí některých předpokládaných slov. Opět je použit podpis BIK, v textu je slovo hrabě, které lze dovodit z nápovědy a dále slova císař, Marie Terezie apod.
V dodatečné napovědě se luštitelé dozvěděli, že jen k šesti písmenou jsou použity homofony a že mezi těmito písmeny jsou čtyři samohlásky a dvě četné souhlásky.

V desáté nápovědě byla zveřejněna další verze šifrového textu. Tím se dá zjistit, které homofony k sobě patří a úlohu převést na luštění jednoduché záměny. V době zvěřejnění této nápovědy mělo již úlohu vyřešeno 13 soutěžících.

Příklad: II/4
dopis baronu Ignázi von Kochovi

Systém: polyalfabetická substituce, varinata Vigenere-Beaufort

Upřesnění: použito periodické heslo SCHMIDT (délka 7).
Způsob skládání hesla a otevřeného textu varianta Vigenere-Beaufort:

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (3)
Správná odpověď: BARONE
Body: 3

Otevřený text:
Urozený pane barone. Pokud jste skutečně tím, za koho vás považuji, určitě jste našel způsob, jak si můj dopis přečíst. Přijal jsem službu písaře, i když jsem v koleji studoval matematiku. Věřím, že vše řídí Pán a nic se neděje bez jeho požehnání. Ale věřím také, že i lidé dávají některým událostem smysl. Dovolím si vás proto požádat, zda byste mi laskavě neobjasnil, jaký smysl dáváte událostem kolem mé osoby vy. V úctě Štěpán Schmidt. Dovouji si psát tímto způsobem neboť i Vas dopis byl takto obdobne zašifrován.

Převod na mezinárodní abecedu:
UROZENY PANE BARONE POKUD JSTE SKUTECNE TIM ZA KOHO VAS POVAZUJI URCITE JSTE NASEL ZPUSOB JAK SI MUJ DOPIS PRECIST PRIJAL JSEM SLUZBU PISARE I KDYZ JSEM V KOLEJI STUDOVAL MATEMATIKU VERIM ZE VSE RIDI PAN A NIC SE NEDEJE BEZ JEHO POZEHNANI ALE VERIM TAKE ZE I LIDE DAVAJI NEKTERYM UDALOSTEM SMYSL DOVOLIM SI VAS PROTO POZADAT ZDA BYSTE MI LASKAVE NEOBJASNIL JAKY SMYSL DAVATE UDALOSTEM KOLEM ME OSOBY VY V UCTE STEPAN SCHMIDT DOVOUJI SI PSAT TIMTO ZPUSOBEM NEBOT I VAS DOPIS BYL TAKTO OBDOBNE ZASIFROVAN

Šifrový text:
CPHNW KFXYG STXYW LXDGH BLHLH WPRCR XQFBA QKSOC LOWTT GHLCI XNXAR YKGMS
BPAML TGWIG XSLCT GHSQB AMGKW NBGHO LKGLH HOPRY EXKBT AJNNT RWQQT FWFRL
WSXKB TDIHZ WGPAR NRGSH TKTHW JHBGD INBYQ KSSNP LZGWW HXUIL BQKBU MBXXW
YLHHX VGMVH CABSK PIJXJ WOPUR TYWWL QJBRW AHDYC WFBRB CKMER KIJHG LBTAK
RGDAV DMEWE PPDYL DJLAW NHNSA HBXWO TVZBC FWDXZ SYOSF BVJHT GFFSR YDMKJ
FAJWO NXAMS WODLZ BCFYG ILUKX CKLIG TRJMZ AMQMS HXUAA AAAAA LMOCM GPAGI
GSQAQ KMCRM BAMUS EKLJM MWNXZ LMIWK YFTRT YLLVJ BHPFB GIQBT JLCIL

Poznámky k luštění (markanty, nápovědy apod.)
Z textu se dalo odhadnout předpokládané slovo STEPAN SCHMIDT .
I při délce tohoto textu perioda vychází.
V nápovědě byl pak systém upřesněn (varianta Vigener-Beaufort) a to včetně délky periodického klíče (7).

Příklad: II/5
odpověď barona Ignáze von Kocha

Systém: polyalfabetická substituce, systém Vigenere
Upřesnění: použito periodické heslo BIK (délka 3).
Způsob skládání hesla a otevřeného textu varianta:

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Mezi?
Správná odpověď: NAMI
Body: 3

Otevřený text:

```
Byt zasvecenym znamena aby byl clovek vzdelany bystry mel stesti a umel
jednat v pravou chvili spravnym zpusobem Vy vazeny priteli jste to dokazal
Vitejte mezi nami BIK
```

Převod na mezinárodní abecedu:

```
BYT ZASVECENYM ZNAMENA ABY BYL CLOVEK VZDELANY BYSTRY MEL STESTI A UMEL
JEDNAT V PRAVOU CHVILI SPRAVNYM ZPUSOBEM VY VAZENY PRITELI JSTE TO DOKAZAL
VITEJTE MEZI NAMI BIK
```

Šifrový text:

```
CGDAI CWMMF VINHX BUOOI KCGLZ TMMWF FSFAL OMIXZ JITBB ZUOMA DFADJ IENMV
KMNOI DWXBB DYVKR WQVJA ZSIFO GWAXE TWLFU FZDKA MXZXB JBOMQ TTBOU WNPSK
AIVWQ DFRDF UOAQX BUSCQ U
```

Poznámky k luštění (markanty, nápovědy apod.):

Z textu se dalo odhadnout předpokládané slovo – podpis BIK.
Vzhledem k malé délce hesla perioda vychází a luštění je i při délce použitého textu snadné.
V nápovědě byl pak systém upřesněn (Vigenére) a to včetně náznaků, že příjemce (BIK) jej může uhodnout a že je heslo krátké (snad až příliš).

C. Soutěž v luštění 2007 – řešení úloh III. kola

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

Příklad: III/1
přijímací zkouška

Systém: polyalfabetická substituce, systém Vigenere
Upřesnění: použito periodické heslo CERNAKOMORA (délka 11).
Způsob skládání hesla a otevřeného textu varianta Vigenére.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Obraz
Správná odpověď: CNOSTI
Body: 3

Otevřený text:
Věnováno věčné památce. Nevýslovná bolest oživuje posvátný popel zbožňovaného nejjasnějšího císaře Karla VI., který velmi šťastně a plně, se stálostí a statečností Rakušana a nejen v těchto dvou, nýbrž ve všech heroických cnostech byl zcela dokonalým a zdatným císařem, který i v hrobě žije, abys věděl, poutníče, že majestát ani pohřben nikdy nezanikne.
Všeobecnému blahu propůjčen léta Krista, našeho Pána 1685, 1. října, nebeské vlasti vrácen roku 1740, 20. října, nemohl zanechat znamenitější památku nežli obraz cnosti, moudrosti a zbožnosti, Marii Terezii, císařovnu spravedlnosti a vládkyni dobroty, okrasu, vzor a řád. Žil 55 let, 19 dní a 8 hodin.
Text ze sakofágu Karla VI. na jeho památku a pro účel zkoušky zašifroval baron von Koch

Zdroj otevřeného textu:
Nápis na sarkofágu Karla VI. v kapucínském klášteře (Císařské kryptě) ve Vídni.
http://cs.wikipedia.org/wiki/Karel_VI.

Převod na mezinárodní abecedu:
```
VENOVANO VECNE PAMATCE NEVYSLOVNA BOLEST OZIVUJE POSVATNY POPEL
ZBOZNOVANEHO NEJJASNEJSIHO CISARE KARLA VI KTERY VELMI STASTNE A PLNE SE
STALOSTI A STATECNOSTI RAKUSANA A NEJEN V TECHTO DVOU NYBRZ VE VSECH
HEROICKYCH CNOSTECH BYL ZCELA DOKONALYM A ZDATNYM CISAREM KTERY I V HROBE
ZIJE ABYS VEDEL POUTNICE ZE MAJESTAT ANI POHRBEN NIKDY NEZANIKNE
VSEOBECNEMU BLAHU PROPUJCEN LETA KRISTA NASEHO PANA TISIC SEST SET
OSMDESATEHO PATEHO PRVEHO RIJNA NEBESKE VLASTI VRACEN ROKU TISIC SEDMSET
CTYRICATEHO DVACATEHO RIJNA NEMOHL ZANECHAT ZNAMENITEJSI PAMATKU NEZLI
OBRAZ CNOSTI MOUDROSTI A ZBOZNOSTI MARII TEREZII CISAROVNU SPRAVEDLNOSTI A
VLADKYNI DOBROTY OKRASU VZOR A RAD ZIL PADESATPET LET DEVATENACT DNI A OSM
HODIN TEXT ZE SARKOFAGU KARLA SESTEHO NA JEHO PAMATKU A PRO UCEL ZKOUSKY
ZASIFROVAL BARON VON KOCH
```

Šifrový text:
```
XIEBV KBAJV CPIGN MKHOS EEXCJ YOFBM PFLGW KBZSJ GXVPQ WMNTX MBCGE NDSBZ
XCHOE EJSER JTOEB VJUMY BCSGM FVKCV CNVSY FSIYX ICZIC HMGKN GEGYN OGQGK
ANSJG IKGFO KEERF FTSFM YLSCR RNNOX QBMTG GYGON JAIEY DVQIE FGQQY HGVFV
CUMOV TNQWK RCRPK ZQCGP RQOUC ZOCYO EQQAD BKATI UEIRM UHQFP IXLIB BONUX
VADCJ IENSX DFUVR ZPEJS YOAEU XRGAX WBCYR DIEAI URKBV ZCRZX NOJES FBGGE
RMEPX OYURV FCUTQ QBCEV EBEIC HMBRS GLFCA XOFWJ IEWVF TCSFC JMFIJ NTOVA
DRTGL FCRFS TCIIL RRAEL SEYVV NEJGI FFMQV NTSBH TSGUQ JEFQJ RTMHK FZCCX
VUONJ MQRTG LFEIT BMBVM QLCMA XSOVR TBRRZ EXWFS ASKTR ZADYG BVZNM FORKN
```

```
OBFSV MDBUN FAGKI CDSBZ XCEHZ MCVZV TOFQN ZIEMJ NRYJZ IJPTE MRDVB AGKIC
ZCNDU MZWUO DVFGY YYDOJ UXDFE ABOPN ZLREU RSKHB SKLGX URVKH QBRCV HEVAY
GYVFD KRKRX DNQGR RMSWN GEYMF CAUIJ GERCZ OAEJS GNMKH WIRPT SLPEV NWCLS
MCQNS STDCM ANFRE OXJAB BOEL
```

Poznámky k luštění (markanty, nápovědy apod.):
Délka textu umožňuje odhalit periodu. Při luštění lze také s výhodou použít některá předpokládaná slova. Někteří soutěžící také podle indicí v doprovodném textu dohledali nápis na sarkofágu a ten přímo použili při řešení úlohy.

