

Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 12, číslo 11/2010

8. listopad 2010

11/2010

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.

Starší sešity jsou dostupné na adrese

<http://crypto-world.info>

(1376 registrovaných odběratelů)



Všechna práva vyhrazena. Tato publikace ani žádná její část nesmí být reprodukována nebo šířena v žádné formě, elektronické nebo mechanické, včetně fotokopií, bez písemného souhlasu vydavatele.

Obsah:	str.
A. Soutěž v luštění 2010 skončila ! (P.Vondruška)	2 - 3
B. Doprovodné příběhy k úlohám (P.Vondruška)	4 - 8
C. Soutěžní příklady roku 2010, použitý systém, dešifrované texty (P.Vondruška)	9 – 28
D. Ohlasy, připomínky a komentáře soutěžících	29 - 33
E. Mikulášská kryptobesídka /Santa Cryptt 2010 / Program	34 -35
F. O čem jsme psali v listopadu 1999-2009	36 - 38
G. Závěrečné informace	39

A. Soutěž v luštění 2010 skončila!

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

Soutěž v luštění 2010 (<http://soutez2010.crypto-world.info/>), která byla doprovázena fiktivním příběhem z života Giacomo Casanovy, konkrétně s přípravou a zničením jeho knihy Tajnosti mého života (Secrets de ma vie) skončila. Možnost vkládat správné výsledky řešení jednotlivých úloh byla uzavřena 7. 11. 2010.

Ceny (<http://soutez2010.crypto-world.info/index.php?crypto=ceny>) získali první tři řešitelé a dále tři řešitelé, kteří byli vylosováni ze 37 soutěžících, kteří dosáhli více než 15 bodů (limit pro zařazení do losování).

Stručná statistika letošní soutěže:

Úlohy

Celkem publikovaných úloh: 15

Maximální počet bodů za publikované úlohy: 50

Celkem soutěžících: 80

Počet soutěžících, kteří vyřešili aspoň 1 úlohu: 64

Počet soutěžících zařazených do slosování: 37



Všechny úlohy letos vyřešilo celkem 19 soutěžících !:

elpepe73, ony, SHA3, Bob, paulie, peddy, Mirop, Hnizdo, MD5Mir, mim3, fantasy, CASA-NOVA, Jahoda, Bobo, hodiny, Frajer, kasparov2, PackalJ, koc

Pořadí na prvních třech místech:

1	elpepe73	50	26.10 (00:10)
2	ony	50	26.10 (00:55)
3	SHA3	50	26.10 (01:10)

Vylosování soutěžící, kteří dostanou cenu:

8	Hnizdo	50
18	PackalJ	50
23	Zvedavec	37

Všem úspěšným řešitelům blahopřeji!

Sponzoři letošní soutěže:

- TNS (Trusted Network Solutions), <http://www.kernun.cz/>
- BUSLab (Brno University Security Laboratory), <http://www.buslab.org/>
- Zoner Press, <http://www.zonerpress.cz/>
- Autor soutěže, <http://crypto-world.info/oko/index.php>



Prvních pět řešitelů jsem zapsal do vedeného přehledu nejúspěšnějších řešitelů podzimních soutěží. V tabulce je uveden každý, kdo získal v roce 2003-2010 alespoň jedno páté místo. Tabulka je seříděna abecedně.

Přehled na 1. až 5. místě v letech 2003-2010								
Crypto-World	2003	2004	2005	2006	2007	2008	2209	2010
alchymista			3					
Bigbaz					5	5		
Bob							5	4
brubaker		2						
crcker				4				
CyberMage	1							
Dave		4						
elpepe		3						1
gimli2					4			
Jehova							2	
jmkollar					2		1	
kesy							3	
koc						3		
MD5Mir				3	3	2		
misof		1	1					
ony						1	4	2
paulie								5
peta007	2			2				
pierre			2					
rhorecek						4		
rkb	4							
room132			4	1	1			
SHA3								3
Stanislaw		5	5	5				
tnt	5							
xnovakv	3							

B. Doprovodné příběhy k Soutěži v luštění 2010

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

Úvodní doprovodný příběh byl společně s životopisem Giacomo Casanovy a Jana Josefa Kittela zveřejněn již v **e-zinu Crypto-World 9/2010**:

Giacomo Casanova - Tajnosti mého života (Secrets de ma vie)	8 – 10
Giacomo Casanova - Příběh mého života (Histoire de ma vie)	12 – 17
Jan Josef Antonín Eleazar Kittel	18 – 19

Dále byly v tomto čísle uveřejněny i doprovodné texty k soutěžním úlohám 1, 2 a 3.