Příklad: III/2
dopis pruského kurfiřta

Systém: nomenklator

Upřesnění:
Pro převod byl použit tento nomenklátor:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a b c	d	e	f	g h *	i	j	k	l m	N	o	p	q	r	s t	u	v	w	X y	z	A B	C	D	E	F G	H

ST	OV	NI	VA	NE	EN	PO	RA	RO	SE	OU	CH	PR	RN	ND	NH
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

STR	FRIDRICH	AUGUST	VALKY	VOJENSKA	RADA	SLEZKO
Y	11	12	2	31	32	4

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: P1
Správná odpověď: PRITELI
Body: 5

Otevřený text:
```
Můj vznešený a urozený příteli, posoudili jsme návrh tvého vyslance rytíře
von Amerlinga a naše vojenská rada souhlasí, že habsburský dům nebude po
smrti císaře připravený bojovat na několika stranách. To ovšem znamená, že
do boje musíme jít společně a ani jedna ze stran nesmí uzavřít s nepřítelem
jednostranný smír bez účasti druhého spojence. Neboť takovým krokem by
vystavila svého spojence útoku habsburského vojska, které není radno
podceňovat, zvláště pokud by útočilo jen proti jednomu z nás dvou. Proto
naše vojenská rada žádá příslib, že nedojde z usmíření mezi tebou a
Habsburky, aniž bychom toho nebyli účastni i my. Souhlasíme, že si podržíš
českou královskou korunu za předpokladu, že my získáme celé Slezsko.
Odpověď pošli po rytíři von Amerlingovi s návrhem smlouvy, jíž naše
vojenská rada podmiňuje zahájení války. Bůh pomáhej našim zbraním! Fridrich
August Druhý
```

Převod na mezinárodní abecedu:
```
MUJ VZNESENY A UROZENY PRITELI POSOUDILI JSME NAVRH TVEHO VYSLANCE RYTIRE
VON AMERLINGA A NASE VOJENSKA RADA SOUHLASI ZE HABSBURSKY DUM NEBUDE PO
SMRTI CISARE PRIPRAVENY BOJOVAT NA NEKOLIKA STRANACH TO OVSEM ZNAMENA ZE DO
BOJE MUSIME JIT SPOLECNE A ANI JEDNA ZE STRAN NESMI UZAVRIT S NEPRITELEM
JEDNOSTRANNY SMIR BEZ UCASTI DRUHEHO SPOJENCE NEBOT TAKOVYM KROKEM BY
VYSTAVILA SVEHO SPOJENCE UTOKU HABSBURSKEHO VOJSKA KTERE NENI RADNO
PODCENOVAT ZVLASTE POKUD BY UTOCILO JEN PROTI JEDNOMU Z NAS DVOU PROTO NASE
```

VOJENSKA RADA ZADA PRISLIB ZE NEDOJDE Z USMIRENI MEZI TEBOU A HABSBURKY ANIZ BYCHOM TOHO NEBYLI UCASTNI I MY SOUHLASIME ZE SI PODRZIS CESKOU KRALOVSKOU KORUNU ZA PREDPOKLADU ZE MY ZISKAME CELE SLEZSKO ODPOVED POSLI PO RYTIRI VON AMERLINGOVI S NAVRHEM SMLOUVY JIZ NASE VOJENSKA RADA PODMINUJE ZAHAJENI VALKY BUH POMAHEJ NASIM ZBRANIM FRIDRICH AUGUST DRUHY

Šifrový text:

Verze 1 – zveřejněna jako příklad v soutěži a v doprovodném příběhu na webu soutěže a v e-zinu Crypto-World 10/2007

```
q A n C H M R r F c A Q H N F U m z g p l O y S f m p m n y q g r c C w k z
C * k s C G x p c r e * w F z l w g C s r b q h w p l r j b c r a R 31 32 y
S k p a x m H g k a d x d B w x o F f A q M d B f g O x q w z l e l y a w g
U l U a C N G d t n J c z r b M o t p m o a Y a r a T z s J R q H r c q N a
H * f t d s n g q B x l q h n m z y O p g e M c c K n g f r b H h Y a r M y
q l A H a C w m z x M U l z g p h q n h f r s Y b r r G y q m w d * H A e c
I l f w B k g k t x O n N e g M d s z z c o J F q o Q o g q d G C F I c C l
p a x C g k t y O n N e * B z t o B k a d x d A w x o * k s C t n y o a o z
g w * M K P f r s O f e N J a z H C p c I * O o A f d G A z s e m p t n N U
s z m n g f r t q A H r b x f C S U t z t r c R 31 32 H b f a U l x p l d H
h M f s n f h H A x q m w N m q * H l z g d S c k c d x d B w o G a K H d G
T s q z s k s M d G p m A e b I K m q G y S k p b y m q * H h x m O f w H l
x e * y o S o P p J x o S o t w B r A H a U g f O o p a f B H * q F H m y o
b q * e h p * x p h H x o s s f O C h f O y p m O w G z m w m C t r b q * w
p m r j J l x r b C w k * q x q p S C G n l H r a R 31 32 O f q l r B n * H
b k a n N l 2 d A k O q a k h n r a y l q H d P K q 11 12 f w A k G
```

Verze 2 – zveřejněna v doprovodném příběhu na webu soutěže a v e-zinu Crypto-World 10/2007

```
q B n C H M R r G b A Q H N G U m z h p m O x S f l p m n y q * r a C w k z
C g k t C G y p b r e g w F z m w h C t r b q h w p m r j a a r b R 31 32 x
S k p b x m H * k c d y d A w y o F f B q M d A f * O x q w z l e m x b w g
U l U c C N G d s n J b z r c M o s p m o a Y c r a T z t J R q H r a q N a
H * f s d s n h q A x m q h n m z y O p g e M b c K n * f r a H g Y b r M y
q l B H a C w m z y M U l z h p h q n * f r t Y b r r F y q l w d h H A e b
I m f w B k h k s x O n N e g M d s z z c o J G q o Q o g q d G C G I a C l
p c x C * k t x O n N e * B z s o B k a d y d A w y o g k s C s n x o b o z
* w g M K P f r t O f e N J c z H C p c I * O o A f d G A z t e m p s n N U
t z l n g f r t q A H r a x f C S U s z s r a R 31 32 H a f a U l y p m d H
g M f t n f g H A x q l w N l q g H m z g d S c k c d y d B w o F b K H d G
T t q z t k t M d G p l A e c I K m q F y S k p a y l q * H g y m O f w H m
x e * x o S o P p J y o S o s w B r A H c U g f O o p a f A H h q G H l x o
b q h e h p h y p g H y o t s f O C h f O x p m O w F z l w l C s r b q h w
p m r j J m y r b C w k g q y q p S C F n l H r a R 31 32 O f q m r A n g H
c k a n N l 2 d A k O q a k * n r c y m q H d P K q 11 12 f w B k F
```

Verze 3 – zveřejněna v doprovodném příběhu na webu soutěže a v e-zinu Crypto-World 10/2007

```
q A n C H M R r F b B Q H N F U l z h p l O y S f m p m n x q * r c C w k z
C * k s C G y p b r e g w G z l w h C t r b q * w p m r j c a r a R 31 32 y
S k p c x l H h k a d y d B w y o F f A q M d A f * O y q w z m e l x b w *
U l U c C N F d s n J c z r b M o t p m o c Y c r b T z s J R q H r c q N b
H h f t d t n * q A y l q h n m z x O p g e M a b K n g f r a H h Y c r M x
q m A H a C w m z y M U m z h p g q n h f r s Y a r r G x q m w d h H B e c
I l f w B k g k s y O n N e g M d t z z a o J F q o Q o g q d F C G I c C l
p b x C h k t y O n N e h A z s o A k a d x d B w y o g k t C s n x o b o z
h w h M K P f r s O f e N J c z H C p a I * O o B f d G B z s e m p t n N U
t z m n h f r t q A H r b y f C S U s z s r c R 31 32 H b f a U m y p l d H
* M f s n f g H A y q l w N m q g H l z g d S b k c d x d A w o F b K H d F
```

```
T s q z t k t M d F p l B e c I K m q F x S k p b x l q g H g x m O f w H l
x e h x o S o P p J x o S o t w A r B H a U g f O o p c f B H * q G H m y o
a q * e * p h x p g H x o s s f O C h f O x p m O w G z l w m C t r c q g w
p l r j J m x r c C w k * q y q p S C G n l H r a R 31 32 O f q m r B n g H
b k a n N m 2 d A k O q c k * n r b y l q H d P K q 11 12 f w A k G
```

Poznámky k luštění (markanty, nápovědy apod.):
Použitý nomenklátor je sestaven „slabě“. Luštitel může odhadnout jeho konstrukci. Navíc jsou kódová slova odhalitelná podle jiné použité množiny šifrových znaků (číslice).
K řešení vede využití toho, že byly zveřejněny různé verze šifrového textu. To znamená, že porovnáním jednotlivých úseku šifrového textu získal luštitel informaci, které homofony patří ke stejnému znaku otevřeného textu a úloha se tím převedla na řešení jednoduché záměny.
Příklad (začátek šifrových textů):
q A n C H M R r F
q B n C H M R r G
Řešitel z tohoto úseku snadno zjistí, že A,B jsou znaky pro stejné písmeno otevřeného textu a obdobně pak F,G jsou homofony pro jiný znak otevřeného textu.
Při řešení lze použít i odhad některých předpokládaných slov.

Příklad: III/3
dopis carevny Kateřiny

Systém: nomenklator

Upřesnění:
Pro převod byl použit tento nomenklátor:

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
z Z	y	x	w	v V	u	t	s	r R	q	p	O	n	m	l L	k	j	i	h H	g G	f F	e	d	c	b	a

ST	OV	PO	RA	RO	SE	OU	CH	MARIE	TEREZIE	PETR	KATERINA
S1	O1	P1	R1	R2	S2	O2	C1	1	2	3	4

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Jakému stryci?
Správná odpověď: OBDIVOVANEMU
Body: 5

Otevřený text:
```
Mému obdivovanému stryci pruskému kurfiřtu Friedrichovi II. od princezny
Sofie Frederiky Augusty Anhaltské, toho času manželka ruského cara Petra
III. zvaná v Rusku Kateřina. Nemohu již déle snášet hloupost a rozmary
bojarů, kteří vládnou mému manželovi, místo aby car vládl Rusku. Rovněž
nemohu souhlasit s tím, aby ruská vojska bojovala proti zemi mých drahých
příbuzných. Přísaha jsem věrnost ruské carské koruně a jsem ochotná ji
dodržet. Ovšem jsou chvíle, kdy je i carevna bezmocná. Pokud by došlo
k situaci, že by má garda povstala a přitom by zahynul můj manžel car Petr
III., chci vědět, zda v takovém případě uzná můj vznešený strýc moje
nezadatelné právo vládnout v Rusku jako carevna. Pokud by tento nárok
uznal, ruská vojska by přestala podporovat habsburský dům, neboť nikdo mi
není tak protivný, jako ta tlustá a ordinérní Marie Terezie.
```

Převod na mezinárodní abecedu:

MEMU OBDIVOVANEMU STRYCI PRUSKEMU KURFIRTU FRIEDRICHOVI II OD PRINCEZNY SOFIE FREDERIKY AUGUSTY ANHALTSKE TOHO CASU MANZELKA RUSKEHO CARA PETRA III ZVANA V RUSKU KATERINA NEMOHU JIZ DELE SNASET HLOUPOST A ROZMARY BOJARU KTERI VLADNOU MEMU MANZELOVI MISTO ABY CAR VLADL RUSKU ROVNEZ NEMOHU SOUHLASIT S TIM ABY RUSKA VOJSKA BOJOVALA PROTI ZEMI MYCH DRAHYCH PRIBUZNYCH PRISAHA JSEM VERNOST RUSKE CARSKE KORUNE A JSEM OCHOTNA JI DODRZET OVSEM JSOU CHVILE KDY JE I CAREVNA BEZMOCNA POKUD BY DOSLO K SITUACI ZE BY MA GARDA POVSTALA A PRITOM BY ZAHYNUL MUJ MANZEL CAR PETR III CHCI VEDET ZDA V TAKOVEM PRIPADE UZNA MUJ VZNESENY STRYC MOJE NEZADATELNE PRAVO VLADNOUT V RUSKU JAKO CAREVNA POKUD BY TENTO NAROK UZNAL RUSKA VOJSKA BY PRESTALA PODPOROVAT HABSBURSKY DUM NEBOT NIKDO MI NENI TAK PROTIVNY JAKO TA TLUSTA A ORDINERNI MARIE TEREZIE