Úkoly z šuplíku – Kittlův dopis	10
Úkoly z šuplíku – Lóže Svobodných zednářů	11

Další doprovodné příběhy včetně úloh byly zveřejněny v **e-zinu Crypto-World 10/2010**.

Najdete zde

C2. Úkoly ze šuplíku – Adelaide de Gueidan	str.14
C3. Úkoly ze šuplíku – Francesca Buschiniová	str.15
C4. Rekapitulace 1	str.16
C5. Cesta do Ruska	str.17
C6. Madam de Urfé	str.16
C7. ICOSAMERON - písmo Megamikrů	str.19
C8. Tři šifry z let 1765 - 1767	str.20
Nová mise – zpráva 1	str.20
Mise v Polsku - zpráva 2	str.21
Jan Josef Kittel - zpráva 3	str.22
C9. Stín hraběte Branického	str.22
C10. Adelaide de Gueidan podruhé	str.23

Z tohoto důvodu v tomto čísle již jen doplníme zbývající doprovodné příběhy k posledním soutěžním úlohám (č. 14 a č. 15) a to včetně zveřejněné nápovědy a celkovou rekapitulaci.

C1. Rekapitulace 2

Giacomo se rozhodl, že má připraveno již dostatek materiálů pro svoji připravovanou knihu *Tajnosti mého života*. Přemýšlel nyní, jak zašifrované texty třídit, zda podle let nebo propojit nějakým výkladem nebo propojit příběhem ze svého života nebo zda bude materiály třídit jiným způsobem. Začal tím, že si je označil a setřídil podle šifrových systémů, které byly použity.

1-3) Tři zástupci naivních šifer - sem Giacomo zařadil **Kittelův dopis** psaný jeho slabou italštinou a zašifrovaný tím nejjednodušším způsobem a pak také další Kittlem zašifrovaný text z doby, kdy se u něj Giacomo léčil. **Kittel použil šifru**, kterou sám vymyslel. Jednalo se o jednoduchou dynamickou úpravu Caesarovy šifry.

Se zařazením dopisu **Francesci Buschiniové** měl problém. Francesca použila najednou hned dva jednoduché systémy, které od Giacoma znala. Jednak naivní systém a jednak jednu z neznámějších a nejjednodušších verzí jednoduché záměny.

4) **Tajný inkoust + naivní šifra** – do této kategorie zařadil Giacomo dopis, který jej zastihl v Šumburku, kde se léčil se svojí zraněnou paží u známého léčitele Jana Kittela.

5) **Jednoduchá záměna** – grafická abeceda, základní šifra, kterou používali v Lóži Svobodných zednářů v Lyonu a se kterou jej seznámil hrabě Henri Gaspard de Gueidan.

6) **Homofonní šifra** – zástupce této šifry byl dopis **od Adelaidy**. Adelaida svoji převodovou tabulku nesestavila příliš šikovně. Nejprve si připravila tabulku jednoduché záměny a pak pro šest samohlásek jednoduše přidala homofon. Tyto přidání homofony byly číslice 1-6.

7) **Homofonní šifra s dělbou na slova** – do této kategorie zařadil Giacomo písmo Megamikrů ze své knihy ISOCAMERON.

E
o
o

8-9) **Periodická šifra** – zašifrovaný text, který použil hrabě **Henri Gaspard de Gueidan** když jej zasvětil do tajemství Lóže a předvedl mu, jak lze takovou šifru poměrně snadno vyluštit.

Druhým zástupcem (Beaufortova varianta) byl dopis, který mu ukázala **markýza Jeanne de Urfé** a který k jejímu velkému údivu dokázal vyluštit.

10) **Úplná transpozice** – dopis z podzimu roku 1764, na základě kterého se rozjel na svoji dlouhou cestu do Ruska.

11) **Cardanova mřížka** dopis z podzimu roku 1765, na základě kterého odjel z Petrohradu do polského Krakova.

12) **Fleissnerova mřížka** – zašifrovaná zpráva z roku 1765 s příkazem k velmi nebezpečnému úkolu. Soubojem s hrabětem Branickim

13) **Knižní šifra** - dopis hraběnky Adelaide de Gueidan. Klíčem byl text, který znali jen oni dva. Giacomo považoval tuto šifru za nejlepší ze všech, které měl ve své sbírce.

C2. Zednářská lóže 3

Na jaře roku 1798 se Giacomo Casanova cítil již velmi sláb a unaven. Cítil, že je na konci své cesty. Pomalu se smiřoval s myšlenkou na svoji smrt. Vyřizoval své záležitosti. V literárně hodnotných dopisech, které rozeslal svým známým a milým, se vyznává ze svého přátelství a lásky k nim a k lásce k životu. Vybízí je, aby žili tak, jak jim velí čest, rozum a cit. Na závěr dopisů pak připomíná, že svůj život nepromarnil a snažil se jej žít tak, aby byl nápomocen jiným. Upozorňuje na svoji knihu *Příběh mého života (Histoire de ma vie)*, kde popsal to, co mohl ze svého života prozradit, aniž by tím ublížil jim nebo někomu jinému.

Na závěr pak naznačuje, že chystá ještě jednu knihu, která se zabývá tajemstvími, která často s nimi sdílel, ale za svého života je nevyzradil. Doufá, že jeho knihu někdo po jeho smrti najde a vydá. Nechce však, aby to bylo dříve než 50 let po jeho smrti, aby tím nikomu z nich neublížil.

Poté co rozeslal tyto dopisy, otevřel šuplík s podklady pro svoji poslední knihu, kterou chtěl nazvat Tajnosti mého života (Secrets de ma vie). Prolistoval zde uložených třináct šifrových

textů a rozhodl se, že materiálu má již dost a začne je opatřovat komentáři a vysvětleními, a to včetně popisů použitých šifrových systémů.

Pomyslel si: „Snad Bůh ve své milosti mi dá čas a sílu, abych toto své poslední dílo dokončil a někdo jej zde na Duchcově našel a vydal.“

Potom vzal list čistého papíru, namočil péro do kalamáře a svým rozmáchlým rukopisem napsal:

Secrets de ma vie. Prosím nálezce, aby vydal rukopis uložený v tomto šuplíku jako moji poslední zpověď. Nejdříve však vydejte padesát let po mé smrti! Věřím, že moji poslední vůli nálezce vykoná.

Giacomo Casanova, Duchcov 4. dubna 1789.

To se stalo přesně dva měsíce před jeho smrtí.

Jenže osud tomu chtěl, aby sbírku uložených šifrových textů stačil ještě rozšířit. Asi za týden po této události přišel list od jeho známého českého kněze, knihovníka pražské univerzitní knihovny Karla Rafaela Ungara. Zpráva byla psána šifrou.

Karel Ungar byl významnou osobností českého království. Byl třikrát děkanem teologické fakulty Univerzity Karlovy a v akademickém roce 1789-1790 dokonce rektorem Karlovy univerzity. Jako takový byl i členem Veliké zednářské Lóže pražské a stal se dokonce i velmistrem Lóže. Ta pod jeho vedením v osmdesátých a na počátku devadesátých let 18.století prožívala nebývalý rozmach. Jenže pak přišla pro zednáře krutá léta. S nástupem císaře Františka na trůn byla jejich práce zakázána (roku 1794) a to především v souvislosti s obavami se šířením revolučních myšlenek z Francie. Byl to právě Giacomo, který zajišťoval komunikaci Lóže Pražské s francouzskou Lóží lyonskou, kde měl řadu přátel a také pomáhal s překlady některých spisů, které se díky němu mohly v Rakousku šířit. Během této doby se s Karlem Ungarem seznámil a spřátelil.

Nedočkavě se dal do luštění listu. Tušil, že se Karel Ungar nehodlal se zákazem zednářské práce smířit. Jistě to je důvod, proč je list zašifrován. Co však Karel chce, jak má bratrům pomoci?

I přes zkušenosti, které se šiframi a luštěním měl, mu tentokrát trvalo celý večer, než zprávu vyluštil.

Se svým výsledkem byl spokojen. Pak otevřel šuplík a uložil text mezi kombinované šifry.