Šifrový text:

n V n F l y w r e O1 z m v n F S1 i b x r k i F H p V n F p f i u r i G F u
i R v w i r C1 O1 R R r L w k i R m x V a m b h l u r v u i v w v i r p b Z
f t F S1 b Z m s Z o g h p v g L s L x Z h F n Z m a v o p Z i F h p v s L
x z R1 3 Z R r R a e Z m z e i f H p f 4 m v n L s F q R a w V o V H m z S2
G s o O2 P1 S1 Z R2 a n Z i b y L q Z i f p G V i R e o Z w m O2 n v n f n
Z m a V o O1 r n R S1 L Z y b x Z i e o z w o i F H p F R2 e m v a m V n L
s f H O2 s o Z H r g h g R n Z y b i F H p z e l q H p z y l q O1 Z o Z k
R2 g R a V n R n b C1 w R1 s b C1 k i r y f a m b C1 k i R h Z s z q S2 n e
V i m L S1 i f H p v x z i h p v p l i f m v z q S2 n l C1 L G m z q r w l
w i a v G O1 S2 n q H O2 C1 e r o v p w b q V R x z i v e m z y V a n L x m
Z P1 p F w y b w L h o l p h R g f Z x r a v y b n z t Z i w z P1 e S1 Z o
Z z k i r g l n y b a z s b m f o n f q n z m a v o x Z i 3 R r r C1 x R e
v w V g a w z e G z p O1 V n k i R k Z w V F a m z n f q e a m V S2 m b S1
i b x n l q V m v a Z w Z G V o m v k R1 e L e o z w m O2 G e i F h p F q Z
p l x Z i V e m z P1 p f w y b g v m g l m z R2 p F a m z o i F h p z e l q
h p Z y b k i v S1 Z o z P1 w P1 R2 e z g s Z y h y f i h p b w f n m v y l
G m R p w l n r m V m R G Z p k R2 g r e m b q Z p L G Z G o F S1 z Z l i w
r m v i m r 1 2

Poznámky k luštění (markanty, nápovědy apod.):

Použitý nomenklátor je sestaven „slabě“. Jedná se o reciprokou jednoduchou záměnu. Jako homofony jsou použita malá a velká písmena šifrové abecedy … Luštitel může odhadnout jeho konstrukci. Šifrová abeceda použitá pro záměnu slabik a kódů je jiná než abeceda pro záměnu jednotlivých znaků. Pokud to luštitel zjistí, může jendotlivé části luštit jako jednoduchou záměnu.

Při řešení většina soutěžících využila odhad některých předpokládaných slov a to zejména MARIE TEREZIE.

Příklad: III/4
šifra vyluštěna v Bad Ischlu

Systém: jedna z verzí šifry „podle plotu“ (Rail fence cipher)

Upřesnění:

Klíčem k této šifře je tedy domluvená tabulka (počet řádků) a způsob zápisu textu do této tabulky.
V tomto konkrétním případě se text vepisuje do níže uvedené tabulky na místa označená hvězdičkami. Šifrový text se získá tak, že se opíší znaky nejprve z prvého řádku tabulky, pak z druhého a nakonec třetího.

*				*				*				*				*
	*		*		*		*		*		*		*		*	
		*				*				*				*		

N				Z				A				E				E
	A		I		U		I		B		S		N		S	
		R				J				Y				A		

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Odkud?
Správná odpověď: VRATISLAVI
Body: 3

Otevřený text:
Nařizuji, aby se naše vojska přesunula od Vratislavi ku Praze, neboť po neúspěchu u Kolína je nutné co nejdříve město dobýt. Do zimy je třeba získat útočiště pro naše oddíly, abychom byli připraveni na další válku během příštího jara proti habsburské armádě.

Převod na mezinárodní abecedu:
NARIZUJI ABY SE NASE VOJSKA PRESUNULA OD VRATISLAVI KU PRAZE NEBOT PO NEUSPECHU U KOLINA JE NUTNE CO NEJDRIVE MESTO DOBYT DO ZIMY JE TREBA ZISKAT UTOCISTE PRO NASE ODDILY ABYCHOM BYLI PRIPRAVENI NA DALSI VALKU BEHEM PRISTIHO JARA PROTI HABSBURSKE ARMADE

Šifrový text:
NZAEE SRNOA LKAEP UCKNN EEIED TIEBS UIPAD YCBPR NDIKH RIARH BKMAI UIBSN
SVJKP EUUAD RTSAI URZNB TOESE HUOIA EUNCN JRVMS OOYDZ MJTEA IKTTC SERNS
ODLAY HMYIR PAEIA ASVLU EEPIT HJRPO IASUS ERAER JYAOA SLVIV PEONP ULJTO
DETBO YRZAO TOEIB OLIVN LABMS OATBR AD

Poznámky k luštění (markanty, nápovědy apod.):
Princip vysvětlen v nápovědě č. 9. V nápovědě použit jiný, leč obdobný způsob zaplnění tabulky. Hloubka (počet řádků) byla použita stejná a to 3.

Příklad: III/5
šifra z roku 1757, obležení Prahy

Systém: homofonní substituce
Upřesnění:
Použitá převodová tabulka

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	a	A	4	d	D	7	g	G	10	i	I	13	l	L	16	o	O	19	r	R	22	u	U	25	x	
2	b	B	5	e	E	8	h	H	11	j	J	14	m	M	17	p	P	20	s	S	23	v	V	26	y	
3	c	C	6	f	F	9	ch	CH	12	k	K	15	n	N	18	q	Q	21	t	T	24	w	W	27	z	

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (3)
Správná odpověď: TYDNU
Body: 5

Otevřený text:
Již mnoho týdnů obléhá naše vojsko Prahu, ale zatím bez většího úspěchu, neboť město je hrubě opevněné a v jeho hradbách stojí početné a dobře vycvičené oddíly a je smutnou pravdou,. že i domácí obyvatelé bojují proti nám, jako bychom byli nepřátelé my a nikoli dům habsburský, který už více než sto let drží českou královskou korunu neprávem. Jak se nám doneslo od zvědů, od východu se blíží silné rakouské oddíly vedené generálem Daunem. Rozhodli jsme se vyjít jim vstříc a utkat se s nimi u Kolína, abychom nadále udrželi Prahu v obležení. Protože je naše vojsko početně silnější, lze doufat s boží pomocí ve vítězství. Proto naše vojenská rada vypracovala nový plán bitvy, abychom nepřítele zcela zničili. Bitvu zahájíme útokem jízdy na pravé křídlo a tak obklíčíme střed rakouské armády. Proto nařizuji velitelům jízdy soustředit do týdne oddíly u vesnice Kutlíře.
Já, z boží milosti pruský kurfiřt Friedrich, toho jména druhý. V květnu léta Páně 1757.

Převod na mezinárodní abecedu:
JIZ MNOHO TYDNU OBLEHA NASE VOJSKO PRAHU ALE ZATIM BEZ VETSIHO USPECHU NEBOT MESTO JE HRUBE OPEVNENE A V JEHO HRADBACH STOJI POCETNE A DOBRE VYCVICENE ODDILY A JE SMUTNOU PRAVDOU ZE I DOMACI OBYVATELE BOJUJI PROTI NAM JAKO BYCHOM BYLI NEPRATELE MY A NIKOLI DUM HABSBURSKY KTERY UZ VICE NEZ STO LET DRZI CESKOU KRALOVSKOU KORUNU NEPRAVEM JAK SE NAM DONESLO OD ZVEDU OD VYCHODU SE BLIZI SILNE RAKOUSKE ODDILY VEDENE GENERALEM DAUNEM ROZHODLI JSME SE VYJIT JIM VSTRIC A UTKAT SE S NIMI U KOLINA ABYCHOM NADALE UDRZELI PRAHU V OBLEZENI PROTOZE JE NASE VOJSKO POCETNE SILNEJSI LZE DOUFAT S BOZI POMOCI VE VITEZSTVI PROTO NASE VOJENSKA RADA VYPRACOVALA NOVY PLAN BITVY ABYCHOM NEPRITELE ZCELA ZNICILI BITVU ZAHAJIME UTOKEM JIZDY NA PRAVE KRIDLO A TAK OBKLICIME STRED RAKOUSKE ARMADY PROTO NARIZUJI VELITELUM JIZDY SOUSTREDIT DO TYDNE ODDILY U VESNICE KUTLIRE
JA Z BOZI MILOSTI PRUSKY KURFIRT FRIEDRICH TOHO JMENA DRUHY V KVETNU LETA PANE TISIC SEDM SET PADESAT SEDM

Šifrový text:

Verze 1: zveřejněna v doprovodném příběhu na webu soutěže a v e-zinu Crypto-World 10/2007
10 G z 14 l N g M r 25 6 m R M c I f g 3 m 2 19 d 24 L 10 21 i M 18 P 3 ch R 1 J e z 2 r H 15 a e y 22 f r 19 G g N T 21 17 f C ch R l f b N s 13 f 21 s N 10 e ch O S a f M 18 f 23 l e l d 2 22 11 d h M ch P 3 6 b 3 A h 19 t L 11 H 18 L B d r l d 3 6 N c Q e 23 26 A 23 H C f m f L 5 5 G K 27 1 12 d 19 13 T r m N R 17 P 1 23 4 M T y f G 4 M 13 2 A H N b 27 22 2 s e K d a N 12 S 11 CH 16 Q M s H m 2 13 10 2 k L a 26 B h L 15 a 27 K H m f 18 P 3 r f K e 14 27 1 m CH i N J CH 6 T 15 h 3 c 19 c R O 19 j 27 k r d P 27 S x 23 G A e m e x 19 r L I f t 6 P x CH A d 19 i M R k P 1 I M 22 19 j M R j L Q S m R m d 17 O 1 24 e 14 11 3 j 19 e m 1 13 4 L m f 19 I M L 6 y 24 d 5 S L 6 24 27 C g N 5 T 19 e b K CH z CH 19 H J l f Q 1 k N R 20 k d L 6 4 CH K 25 24 d 6 d m d 7 d m e Q 1 K e 14 6 1 S m e 15 O L y ch L 6 K CH 12 20 14 e 20 e 22 26 11 G s 11 H 15 24 20 r P G C 2 S r j 3 t 21 e 21 m H 13 G S i M I H m 1 3 a 27 A ch M 13 l 2 4 2 K d R 4 P z f J H 16 O 2 ch S 23 L a I d x d l H 16 O M r L x e 10 f m 2 19 e 23 L 11 20 i L 16 L B f r m d 21 G J m e 11 20 CH K x f 4 L R D 2 t 19 a L z H 18 L 15 N B H 23 d 22 G r d z 21 t 23 CH 17 Q L r N m 3 20 d 22 N 11 d m 19 j 1 O 3 5 1 23 27 16 Q 1 C N 23 1 I 3

l L 24 25 17 K 2 m a H t 24 25 1 a 27 A h N 13 l f 17 P H s f J d y C d I 2
y m H C G I CH b H t 23 S y 3 g 2 10 CH 14 f T s N i d 13 11 G y 4 26 m 3
17 Q 3 23 f i P CH 5 K L 1 r 1 k L a i I CH C CH 15 f 20 s Q d 5 P 3 k N T
19 j e 1 Q 15 1 6 27 16 O N t M m 3 O H x S 10 H 24 e K G r e I S 13 11 H y
5 27 19 M S 20 r Q e 5 G r 6 N s 25 4 l d L 6 4 G J 25 R 23 e 20 l CH B f k
S r K H P e 12 2 y a L z CH 14 CH I N 20 t CH 18 P S 21 k 25 k R O D H Q t
D O H f 5 O H C g s M h L 10 13 d l 3 6 O S g 27 22 i 22 d s l T J e r 2 16
1 m e r G 19 CH A 21 d 5 13 20 d r 18 2 5 d 21 2 r 20 f 4 15

Verze 2: zveřejněna jako příklad v soutěži

10 G x 14 m L g L t 26 4 l T L a J d ch 1 l 1 19 e 24 N 11 21 k N 16 P 1 ch
T 3 J d x 2 r G 14 b d y 24 f s 20 CH h N R 21 16 e A h R m d c M s 14 e 20
t L 10 e h Q T b e L 16 e 24 m d l d 1 22 12 f g M g O 2 5 b 1 C g 21 t M
10 H 17 L B f s m d 1 6 N a P d 23 25 B 23 H B d m e N 6 6 G K 25 2 12 d 19
13 T s m L T 16 P 2 23 6 N T z f H 5 M 13 3 B CH N c 27 22 3 s d K f b L 10
S 11 G 16 Q N r H m 1 15 10 3 k M a 25 A h M 15 a 27 K CH m f 16 Q 3 t d K
e 15 25 2 l G k M J H 5 T 14 g 2 a 19 a S P 21 j 25 i r f P 26 T y 23 CH A
e m e x 21 s M K e t 5 Q x CH C f 19 i M T j O 1 J N 22 20 i M T k M P R m
S m e 16 O 1 22 d 15 10 1 k 19 d m 2 14 4 N l f 20 I M N 4 y 23 e 4 S N 6
24 27 A ch L 6 R 20 d b K H z H 19 CH K l d O 2 k N R 19 j e L 4 6 CH I 26
22 f 6 f m f 9 f l d Q 3 I f 15 6 1 T m e 13 Q L x ch L 5 I G 12 21 13 e 21
d 23 25 12 G r 10 G 13 23 20 t P CH C 3 R s j 3 t 21 e 19 m CH 14 CH R j L
K CH m 3 3 b 26 B g M 14 m 3 6 2 I e R 6 Q y d K CH 18 O 3 ch S 22 L b K d
z d m CH 16 O L t L x e 10 e m 2 21 f 22 M 11 21 k N 17 N A e t m e 19 G J
l e 10 21 G K z f 4 L S D 3 t 19 c M y CH 17 M 15 N A H 23 d 23 G r e x 20
r 23 CH 17 P M t N l 2 19 f 22 L 11 f m 19 i 3 P 1 4 3 22 26 17 O 3 A L 22
1 J 3 m M 24 27 16 I 1 m b CH s 22 27 1 b 27 A g L 13 m f 18 P H t e K d z
A e I 2 x m G C H J CH b CH r 23 S y 3 g 1 12 CH 14 e T r N j e 14 11 CH y
5 27 l 2 17 Q 2 24 e k P G 4 K M 3 t 2 k L c k J H C G 14 f 19 s O e 5 P 2
i M S 21 j f 3 Q 13 2 5 27 18 O M r N l 3 Q G y R 12 H 23 e K H r e I S 13
12 CH z 6 25 21 M R 19 t O d 6 G r 6 N t 26 6 m e N 5 6 H K 25 T 24 f 19 l
H C e k T t K G Q f 12 1 z b N x H 15 CH J L 20 s H 17 O R 19 k 25 i S Q F
H O s D Q H e 6 P H C g s N h L 12 13 d m 2 6 P S g 26 24 j 24 f s m R I d
r 2 18 1 l d t CH 19 H C 20 e 5 14 19 d r 16 1 6 f 19 2 t 21 d 4 13

Verze 3: zveřejněna v nápovědě č.8

12 CH x 14 m N ch N s 27 4 m T N b I d g 1 m 1 21 d 24 N 12 19 i M 16 P 3
ch S 1 I e x 1 s CH 13 b d z 23 f t 19 CH g L R 20 16 d A h S n e c N s 15
d 20 t M 10 e h Q T b f L 16 d 23 n f n f 2 23 11 d h M ch Q 3 6 a 2 A g 21
t L 11 CH 16 N B f s m f 1 4 N a Q d 23 25 B 24 CH A f l f L 4 4 H K 27 1
10 d 21 15 R r n L S 17 P 3 24 6 N T y f CH 4 N 15 1 C CH L b 25 23 2 r d J
d a M 11 R 10 CH 18 P M t H n 2 15 10 2 i L a 26 B ch M 15 c 27 K G l f 18
Q 2 t e K e 14 27 1 n H j M J H 4 R 13 ch 2 a 20 b S P 21 j 27 j s e Q 26 S
y 24 H B d l e z 19 s L K e s 4 Q z CH A f 20 k L S j P 2 K M 23 20 k M R j
N O S m R n d 16 O 1 24 f 15 11 3 k 19 d l 3 14 6 M l f 21 J N L 4 y 24 d 6
S L 5 23 25 C g N 6 S 21 d a J G z G 20 H J m f O 2 j M R 21 j e M 6 6 G K
26 24 f 5 f l d 8 d l d P 2 K e 13 4 1 T m e 15 P M z ch M 6 I G 12 21 13 f
19 f 22 26 12 H t 11 CH 14 22 21 t O CH A 2 T t i 1 s 20 d 19 n CH 13 H R k
N K CH n 2 2 c 25 B h N 15 n 2 4 2 I d T 5 O z e K G 18 Q 2 h R 23 N a J d
y d l G 18 Q L r M x e 11 e n 1 19 e 23 N 10 21 j M 16 M C f t m d 19 G I l
f 10 20 G K x d 4 L S D 3 s 20 a M y G 17 M 13 L A CH 22 f 24 G t d z 19 s
22 G 16 P M t L n 3 21 d 22 M 12 f l 19 i 3 O 2 6 2 22 25 17 Q 3 C N 23 2 J
1 m M 24 27 18 K 1 m b G t 24 25 3 c 25 A h N 14 m f 17 O CH s f J e x B f
K 1 x m CH B G I H c CH s 22 S z 3 g 1 12 G 14 e S t L i d 13 12 CH z 5 27
n 1 16 O 1 23 f j P G 4 J N 1 s 1 k M a i J CH C H 15 e 21 r Q d 5 P 3 j N
S 21 k f 1 P 14 3 6 27 17 P N t M n 1 O G y S 11 H 23 d J H t e J T 14 11 H
z 5 25 21 M S 21 s P f 6 H s 5 M t 25 4 n d N 4 5 CH J 26 S 24 f 19 n G A d
i S t I G O f 11 3 x a L y CH 14 G I L 19 r CH 18 Q S 21 k 25 i R Q E G P r
D O H d 4 O H A g t M g M 12 13 f l 3 6 P R g 25 23 i 24 d s n T K f r 3 18
3 l f s CH 19 H C 21 e 4 14 20 e s 16 1 4 f 19 1 s 20 e 4 15

Poznámky k luštění (markanty, nápovědy apod.):

Použita převodová tabulka je sestaven „slabě“. Luštitel může odhadnout její konstrukci.
K řešení vede využití toho, že byly zveřejněny různé verze šifrového textu. To znamená, že porovnáním jednotlivých úseku šifrového textu získal luštitel informaci, které homofony patří ke stejnému znaku otevřeného textu a úloha se tím převedla na řešení jednoduché záměny.
Příklad (začátek šifrových textů):
10 G z 14 l N g M
10 G x 14 m L g L
12 CH x 14 m N ch N
Řešitel z tohoto úseku snadno zjistí, že např. 10,12 jsou znaky pro stejné písmeno otevřeného textu a obdobně pak G,CH jsou homofony pro jiný znak otevřeného textu a dále ztotožní l,m resp. N,L, M , resp. g,ch.
Z těchto zřetězení homofonů může zpětně odvodit, že tabulka je sestavena slabě a zjistit jak je pravděpodobně zkonstruována, což mu významně pomůže při luštění.

Při řešení lze použít i odhad některých předpokládaných slov.

Zajímavé je, že jen málo luštitelů se všimlo, že verze šifrového textu zveřejněná na webu soutěže je jiná než verze otištěná v e-zinu. Těmto luštitelům pomohlo teprve zveřejnění třetí verze v nápovědě č.8.

Příklad: III/6

Švédové se chystají uplatnit své nároky v Baltském moři

Systém: transpozice
Upřesnění: sloupcová transpozice, 6 sloupců,
transpoziční abecední heslo: GUSTAV
heslo po vyčíslení: 2-5-3-4-1-6
délka otevřeného textu: 621 znaků
rozměr tabulky: 624=6*104
na úplnou tabulku doplněn otevřený text o 3 znaky X

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (3)?
Správná odpověď: VALECNE
Body: 3

Otevřený text:
Protože ruské válečné lodě stále častěji křižují poblíž našich švédských břehů, což je samo o sobě na pováženou, a na opakované výzvy naší královské milosti odpovídá ruský car Petr III. Fjodorovič s posměchem svému hloupému rodu vlastnímu, navrhujeme zahájit jednání o spojenectví s pruským kurfiřtem Fridrichem. Jeho vojska utrpěla četné porážky, v posledních měsících také od ruského generála Rumjanceva a pokud naše síly nezasáhnou, mohl by být vliv Ruska ještě silnější, což nelze připustit. Naše sbory o síle 22 tisíc mužů se vylodí poblíž Rujany a odtud zahájí pochod na jih. Než se tak stane, požadujte příslib od pruského kurfiřta, že za naši pomoc podpoří naše nároky v Baltském moři na přístavy, které uchvátil car Petr zvaný Veliký.