Úloha č.14 Zednářská lóže 3

Šifrový text

Nakonec obnos puvab trochu rodopis relief rezba Glasgow. Nerv venku houf pivo svab drama elf ruze kyvadlo. Slib prepis pucet zapal postup. Tetrev Q krokus zpusob duvod hoboj. Dabel venku trumf jas Jakob. Rtut trumf objev dolozit ucitel zjev dvou. Relief odchod fiasko rozvoj. W ocenit puvab podzim slib dragoun. Dostup dav vsechno chlap W. Elf zad berni kongres pohyb. Potesen kov Q. Obrys krab premena dokazat azyl elf. Narizen Q vas Glasgow sidlo. Konvoj rameno relief vule trumf. Album carodej konzul W. Tarif cloveku kouzlo sestup W. Nakup priliv W relief. Predtim shon nastroj tajnost cemum Eros. W houf datum orloj sokol elf. Islam biskup laska trumf Q. Prinoshrob schuzka adresat kristal relief

C3. Zničení Casanovovy knihy o šifrách

Asi týden po té, co Giacomo obdržel dopis od Karla Ungara, přišel za ním hrabě Valdštejn. Po krátké nezávazné konverzaci přešel přímo k tématu, které jej zajímalo.

„Giacomo, také jsi obdržel list od pražského knihovníka Karla Ungara?“

Giacomo přisvědčil. Po chvíli otálení jej hrabě požádal, zda by mu jej neukázal.

A tehdy udělal Giacomo první chybu tohoto večera. Otevřel před Valdštejnem šuplík, šifru z něj vyjmul a podal mu ji.

Hrabě vyndal svůj list, který obdržel a ukázal jej Giacomovi. Konstatoval, že jsou zcela shodné.

„Jsou stejné. Mohu tě tedy s čistým svědomím požádat o pomoc s jeho dešifrováním. Obsah tím nebude vyzrazen nepovolané osobě.“

Giacomo hraběti prozradil, že již zprávu dešifroval a seznámil jej s obsahem. Hrabě, který byl také členem Veliké zednářské Lóže pražské až do jejího rozpuštění, mu velmi děkoval. Byl obsahem nadšen. Podívoval se však, že Giacomo dokázal šifru tak rychle vyluštit.

A tehdy udělal Giacomo druhou chybu večera a pravděpodobně i poslední chybu svého života. Zasvětil hraběte do obsahu své připravované knihy *Tajnosti mého života* a ukázal mu i texty, které do této knihy hodlá zveřejnit.

Giacomo netušil, co bude následovat.

Hned následující květnovou neděli se hrabě sešel s Karlem Ungarem a seznámil jej s tím, co Giacomu připravuje. Hrabě Valdštejn ho informoval i o tom, že se Giacomo chystá vyzradit některá tajemství své bývalé zednářské Lóže. Např. postup při luštění periodické šifry, ale také úpravu šifrování záměny „podle kříže“.

Karel Ungar tuto informaci probral s dalšími členy Lóže a na základě toho poslal hraběti šifrovaný dopis s úkolem.

Dopis hraběte zastihl 5. června v Duchcově, kam narychlo přijel z Teplic. Hrabě se totiž dozvěděl o skonu Giacoma Casanovy (4. června 1798) a chtěl osobně připravit a řídit jeho důstojný pohřeb. Valdštejn text dopisu snadno dešifroval. Nedělalo mu to velký problém, byla totiž použita šifra, kterou v Lóži běžně používali.

Úkol, který touto cestou obdržel, jej netěšil. Ale přesto se rozhodl jej splnit. Vešel do pracovny, kde večer před tím Giacomo v křesle skonal a šel k šuplíku s jeho rozepsanou knihou. Otevřel ji, přečetl si list, ve kterém Giacomo prosí, aby byl obsah publikován za padesát let. Smutně pokýval hlavou a řekl si, bratře Giacomo, omlouvám se, ale toto ti splnit nemohu. Pak šel ke krbu, kde slabě hořel oheň a celý obsah šuplíku do něj vyklopil.

Vzplál oheň, který velkými plameny navždy tato tajemství pohřbil v popelu...

Žádná ze čtrnácti šifrových zpráv, které Giacomo připravoval do své knihy *Tajnosti mého života*, se tak díky této události nedochovala. Ze všech patnácti šifrovaných textů, které se v tomto příběhu objevily, zůstal dochován pouze jeden jediný. Touto jedinou zprávou je dopis s úkolem, který hrabě Valdštejn obdržel od Karla Ungara. Je však samozřejmé, že jej nevložit do šuplíku, kde šifry a podklad ke své knize uchovával za svého života Giacomo. Z tohoto důvodu ji tam ani vy nemůžete najít. Předpokládám, že ji však snadno objevíte. Nemusíte kvůli tomu jezdit na Duchcov. Ostatně tato šifra tam již dávno není. Během těch dvou staletí

putovala z místa na místa od jednoho majitele k jinému. Současný majitel se rozhodl ji zveřejnit a tím uzavřít tento utajený příběh ze života Giacoma Casanovy ...