Převod na mezinárodní abecedu:

PROTOZE RUSKE VALECNE LODE STALE CASTEJI KRIZUJI POBLIZ NASICH SVEDSKYCH BREHU COZ JE SAMO O SOBE NA POVAZENOU A NA OPAKOVANE VYZVY NASI KRALOVSKE MILOSTI ODPOVIDA RUSKY CAR PETR TRETI FJODOROVIC S POSMECHEM SVEMU HLOUPEMU RODU VLASTNIMU NAVRHUJEME ZAHAJIT JEDNANI O SPOJENECTVI S PRUSKYM KURFIRTEM FRIDRICHEM JEHO VOJSKA UTRPELA CETNE PORAZKY V POSLEDNICH MESICICH TAKE OD RUSKEHO GENERALA RUMJANCEVA A POKUD NASE SILY NEZASAHNOU MOHL BY BYT VLIV RUSKA JESTE SILNEJSI COZ NELZE PRIPUSTIT NASE SBORY O SILE DVACETDVA TISIC MUZU SE VYLODI POBLIZ RUJANY A ODTUD ZAHAJI POCHOD NA JIH NEZ SE TAK STANE POZADUJTE PRISLIB OD PRUSKEHO KURFIRTA ZE ZA NASI POMOC PODPORI NASE NAROKY V BALTSKEM MORI NA PRISTAVY KTERE UCHVATIL CAR PETR ZVANY VELIKY

Šifrový text:

OKCEC IJICS RZONZ NOYSO IODYT IRPHM PDTAE ADSEP MRIEV UAPYE MCOEE UEKEE
NLVST EZPTE OVVCE IZYDI DNAEU IDEFE IPIAB ENTEV AZEXP EVETS RPNSY HESPN
OAVKS OPRAT JVSMH MVIRE IAOTU UERJJ RERPN STROA JADIA UYIAS SEITB ICTUY
OUOAO AZSOT LRORA ODAOL MPVET PAIOU LOLEZ BSEHC ABVUA ENAET VSPED CEVOR
AUUAJ IEIKF FCHKE NZSCC KSEAN PAYAO YRELC ZUARE TSUOL ATAHI EAAPB SUAAO
OEYSR IKCLT YYTSE DEJUL IDBOM EAAKV ALMII KETOS CEUOS NJHEO NSYIR HOALE
KLHIE KNRCO SNHHT USNOE SSYDD ISDIN UJOHT NDROK RZSCR NVKIS THCRV XRRAL
ATIOA VCUSO OOPNY RKSOU RROIM SLULM HZTNJ VSRMI ESPTA OIIAU GLAAN LSMBV
JIILP NOLEI ZLBJD HCJST ZEIUK TNMPS KTORY UIENK ZENSA KIZHK EJOAE AVZIV
LDACR FOOEU EUNVM JNPCR KTDMO TCOVD EHDHR MVUSZ OBLKE JNRIS SAAMV PRAZP
NEKPJ SPHIZ PONRA MAARA RVLX

Poznámky k luštění (markanty, nápovědy apod.):

Charakter otevřeného textu byl zachován, uživatel mohl předpokládat, že jde o transpozici, rozměr transpoziční tabulky lze získat odhadem (lze podpořit výpočtem poměr samohlásek : souhláskám), jako padding (doplněk na celou tabulku) použita „klasická“ písmena X, což umožňuje se jednak ujistit o správné velikosti tabulky a jednak k sobě přiřadit sloupce ukončené X.

D. Soutěž v luštění 2007 – řešení úloh IV. kola

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

Příklad: IV/1

Klementin dopis

Systém: polyalfabetická substituce, systém Vigenere

Upřesnění:
Klíč použitý k zašifrování dopisu získá luštitel, po dešifrování komentáře k dopisu/úloze. Je zašifrován pomocí stejného systému (Vigenére), a bylo použito heslo, které je sestavano ze slov, kterými luštitel prokazoval vyluštění předchozích dvaceti úloh. Délka hesla je 136 znaků. Použití tohoto hesla se dá odvodit z doprovodného textu k příběhu:

BUHALESIEDEUSMEDUSANOSTRADAMUSPRATELSTVIPITISTUDENTJOSEFLOYOLY
ZKOUSKUMORGESTERNBARONENAMICNOSTIPRITELIOBDIVOVANEMUVRATISLAVI
TYDNUVALECNE

Tento zašifrovaný komentář má délku 230 znaků a je předřazen před dopis.

K zašifrování samotného dopisu (otevřeného textu) je použito periodické heslo, které je sestaveno ze třetích slov otevřených textů předchozích dvaceti úloh, délka 115 znaků:

OBLOHUVYSOKYMCREAVITKDOKOLIPRACOVALMUSIMMLUVISTUDENTNIKDY
CHCEZAVERECNOUABYBARONEZNAMENAPAMATCEASTRYCISETYDNUVALECNE

	Hesla k úlohám	Třetí slova úloh
I/1	BUH	OBLOHU
I/2	ALESIE	VYSOKYM
I/3	DEUS	CREAVIT
I/4	MEDUSA	KDOKOLI
I/5	NOSTRADAMUS	PRACOVAL
I/6	PRATELSTVI	MUSIM
I/7	PITI	MLUVI
I/8	STUDENT	STUDENT
I/9	JOSEF	NIKDY
II/1	LOYOLY	CHCE
II/2	ZKOUSKU	ZAVERECNOU
II/3	MORGESTERN	ABY
II/4	BARONE	BARONE
II/5	NAMI	ZNAMENA
III/1	CNOSTI	PAMATCE
III/2	PRITELI	A
III/3	OBDIVOVANEMU	STRYCI
III/4	VRATISLAVI	SE
III/5	TYDNU	TYDNU
III/6	VALECNE	VALECNE
20	136	115

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil:
není (je uvedena v komentáři, který luštitel získá v prvém kroku)

Správná odpověď: PENIZE
Body: 12

Otevřený text (KOMENTÁŘ):
Blahopřeji, za chvíli vyřešíte poslední úkol a možná získáte celkové vítězství. Sestavte nový klíč a to ze třetích slov vyřešených úloh. Délka klíče bude sto patnáct. Potom dešifrujte poslední úlohu – Klementin dopis. Jako důkaz o vyřešení této úlohy zadejte šesté slovo od konce!

Převod na mezinárodní abecedu (KOMENTÁŘ):
BLAHOPREJI ZA CHVILI VYRESITE POSLEDNI UKOL A MOZNA ZISKATE CELKOVE VITEZSTVI SESTAVTE NOVY KLIC A TO ZE TRETICH SLOV VYRESENYCH ULOH DELKA KLICE BUDE STO PATNACT POTOM DESIFRUJTE POSLEDNI ULOHU KLEMENTIN DOPIS JAKO DUKAZ O VYRESENI TETO ULOHY ZADEJTE SESTE SLOVO OD KONCE

Šifrový text (komentář):
CFHHZ TJMNL DUUTZ LFAVL FWLZT HPAMD TUNBY VGEVU DHGIR BMNEG
XLSDO TGSTW ECYCH PACYE HRBXW GSMLL LZQNX BZQBT RHAVP HCWOZ
JZSTH VTQCU YSTXZ CKTSD TCZJN BHFNJ PLXPN GUJVT ZQVMW LJLMV
XHJGS YSVGZ UOOTO CAVMX REAGY WEQLR SDIGY XTICN CWPGC BTRDD
CODYB KNRJI BMIJR TTVGY SIOAL MBBUX

Vigenérova šifra
Délka textu: 230
Délka klíče: 136
Klíč.
BUHALESIEDEUSMEDUSANOSTRADAMUSPRATELSTVIPITISTUDENTJOSEFLOY
OLZKOUSKUMORGESTERNBARONENAMICNOSTIPRITELIOBDIVOVANEMUVRATISLAVI
TYDNUVALECNE

Otevřený text (DOPIS):
Štěpán Sch. pracuje v kanceláři, která patří pod ministra zahraničí. Kdysi mne naučil práci se šiframi a jsem si jistá, jak jsem již ostatně psala, že tuto znalost využívá i nyní. Naposledy se zmínil o jakémsi baronovi, ale pak se to hned snažil zamluvit. Od posluhy z jeho úřadu jsem se dozvěděla, že tam pracují dva, Ignác von Koch a baron Humprecht z Chudenic. Pravděpodobně bude pracovat u Ignáce von Kocha. Ten sice není baronem, ale nechává si tak u dvora vždy říkat. Pokusím se dostat do jeho blízkosti. Bylo by také vhodné sdělit našim spojencům, aby byli opatrnější při zasílání tajných zpráv. Domnívám se, že některé z používaných systémů Štěpán zná. Jak se k nim dostal, nevím. Poznala jsem to z popisů šifer, které mi ukazoval. Opravdu jsou shodné s těmi, které jste mi doporučili používat. Přiměla jsem Štěpána, aby mi posílal milostné vzkazy zašifrovaně. Posílám jejich opisy, aby bylo zřejmé, jaké šifry Štěpán zná a používá. Je možné, že je ve Vídni u dvora používají také. Štěpán také tvrdí, že vymýšlí šifru, kterou nebude možné rozluštit. O tom ostatně mluvil již před lety, kdy jsem se s ním seznámila. Nevím proto, zda je to pravda nebo jen jeho velké přání. Nechala jsem si ji ukázat a vysvětlit. Její přesný popis včetně klíče zasílám starým kódem. Tento nový je již zašifrován Štěpánovou metodou. Doufám, že předchozí dopis dorazil a tento díky tomu bez problémů dešifrujete. Peníze mi pošlete jako obvykle. Klementina.

Převod na mezinárodní abecedu (DOPIS):
STEPAN SCH PRACUJE V KANCELARI KTERA PATRI POD MINISTRA ZAHRANICI KDYSI MNE NAUCIL PRACI SE SIFRAMI A JSEM SI JISTA JAK JSEM JIZ OSTATNE PSALA ZE TUTO ZNALOST VYUZIVA I NYNI NAPOSLEDY SE ZMINIL O JAKEMSI BARONOVI ALE PAK SE TO

HNED SNAZIL ZAMLUVIT OD POSLUHY Z JEHO URADU JSEM SE DOZVEDELA ZE TAM PRACUJI DVA IGNAC VON KOCH A BARON HUMPRECHT Z CHUDENIC PRAVDEPODOBNE BUDE PRACOVAT U IGNACE VON KOCHA TEN SICE NENI BARONEM ALE NECHAVA SI TAK U DVORA VZDY RIKAT POKUSIM SE DOSTAT DO JEHO BLIZKOSTI BYLO BY TAKE VHODNE SDELIT NASIM SPOJENCUM ABY BYLI OPATRNEJSI PRI ZASILANI TAJNYCH ZPRAV DOMNIVAM SE ZE NEKTERE Z POUZIVANYCH SYSTEMU STEPAN ZNA JAK SE K NIM DOSTAL NEVIM POZNALA JSEM TO Z POPISU SIFER KTERE MI UKAZOVAL OPRAVDU JSOU SHODNE S TEMI KTERE JSTE MI DOPORUCILI POUZIVAT PRIMELA JSEM STEPANA ABY MI POSILAL MILOSTNE VZKAZY ZASIFROVANE POSILAM JEJICH OPISY ABY BYLO ZREJME JAKE SIFRY STEPAN ZNA A POUZIVA JE MOZNE ZE JE VE VIDNI U DVORA POUZIVAJI TAKE STEPAN TAKE TVRDI ZE VYMYSLI SIFRU KTEROU NEBUDE MOZNE ROZLUSTIT O TOM OSTATNE MLUVIL JIZ PRED LETY KDY JSEM SE S NIM SEZNAMILA NEVIM PROTO ZDA JE TO PRAVDA NEBO JEN JEHO VELKE PRANI NECHALA JSEM SI JI UKAZAT A VYSVETLIT JEJI PRESNY POPIS VCETNE KLICE ZASILAM STARYM KODEM TENTO NOVY JE JIZ ZASIFROVAN STEPANOVOU METODOU DOUFAM ZE PREDCHOZI DOPIS DORAZIL A TENTO DIKY TOMU BEZ PROBLEMU DESIFRUJETE PENIZE MI POSLETE JAKO OBVYKLE KLEMENTINA

Šifrový text (DOPIS):

CFHHZ TJMNL DUUTZ LFAVL FWLZT HPAMD TUNBY VGEVU DHGIR BMNEG
XLSDO TGSTW ECYCH PACYE HRBXW GSMLL LZQNX BZQBT RHAVP HCWOZ
JZSTH VTQCU YSTXZ CKTSD TCZJN BHFNJ PLXPN GUJVT ZQVMW LJLMV
XHJGS YSVGZ UOOTO CAVMX REAGY WEQLR SDIGY XTICN CWPGC BTRDD
CODYB KNRJI BMIJR TTVGY SIOAL MBBUX

GUPDH HNAZD BYOWA IVFIG MHZKF TSIVR CDVTC UJGLY UYCNB JTTDL
ETAQM LIFFU MLNZR RYEVZ JRBAJ SVGVJ QNMUE WSTME ICKWT SCRIL
AWQCG CBMOA ERGCW OMLNL NPRGN XYXQJ XVTCS SYOSB JVXEA RCNLP
PSKML YTHDT GCUNI ZLVJK UMPVX MZLZT ROURH IHOCE SEOMM KMAYP
HVXTA DIQWL MAPXL MZSNP DQOES PQURH CAGSK YGYRS DYYRI ECPRB
NYOSU YIRMO PYJCS MVSZA ZSOHX JXWKX MVUCN HLKJR VZVYI GSFBP
HECSE EGFNG NIAFY VGCAO EOQRK GVYYV MFWBA HAYII METBR SNLZL
HZAZO FYEKK EKPLO YUOFN OGGZK CHKOV GMAUE QOINB SMXRN RABJV
LXMVU XHBTP FFAGO EEWFP DESFH DYIFR NSXME PHLIN UNDYD GTCEG
RCUOR YILFM DSTNH MDJSB SRMLE CCCHI BDJNC XVXMA OGZZP ZYCBQ
DPTKW MSCYE ARPPC BQVLO YRTZT RRBAO DALQF KEWZH NFTMP AEKIY
PHBRA DTAQG ULSSN RCCNU DMHRV YUPFL GDSCO JMHCC SPMIO NXXCC
FAWFD PSNTP YCCBQ DPDNB WFCGS CHECM LJKWQ YYIQE KTTVA YLBHT
EDGGI ONNME OYBIB OLKPA DFZJQ ALRXT CXUUY KEUVJ FPGOU YKMKW
VYYLV NIXPH ZLGIO MGQPL QNMEU YYBIW QDCAZ QLNHT NGMVK DNQBB
MUAEI DSBAS TEKCW EMWQR HHDHS EAEOG ZBXEJ AMRIG ALIIY QGUFE
EZTQM NFGMT SNJAG SDDWB XEMWN XHPER PUDQN GFJZW GMLQF AEIHW
KMUWR RFYCF LJLPB TQEYP VXAXR SJTCN SVGAM LFELR NMXLM NXXMM
HKFRQ HVECC WBJMA GHCAI PPUSU DZFGJ OJWGG VAIQG OFVKZ LRHVM
UWEIF WURIF MGSND WMFLX WXWQZ UCUUA TNPDW MGGGB YKMGD EQOFM
KNMEX NRNMW OWGQT WGKMP WNCCC MVTUA DMHES JBYGA YKYFC FMGOV
XOYWN NRIPO XHTGR GRXHZ LCVWB UDXJZ SSCOE GXABY GGMFV SLUWI
QTTBP FENSE EJWSV TWEFI CECIL EFKTO KEVRG RSOHM EISFL PONRQ
SOEWU U

Vigenérova šifra
Délka textu: 1156
Délka klíče: 115
Klíč: OBLOHUVYSOKYMCREAVITKDOKOLIPRACOVALMUSIMMLUVISTUDENTNIKDYCHCEZ
AVERECNOUABYBARONEZNAMENAPAMATCEASTRYCISETYDNUVALECNE

Text závěrečné úlohy:

```
CFHHZ TJMNL DUUTZ LFAVL FWLZT HPAMD TUNBY VGEVU DHGIR BMNEG XLSDO TGSTW
ECYCH PACYE HRBXW GSMLL LZQNX BZQBT RHAVP HCWOZ JZSTH VTQCU YSTXZ CKTSD
TCZJN BHFNJ PLXPN GUJVT ZQVMW LJLMV XHJGS YSVGZ UOOTO CAVMX REAGY WEQLR
SDIGY XTICN CWPGC BTRDD CODYB KNRJI BMIJR TTVGY SIOAL MBBUX GUPDH HNAZD
BYOWA IVFIG MHZKF TSIVR CDVTC UJGLY UYCNB JTTDL ETAQM LIFFU MLNZR RYEVZ
JRBAJ SVGVJ QNMUE WSTME ICKWT SCRIL AWQCG CBMOA ERGCW OMLNL NPRGN XYXQJ
XVTCS SYOSB JVXEA RCNLP PSKML YTHDT GCUNI ZLVJK UMPVX MZLZT ROURH IHOCE
SEOMM KMAYP HVXTA DIQWL MAPXL MZSNP DQOES PQURH CAGSK YGYRS DYYRI ECPRB
NYOSU YIRMO PYJCS MVSZA ZSOHX JXWKX MVUCN HLKJR VZVYI GSFBP HECSE EGFNG
NIAFY VGCAO EOQRK GVYYV MFWBA HAYII METBR SNLZL HZAZO FYEKK EKPLO YUOFN
OGGZK CHKOV GMAUE QOINB SMXRN RABJV LXMVU XHBTP FFAGO EEWFP DESFH DYIFR
NSXME PHLIN UNDYD GTCEG RCUOR YILFM DSTNH MDJSB SRMLE CCCHI BDJNC XVXMA
OGZZP ZYCBQ DPTKW MSCYE ARPPC BQVLO YRTZT RRBAO DALQF KEWZH NFTMP AEKIY
PHBRA DTAQG ULSSN RCCNU DMHRV YUPFL GDSCO JMHCC SPMIO NXXCC FAWFD PSNTP
YCCBQ DPDNB WFCGS CHECM LJKWQ YYIQE KTTVA YLBHT EDGGI ONNME OYBIB OLKPA
DFZJQ ALRXT CXUUY KEUVJ FPGOU YKMKW VYYLV NIXPH ZLGIO MGQPL QNMEU YYBIW
QDCAZ QLNHT NGMVK DNQBB MUAEI DSBAS TEKCW EMWQR HHDHS EAEOG ZBXEJ AMRIG
ALIIY QGUFE EZTQM NFGMT SNJAG SDDWB XEMWN XHPER PUDQN GFJZW GMLQF AEIHW
KMUWR RFYCF LJLPB TQEYP VXAXR SJTCN SVGAM LFELR NMXLM NXXMM HKFRQ HVECC
WBJMA GHCAI PPUSU DZFGJ OJWGG VAIQG OFVKZ LRHVM UWEIF WURIF MGSND WMFLX
WXWQZ UCUUA TNPDW MGGGB YKMGD EQOFM KNMEX NRNMW OWGQT WGKMP WNCCC MVTUA
DMHES JBYGA YKYFC FMGOV XOYWN NRIPO XHTGR GRXHZ LCVWB UDXJZ SSCOE GXABY
GGMFV SLUWI QTTBP FENSE EJWSV TWEFI CECIL EFKTO KEVRG RSOHM EISFL PONRQ
SOEWU U
```

Poznámky k luštění (markanty, nápovědy apod.):
Systém byl dostaečně přesně popsán v doprovodném textu. Luštiteli proto stačilo podle tohoto návodu pouze postupovat. Prvý klíč periodické šifry lze z doprovodného textu odvodit, druhý klíč pak uživatel odovodí z vyluštěné prvé části úlohy.

E. Z poznámek soutěžících

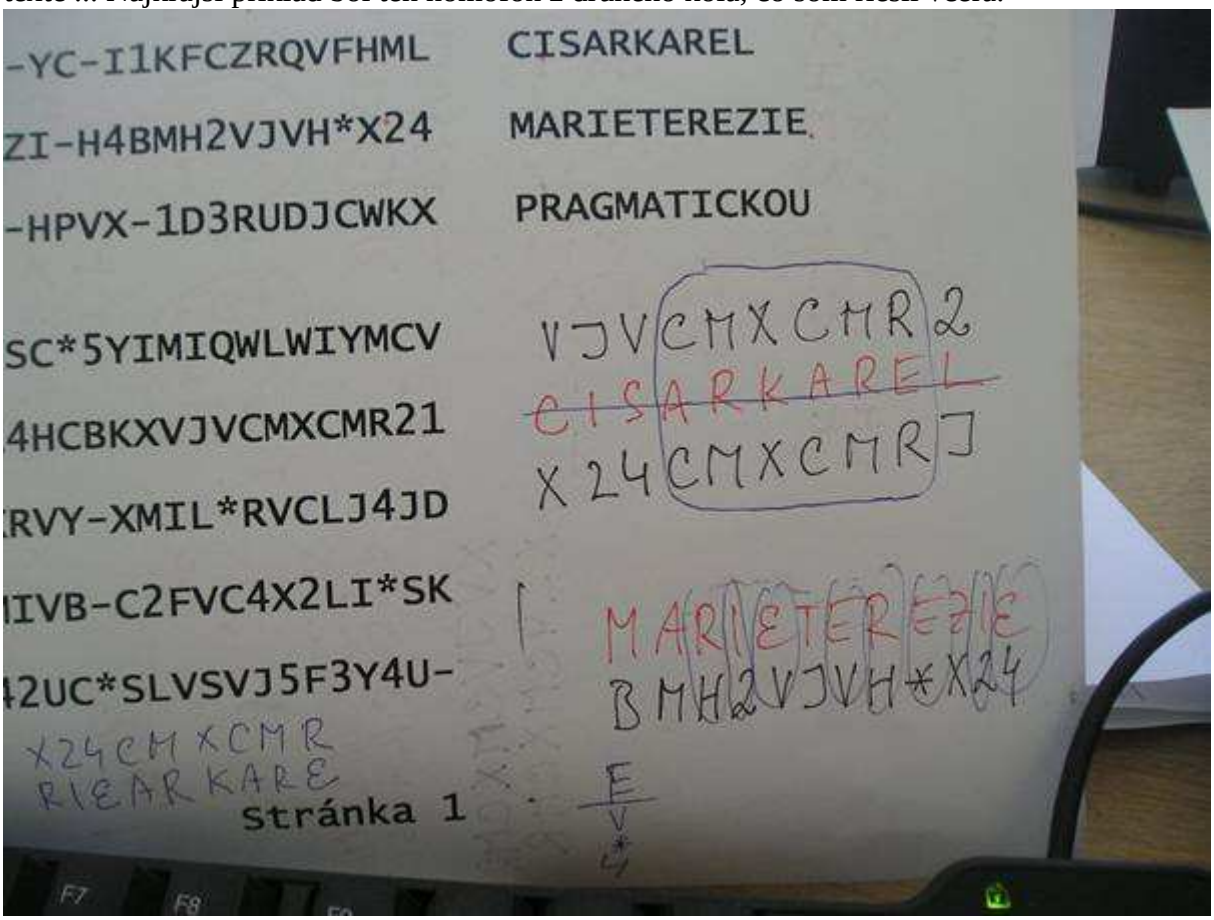
Z e-mailů soutěžících, doprovodné fgotografie F.Půbal.