Úloha č.15 Zničení Casanovovy knihy o šifrách

Text úlohy

Zadna ze ctynacti sifrovych zprav, ktere Giacomo pripravoval do sve knihy Tajnosti meho zivota, se tak díky udalosti popsane v doprovodnem príbehu nedochovala. Ze vsech patnacti sifrovanych textu, ktere se v tomto príbehu objevily, zustal dochovan pouze jeden jediný. Touto jedinou zpravou je dopis s ukolem, ktery hrabe Valdstejn obdržel od Karla Ungera. Je vsak samozrejme, ze jej nevložil do supliku, kde sifry a podklad ke sve knize uchovával za sveho zivota Giacomo. Z tohoto duvodu ji tam ani vy nemuzete najít. Predpokladam, ze ji vsak snadno objevíte. Nemusíte kvuli tomu jezdit na Duchcov. Ostatne tato sifra tam již davno není. Behem tech dvou staletí putovala z místa na místa od jednoho majitele k jinému. Soucasny majitel se rozhodl ji zveřejnit a tím uzavřít tento utajeny príbeh ze zivota Giacoma Casanovy ...

C4. Rekapitulace 3

14) Kombinovaná šifra - Karel Rafael Ungar použil při zaslání pozvánky kombinaci dvou systémů. Nejprve text zašifroval jednou z nejjednodušších klasických šifer. Potom použil šifru, kterou bychom dnes nazvali agenturní šifrou a patří mezi nejjednodušší steganografické metody (výběr 1 písmena z každého slova). Při dešifrování je samozřejmě nutné postupovat opačně ☺.

15) Kombinovaná šifra - nejprve je nutno zašifrovaný text, která poslal Karel Ungar hraběti Valdštejnovi nalézt. Šifra během staletí doputovala až do Hradce Králové. Nemusíte tam však jezdit. Dá se vyhledat na našem soutěžním webu a to včetně klíčů pro dešifraci.

Při zašifrování byl nejprve použit zednářský jednoduchý kříž. Potom byly šifrové znaky periodicky pootočený. O tomto systému se dozvěděl Giacomo již v době svého vstupu do Lyonské zednářské Lóže (viz příběh Úkoly ze šuplíku 2 - Lóže Svobodných zednářů).

Šifrování bylo dokončeno použitím Fleissnerovy mřížky.

Při dešifrování je opět nutné začít opačně – tedy použít mřížku, postupovat pootočením znaků (ve správném směru) a převodem podle kříže.

Příběhy a kompletní doprovodné materiály k soutěži

Všechny doprovodné příběhy a materiály jsou a zůstaly dostupné na stránce soutěže zejména v sekci *příbeh* <http://soutez2010.crypto-world.info/index.php?crypto=příbeh>

C. Soutěžní příklady roku 2010, použitý systém, dešifrované texty Pavel Vondruška (pavel.vondruska@crypto-world.info)

Úloha č.1 Kittlův dopis

Šifrový text

HPESOJ ERACITNEMID IAM ORTOP NON KRUBMUS ELATAN ESEAP OIM LEN
IUQ ENOSREP EL ETTUT ID AIROMEM AL E AIROMEM AIM ALLEN ERPMS REP
ARRAMIR ERBMETTES A OSOIROLG ONROIG LEUQ OTSERRAD ATUTTAB ANU
REP INOIZADNAMOCCAR ID ESAB ALLUS EM REP ITTEFFE NI OIGGAIV OUS
LEN EROTAREPMIL EROTAREPMIL NOC OSSECCUS OIM ID ERALRAP E EM ID
IDROCIR IT EHC OTLOM OIZARGNIR AL OCIMA ORAC

Systém: Celý text psaný neumělou italštinou je napsán pozpátku

Upřesnění: testovací příklad pro uživatele

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (2 CZ) (druhé slovo, ale zadat česky)

Správná odpověď: PRITELI (=AMICO)

Body: 2

Otevřený text:

Milý příteli. Velice děkuji za to, že jsi na mne nezapomněl a promluvil o mých úspěších se samotným císařem. Císař se na své cestě skutečně u mne na základě tvého doporučení zastavil. Tento slavný zářijový den zůstane navždy v mé paměti a paměti všech lidí zde v mém rodném Šumberku. Nikdy ti to nezapomenu. Josef.

překlad

Caro amico. La ringrazio molto che ti ricordi di me e parlare di mio successo con l'Imperatore. L'imperatore nel suo viaggio in effetti per me, sulla base di raccomandazioni per una battuta d'arresto. Quel giorno glorioso a settembre rimarrà per sempre nella mia memoria e la memoria di tutte le persone qui nel mio paese natale Šumberk. Non potrò mai dimenticare. Joseph.

Přepis do mezinárodní abecedy

CARO AMICO LA RINGRAZIO MOLTO CHE TI RICORDI DI ME E PARLARE DI MIO SUCCESSO
CON LIMPERATORE LIMPERATORE NEL SUO VIAGGIO IN EFFETTI PER ME SULLA BASE DI
RACCOMANDAZIONI PER UNA BATTUTA DARRESTO QUEL GIORNO GLORIOSO A
SETTEMBRE RIMARRA PER SEMPRE NELLA MIA MEMORIA E LA MEMORIA DI TUTTE LE
PERSONE QUI NEL MIO PAESE NATALE SUMBURK NON POTRO MAI DIMENTICARE JOSEPH

Šifra: viz **Šifrový text**

System: Periodická šifra de Vigenére

Upřesnění:

Periodická šifra de Vigenére , heslo „AMIGO“

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (5)

Správná odpověď: UTAJOVANI

Body: 2

Otevřený text:

Nejvýznamnější výsledek v oblasti utajování naší korespondence je, že se podařilo najít obecný postup řešení Vigenérova šifrového systému s periodickým heslem, a to na základě analýzy vzdálenosti mezi opakováními v šifrovém textu. Tento objev nebyl zatím nikde publikován. Představitelé naší Lóže patří mezi ty, kteří byli s výsledkem seznámeni. Proto tuto šifru nepoužíváme. Milý Giacomo, teď tento text zašifruji s periodickým heslem AMIGO a předvedu ti, jak jej lze lehce vyluštit.

Přepis do mezinárodní abecedy

NEJVYZNAMNEJSI VYSLEDEK V OBLASTI UTAJOVANI NASI KORESPONDENCE JE ZE SE PODARILO NAJIT OBECNY POSTUP RESENI VIGENEROVA SIFROVEHO SYSTEMU S PERIODICKYM HESLEM A TO NA ZAKLADE ANALYZY VZDALENOSTI MEZI OPAKOVANIMI V SIFROVEM TEXTU TENTO OBJEV NEBYL ZATIM NIKDE PUBLIKOVAN PREDSTAVITELE NASI LOZE PATRI MEZI TY KTERI BYLI S VYSLEDKEM SEZNAMENI PROTO TUTO SIFRU NEPOUZIVAME MILY GIACOMO TED TENTO TEXT ZASIFRUJI S PERIODICKYM HESLEM AMIGO A PREDVEDU TI JAK JEJ LZE LEHCE VYLUSTIT

Šifrování/dešifrování/luštění: Substitute složitá - periodické heslo, srovnaná abeceda, Crypto-World 12/2000, str. 4-10