Dobrý večer,
jak tak koukám na výsledky opravdu bylo třeba spěchat. **69 sekund** je neuvěřitelně malý rozdíl a 10 min na třetí místo to je teda bomba. Je vidět , že soupeři jsou stále kvalitnější, ale my jsme měli i tu pověstnou kapičku štěstíčka. A navíc mí dneska vypomohl kolega Libor Červený protože měl odpolední a nebyla žádná závada. Takže room132nakonec v rozhodující chvíli zafungoval :-)
Jinak poslední úloha super hned jak jsem četl o 20 slovech a spočítal úlohy tak to bylo jasné. Ale měli jsme to opravdu o FOUS.
Zdraví Josef Míka

Dobry vecer,
tak tohle kolo bylo opravdu super. Druhou ulohu se mi podarilozlomit jako prvni (sice celkem kuriozne ale prece- clovek musi mit istesti) a kdyz jsem se kouknul prevodovou tabulku, tak jsem si rekl, zeto asi bude podobne i u ulohy 3 :-). Takze jsem zkusil asi 2 kombinace a pak to vyslo. Uloha 4 .. hmm - 3 druhy znaku, 27 znaku od kazdeho druhu, zkousel jsem lecos, ale marne, po zverejneni napovedy to byla otazka chvilky. Jako obvykle Rail fence neresitelny problem bez znalosti systemu. Ze je to transpozice bylo celkem jasne, ale nějak ta sifraopravdu "nezapadla" do hlavy. Po zverejneni napovedy 5-ti minutova zalezitost, ale stejne se stydim, pohoret na takove prkotine.
Moc setesim na epilog a posledni ulohu.

Dobry den!

… No aby som bol uprimny aj ja pouzivam program CryptoTool. Je to vyborny free nastroj. Pouzivam ho na zistovanie frekvencie znakov, bigramov, trigramov. Cize kazdu ulohu najprv prezeniem tadial a zistim ci sa jedna o transpoziciu, alebo substituciu. Toto ma ten program dobre prepracovane - pekne to zobrazi kazdy znak, pocet vyskytov a percentualny vyskyt v texte. Je to urcite lepsie ako ratat to rucne na papieri. Okrem toho dokaze ten program takmer so 100% ucinnostou riesit vigenerovu sifru, pokial je pomer sifroveho textu ku heslu dost velky. Takze vigenera a beaufird-vigenera som lustil pomocou toho. Problem tam bol s jednou z tych sifier, pretoze program zle odhadol periodu (tusim hadal 3). Ale v napovede bola zverejnena dlzka hesla 7 a ked som mu zadal, ze heslo je dlzky 7, okamzite som mal otvoreny text - ak by som nebol prispaty, tak som aj sam mohol skusit dlzky trebars od 2 do 10, pretoze typ sifry som uhadol uz davno predtym. Takze tolko pokial ide o moje pocitacove lustenie. Inak vyuzivam pocitac na pisanie textov - nepisem si to na papieriky ako bolo na tej fotke :-). Napr. substituciu som robil tak, ze som v obycajnom textovom editire (joe pod linuxom) zamienal pismena: male boli sifrovy text, velke otvoreny a skusal som co vznikne. Podobne transpozicie - tam som si napisal text do prislusnej tabulky a menil riadky, resp. stlpce. Takisto sa mi to zda rychlejsie nez papier. Podobne aj tie zvysne ulohy som robil rucne s tym, ze pocitac nahradzal papier. Inak co ma prekvapilo bolo, ze dost velku cast uloh som tento rok zvladol utokom so znalostou otvoreneho textu - proste som uhadol nejake to slovo v texte ... Najkrajsi priklad bol ten homofon z druheho kola, co som riesil vcera.

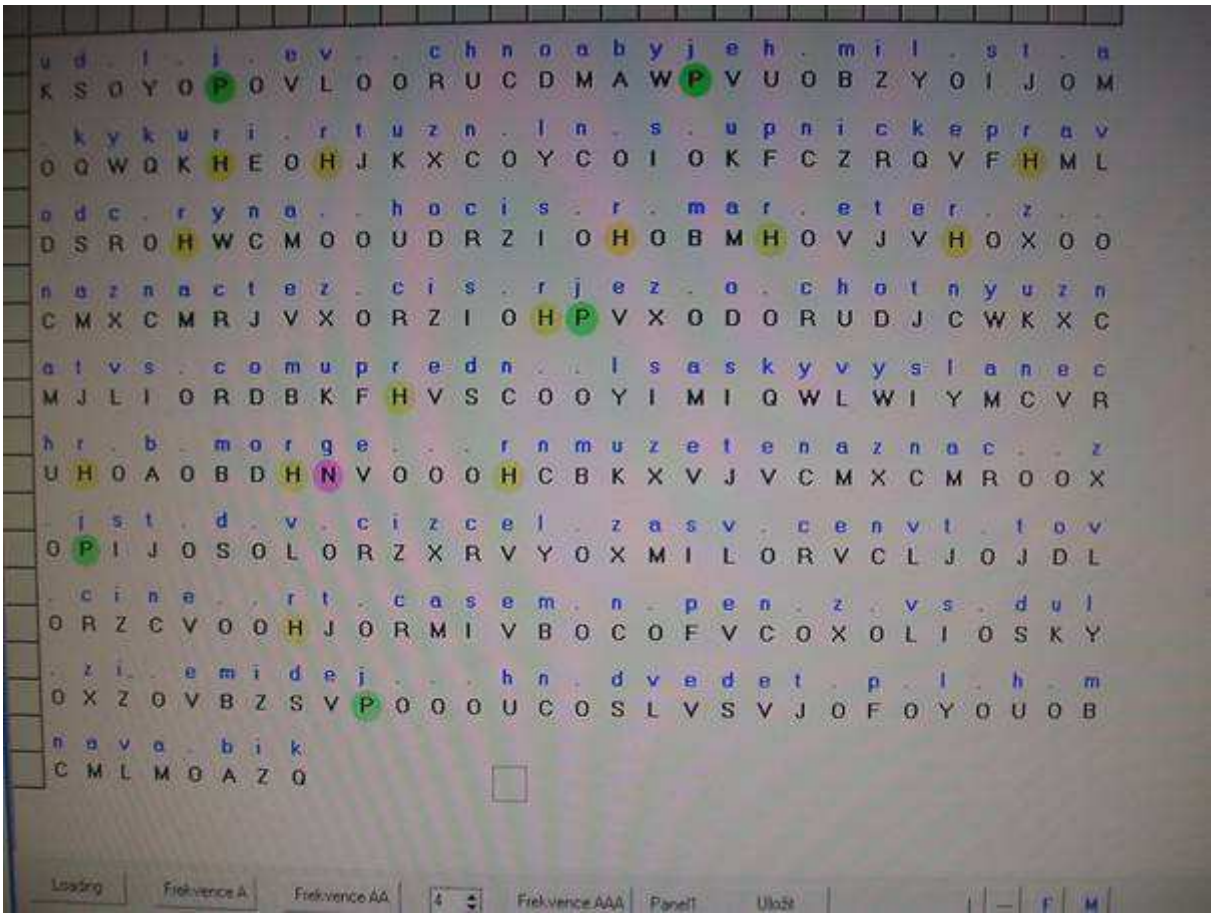


Cezara, augusta a vsetky taketo rotacne sifry program CryptoTool zvlada takisto takmer so 100% ucinostou. A to bez ohladu na jazyk, podobne ako vigenera. Ta latincina ma nijako nezarazila ani neprekvapila. Po latinsky trochu rozumiem a volakedy ako student som organizovaval maticke sustredenia pre stredoskolakov, kde v ramci GrandPrix dost casto byvali "pseudosifry" typu latinsky text napisany odzadu a pod. V case komunizmu bolo romanticke vidiet tlupy stredoskolakov ako sa nahanaju po nejakom mestecku alebo dedine a

zhanaju najblizsieho farara :-) CryptoTool som pouzil este aj pri tom homofone z tretieho kola. Tam som na Vasu radu pomocou napovedy (TRETIA verzia textu) zmenil homofonnu sifru na jednoduchu substituciu. Program CryptoTool dokaze automaticky riesit jednoduchu zamenu len pre anglictinu a nemcinu. S cestinou a slovencinou ma velke problemy a vacsinou neda ziaden rozumny vysledok. Mne sa to moc riesit rucne nechcelo, pretoze jednoduchu zamenu povazujem za velmi pracnu na riesenie, tak som to len tak skusil, ci nahodou motyka nevystreli. A vystrelila! Ako vzorovy text (pre program CryptoTool) som pouzil Babicku od Bozeny Nemcovej. Vacsinou to nefunguje - okrem ineho aj preto, ze texty do sutaze volite dost "nestandardne" - to nie je kritika, ale chvala :-) Ale tentoraz Babicka zabrala a mal som okamzite otvoreny text. Inak by som to asi ani nebol riesil... Inak este tam je jeden hacik - bigramy a trigramy. Ono ten program vyzaduje aby boli medzery tam kde maju byt. No potom by to aj rucne bola hracka. Inak su frekvencie bi- a trigramov dost nezmyselne, pretoze sa spajaju konce a zaciatky slov. Takze ja som aj tu Babicku upravil tak, ze som vyrazil vsetku interpunkciu, vsetky znaky su velke a vyhodil som vsetky medzery. Podobne aj v sifrovom texte najskor vyhodim vsetky medzery a az potom to spracovavam tym programom, aby frekvencie vzoru a lusteneho textu aspon ako-tak sedeli. Mozno to nie je moc vedecky postup, ale co uz...

Uz sa tesim na buduci rok. Vasa sutaz mi kazdorocne sprijemnuje inak velmi neprijemnu jesen.

So srdecnym pozdravom Jozef Kollár



Dobry den,

Dekuji za blahoprani, bohuzel se musim priznat k podvodu.

U ulohy III/1 jsem vedel, kde najdu otevreny text (Wikipedia, heslo Karel VI). Reseni uloh III/2 a III/5 jsem ziskal pri reseni posledni ulohy (manipulaci s heslem pro Vinegere).

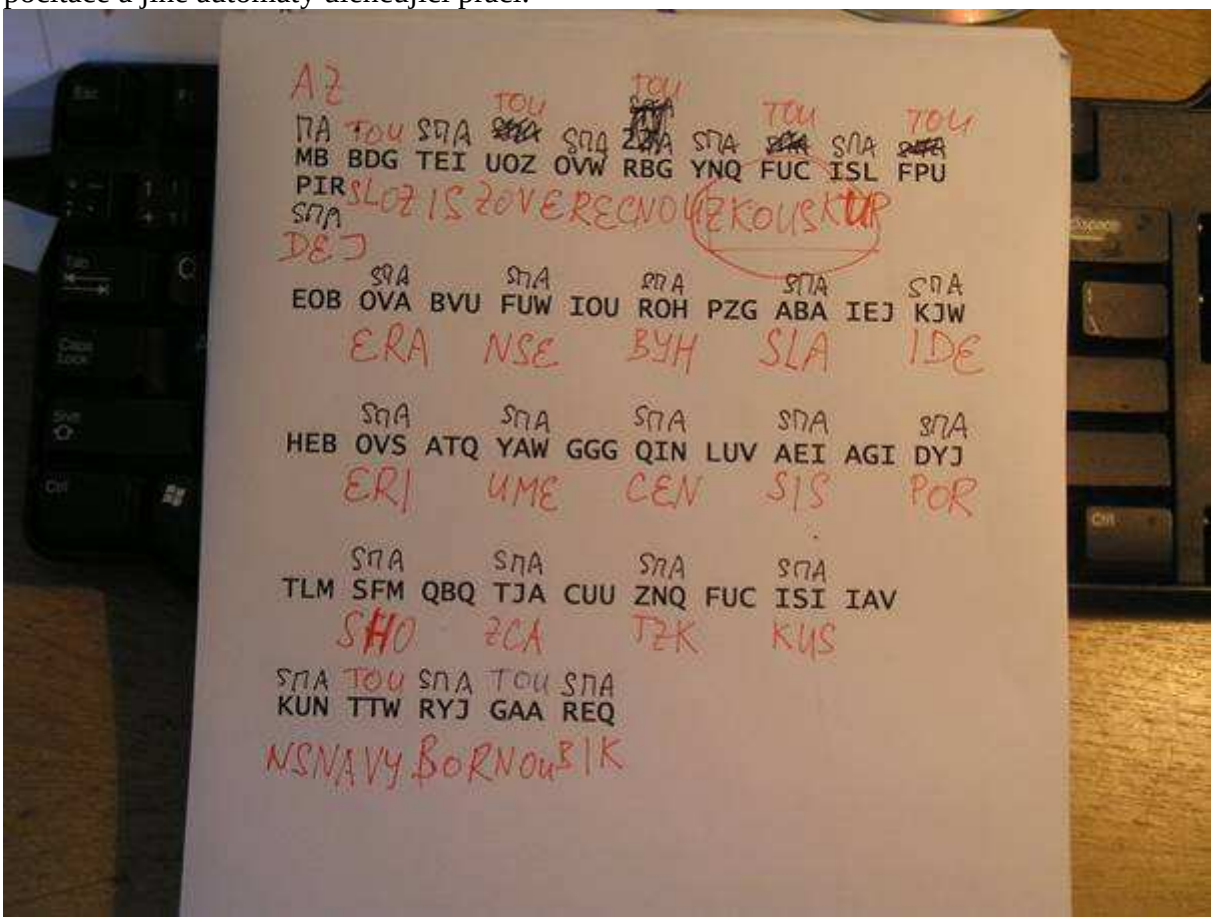
Moc dekuji za skvele pripravenou soutez, uzil jsem si hezkych par veceru zmitaje se mezi beznadeji a euforii.
S pozdravem David Hofbauer