Úloha č.4

Adelaide de Gueidan

Šifrový text

EUGOP ICJB2 E1E2D IQBJK HQHR3 KP4R4 ZAE3Q MCIZH Q2RIB RJEIE KJMHR Z1GQ3
 QAEF4 UCMH QARHK JMCD5 LHRQ1 QR2V3 DIGQA EQ3K4 ODARV 1QHTP JVIMH R2L5D
 B6BRA P45GQ HE3O2 DP1OA GHQVJ G3VDI QRFHC FAOG2 BQ1QA EF4UQ ARBIQ RIBRH
 O2EGA GHJK3 QV3EZ 1QAFAL50AQ EJMO4 MBIRI ZQHKJ EJMHR 1RJEAL2LUB YVBD3
 OUO4K HQKPA DJZ3Q UPMHR 1GQ3Z VAO2V 6M4VF AEKHQ HIDAF IF2Q1 EQARB 2F3R3
 RJFAP 1BF5Q RYOAD IL6MC QARIB R4RJZ 5QRIF 1F2VZ OYL1Z KAMFA ZIQHT PJV2F
 12FHB O4FAK 4VJDI F6Q3R JFAKP AMRAM 4Z1R4 RIBRI GFACJ R3MCM HF2QK IRGAQ
 RDHGQ HKPAD JZ3DO 4KHQI ZQ1ER 2BQ1K RIERU Q3QRJ RIBRA OY2FJ P4ZCJ ODIGQ
 AEQ1Z ARVUG F2VPC KP3GE 5IKPV FHPHH GF4VJ 5FAOA D3KP3 G1OUZ 2RALJ 5FID4
 V1MBY ZIEAM 1BRVA CJKPH RADAZ UQR2F 5RIEQ R1LJU KP1QF JMIDA QDHLE HZAF3
 BEUIF HBOY4 R4EF1 L5O1Q F3MVY KP2VA REHD2 MBUEJ MQ1R1 Q3EDI QB4E4 G1RV2
 CJD5L HMBIX

Systém: Homofonní šifra**Upřesnění:**

Převodová tabulka pro tuto šifru:

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 Alphabet1:	I	L	M	O	A	T	S	C	H	G	B	D	E	F	J	K	N	P	Q	R	U	V	W	X	Y	Z
Cipher Text Alphabet2:	2		1					3							4						5				6	

Převodová tabulka vznikne z klíče:

Il mio amato si chiama Giacomo (Můj milý se jmenuje Giacomo)

Řádek šifry: ILMOATSCHGBDEFJKNPQRUVWXYZ

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Tvá?

Správná odpověď: H12

Body: 3

Otevřený text:

Můj drahokame, ma láska. Píši ti, protože mi scházíš a takto mám pocit, že jsi se mnou. Chci se Ti pochlubit. Sestavila jsem si podle tvé šifrovačí tabulky, kterou jsi mi dal raději svoji vlastní. Hned jak se se mnou setkáš, tak Ti dám její opis. Víím, že se nebudeš moc dočkat až si pomocí této mé tabulky v klidu dopis přeložíš. Určitě jsi zvědavý, co v něm píše. Ale na našem setkání ti to neřeknu. Styděla bych se. Takto to zůstane navždy bezpečně zašifrované a nikdo nepovolany si to nepřečte. Cože to tak tajného Ti chci naspat? Jestli jsi přeložil dopis až sem, tak se ptám: Tušíš to? Tak tedy ano. Rozhodla jsem se, že Tvůj návrh přijmu a první říjnovou neděli přijedu za Tebou na lovecký zámek tvého přítele. Zůstanu tam s Tebou přes noc. Ale slib mi, že nikmu a nikdy o tom nebudeš nic vyprávět. Miláčku moc se těším. Láska moje. Tvá holubička.

Přepis do mezinárodní abecedy

Muj drahokame ma lasko Pisi ti protoze mi schazis a takto mam pocit ze jsi se mnou Chci se Ti pochlubit Sestavila jsem si podle tve sifrovaci tabulky kterou jsi mi dal radeji svoji vlastni Hned jak se se mnou setkas tak Ti dam její opis Vim ze se nebudeš moc dočkat az si pomoci teto me tabulky v klidu dopis prelozis Urcite jsi zvedavy co v nem pisi Ale na nasem setkani ti to nereknu Stydela bych se Takto to zustane navzdy bezpecne zasifrovane a nikdo nepovolany si to neprecte Coze to tak tajneho Ti chci naspat Jestli jsi prelozil dopis az sem tak se ptam Tusis to Tak tedy ano Rozhodla jsem se ze Tvuj navrh prijmu a prvnii rijnovou nedeli prijedu za Tebou na lovecky zamecek tveho pritele Zustanu tam s Tebou pres noc Ale slib mi ze nikmu a nikdy o tom nebudeš nic vypravet Milacku moc se tesim Lasko moje Tva holubicka

Převod podle šifrové tabulky dá šifrový text:

EUGOP ICJB2 E1E2D IQBJK HQHR3 KP4R4 ZAE3Q MCIZH Q2RIB RJEIE KJMHR Z1GQ3
Atd.