Dobry vecer,
dekuji za blahoprani a hlavne za celou soutez!!! Podal jste (tak jako jiz obvykle) velmi dobry vykon!!! (hi hi) Letos mne nejvic potesil dopis carevny Kateriny (i kdyz to, jak se vyjadrila o "nasi" MT, to bylo na facku). Snad proto, zze se mi podarilo pouzit metody predpokladaneho slova a jeji realizace... Ale ten prusky kurfirt!!! Ten mi dal zabrat - popsal jsem nejmene dva baliky papiru. Skocil jsem vam totiz pekne na spek, spocital jsem si ze velkych pismen v textu je 17, v "napovedne" tabulce je homonymu taky akorat presne 17, cili je to jasne, jde se na vec, a stale jsem rouboval bigramy na velka pismena....v malych pismenech jsem se zase nemoh' usadit "u" , inu tezko, kdyz tam nebylo A jeste - kdyz jsem mel uz vsechna klicova slova pro K. dopis, tak jsem si z jakehosi duvodu myslel, ze to by jste prece nenechal uplne stejne, jako v pripravne fazi, to jsem si vzal do hlavy a asi 3 hodiny jsm klicova slova sestavoval podle abecedy, podle poctu znaku v nich, stale nic nevychazelo, pak jsem si z hruzou uvedomil, ze pisete, sestavte klic ze tretich slov, asi tedy v normalnim poradi, ale nebudou odzadu ?????, atd atd.. pak jsem se vzpamatoval a skusil jsem to nejjednodussi, tam se mi libilo ze jste pouzil pro kontrolu 6. slovo odzadu - inu penize jsou vzdy az na prvnim miste...
Co kategorie "brk a kalamar " ???? tak jeste jednou dekuji, a zaroven se omlouvam za trosku emocionalni. majl (dusledek lusteni...) a ted jdu sebrat ty hromady papiru po celem byte, to by mela mistni sberna papiru trzbu, ovsem, kdyby tu nejaka byla... Dekuji a hezky vikend !!!! 73!!! Frantisek, 7X0RY..... (Key No 9)

Zdravim,

Hm, tak jsem to asi napsal nejasne ale ulohu 1/3 (auhustova sifra) jsem lustil takto nagenerovanim vsech posunu a zkoumanim vysledku (spravny posun to je tusim o 25 a vychazi tak pak "INPQINCIPIOCQEAVITDEURCAELUMETTEQQAMTEQQAAUTEMEQATINANIR...", kde DEUR zni divne, ale "IN PqINCIPIO" primo rika, posun Q na R a pak analogicky R na S... - dodatecne az po uspesne odpovedi DEUS overeno jeste scb solverem jako jednoducha zamene v latine) …

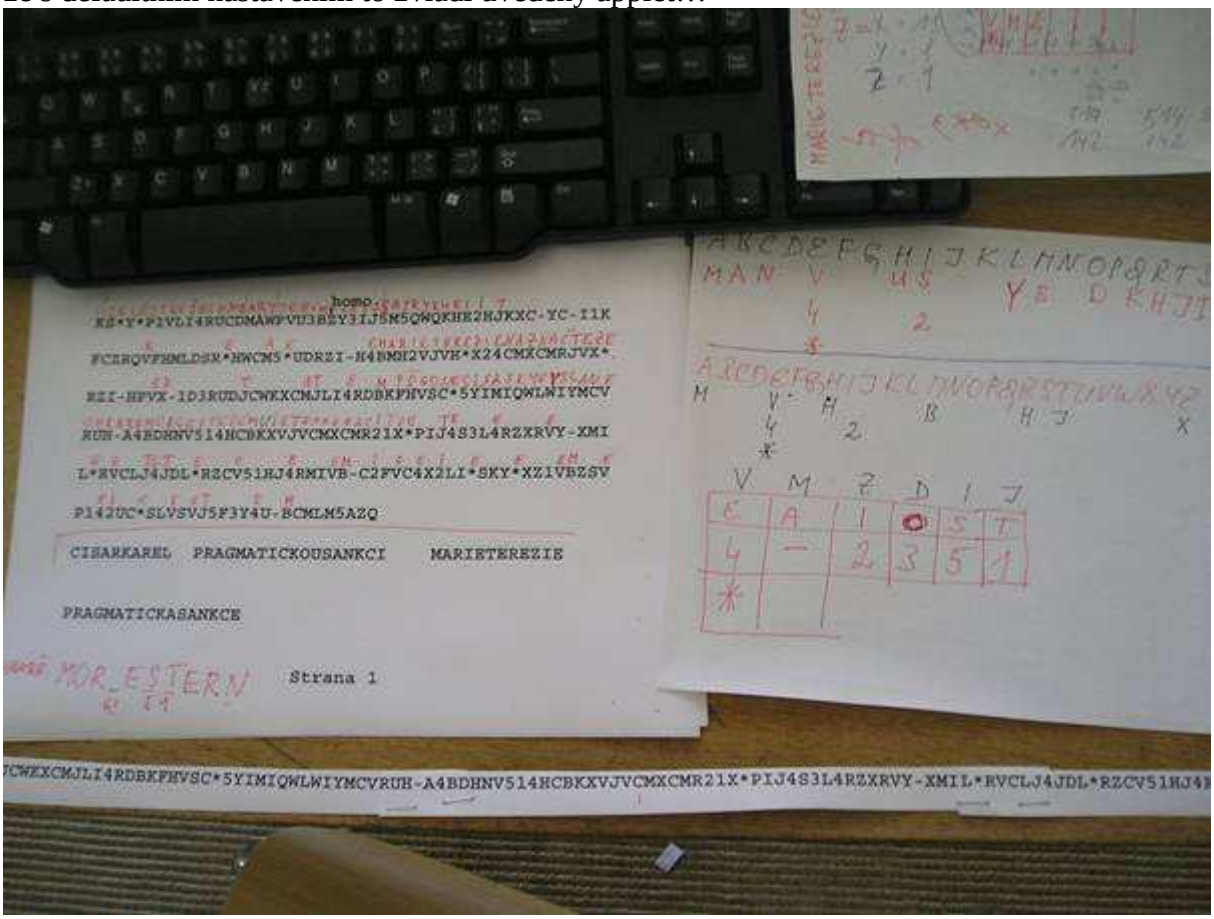
Tomuhle rikam vydrena sifra ;-) A musim do pristiho roku najit lepsi, nebo si napsat, nebo aspon upravit SW na reseni homofonnich sifer. Protoze to co mam kdispozici je bida. (uvedeny ceckovy, pak jeste jeden nefunkcni javovej (http://www.cs.umbc.edu/~stephens/crypto/SOFTWARE/Homophonic.java) - aspon ja honepresvedcil k fungovani).
Skutecne obdivuju lustitele z dane doby, ale vubec i ty do 40-50. let 20. st, kdyz nebyly pocitace a jine automaty ulehcujici praci.



Třetí varianta šifrového textu obležení Prahy ... nejak mi unika 2. varianta
Kazdopadne dekuji za skvelou zabavu na dlouhe (a jak koukam na hodinky, tak az trochu moc ;-)) vecery. Trochu me mrzi, ze letos vubec nebyla steganografie, ale zase na druhou stranu, ocenuji na soutezi to, ze jsem se dokopal napsat si vlastni devignerator a par dalsich uzitecnych skriptu (php), za rok to pujde zas o neco snaz a rychleji.

- ad sifra 3/4 (z bad ischlu)
IC mi ukazalo na cestinu, takze jsem zavrhl ruzne zameny. Transpozice jakkoli nevychazela a pritom jsem v doprovodnem textu nezavadil o nic co by mohlo ukazovat na heslo. Pro mrizku (kdyz by otocenim nepokryla vse) by bylo od vas osklive tam zbyla pismena nahazet tak, aby

to odpovidalo frekvencim pro cestinu. Takze i mrizku jsem prozatim (a jak se ukazalo naporad) zavrhnul. Takze jsem hledal sifru aspon priblizne z te doby, k jejimuz vylusteni netreba heslo, ale max. nejaka snadne nastaveni marametru. Takze jsem si proklikal jeden ze SW,
ktere pouzivam (http://members.aon.at/cipherclerk/CipherClerk.html) a dogooglil u sifer, ktere nepotrebovaly heslo a pripadaly v uvahu, ze kdy pochazeji. Pak uz to bylo spis o stesti, ze s defaultnim nastavenim to zvladl uvedeny applet…



- Softwaru pouzivam docela dost, postupne rozsiruji sbirku. Na monoalfabeticke sifry je naprosto perfektni scb solver (http://secretcodebreaker.com/scbsolvr.html) a i dalsi sw z daneho webu neni k zahozeni a pokud se nepletu je vetsina free. Napr. word pattern. Je potreba si nagenerovat vhodne slovniky ci soubory s frekvencemi. Jako zdroj jsem loni pouzil asi 20MB plaintextu stenoprotokolu z poslanecke snemovny, ale uz to hadi na webu predelali, takze se da stahovat po malych castech (promluva 1 poslance), takze se asi da nejit lepsi zdroj bezneho textu. Po letosku mam i novy soubor s frekvencema pro latinu ;)… Dalsi uzitecny je ten vyse uvedeny cipher clerk. A pak uz jsou to ruzne utility napriklad na vypis delitelu. Na prepis transpozice do tabulky nebo na zakladni polyalfabetickou frekvencni analyzu se hodi (http://sifry.sourceforge.net/). A pak sada mych vlastnich jednoucelnych PHP skriptu, ktere jsou tak prasacky napsane a bez jakehokoli gui, ze jejich zverejneni by se asi nesetkalo s kladnou odezvou. Kdyz budu mit cas, ty nejlepsi (devignerator) asi zkultivuji, …

Gimli2

F. O čem jsme psali v prosinci 2000 – 2006

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

Crypto-World 12/2005

Crypto-World 12/2006

Příloha : Šifra Delastelle – BIFID.pdf

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@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/