Pro luštění šlo využít to, že homofony nahraovaly pouze samohlásky a navíc byly použity pro ně číslice... Jinými slovy tabilka homofonní záměny je velmi špatně sestavena

Úloha č.5

Úkoly ze šuplíku – Francesca Buschiniová

Šifrový text

DFVHFQDUI DYW DELO RQWXPV LP HM HV LYCR PLVRUS VHQDWVRG HY-
LUGMHQ RF XVLSRG N HV HC PDIXRG D ODG LP LVM XRUHWN XVHUGD DQ
LVLS HEHW R HV PLMRE VDYBCRHQ HV RKXROG HW LMXEHWRS RQWXPV
LP HM HQDOG LFLMDNVDO D DWVX DYW LP LEBKF LVMHOLPMHQ MXP

Systém: složená šifra

- Text napsaný pozpátku a potom použita Caesarova šifra

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (3)

Správná odpověď: CHYBI

Body: 3

Otevřený text:

Můj nejmilejší. Chybí mi Tvá ústa a laskavé dlaně. Je mi smutno. Potřebuji Tě. Dlouho se neozýváš. Bojím se o Tebe. Píši na adresu, kterou jsi mi dal, a doufám, že se k dopisu co nejdříve dostaneš. Prosím ozvi se! Je mi smutno. Líbá tvá Francesca.

Přepis do mezinárodní abecedy

MUJ NEJMILEJSI CHYBI MI TVA USTA A LASKAJICI DLANE JE MI SMUTNO PO-
TREBUJI TE DLOUHO SE NEOZYVAS BOJIM SE O TEBE PISI NA ADRESU KTEROU
JSI MI DAL A DOUFAM ZE SE K DOPISU CO NEJDRIVE DOSTANES PROSIM OZVI
SE! JE MI SMUTNO LIBA TVA FRANCESCA

Pozpatku

ACSECNARF AVT ABIL ONTUMS IM EJ ES IVZO MISORP SENATSOD EVIRDJEN
OC USIPOD K ES EZ MAFUOD A LAD IM ISJ UORETK USERDA AN ISIP EBET O ES
MIJOB SAVYZOEN ES OHUOLD ET IJUBERTOP ONTUMS IM EJ ENALD ICIJAKSAL
A ATSU AVT IM IBYHC ISJELIMJEN JUM

Posun o 3 znaky – Caesarova šifra

DFVHFQDUI DYW DELO RQWXPV LP HM HV LYCR PLVRUS VHQDWVRG HY-
LUGMHQ RF XVLSRG N HV HC PDIXRG D ODG LP LVM XRUHWN XVHUGD DQ
LVLS HEHW R HV PLMRE VDYBCRHQ HV RKXROG HW LMXEHWRS RQWXPV
LP HM HQDOG LFLMDNVDO D DWVX DYW LP LEBKF LVMHOLPMHQ MXP

Úloha č.6

Cesta do Ruska

Šifrový text

DAAEK ENKZZ YRAPC MIPJP YVCCH NZRSV UTAAE VMSKD NUVPJ ALDEO TEOTE OTRTD
UPTDE RIVYD NXDRT NETEV EINTR UDSNO RAHEL PIUPE AIRIA DCNDI MAAKA VOAVR VE-
IEK ODEEI IOYOE OUEVI OSUJO LEHDY NEBVA EEVNV ARACN JJRLD LSRCE ZTOEE EARZA
EVUAP LPAKL ONUDT AOZIV TESKA YKIHA RJNAT VTSRV MEYNL SHOKE SDHXS SSSUS
NNSLA CDEEV ORKTE RTUKA NEEAT HNIJY MALDS NTASN ENOZN SFMRE STOKO KAEIC VE-
UBD ANEAM TEDMA KLRIP ZTAAT DEOIN EARPI RHRST EAKEK RITCE TUSIY RBIVP AETTS
KSCIR CIOOE OUBET OEMEH CERTE CEVLL OBAUA VPATR HPTET RSOAE OEAEL OSDBU VE

System:

Úplná sloupcová transpozice

Upřesnění:

Transpoziční klíč odvozen z textu: Svému synovi dvě / Suo figlio due.

Klíč po vyčíslení: 10-11-8-3-5-4-7-6-9-1-12-2

Délka textu 431 letters. ($432=36*12$, doplněno X), doplnění pomocí X lze použít k určení velikosti tabulky.**Luštění:** inspirace - Jednoduchá transpozice, Crypto-World 11/2000, str. 2-6**Nápověda: (4)****Správná odpověď: BERLINA****Body: 2****Otevřený text:****Benátky 1764.**

Před odjezdem z Berlína navštivte maršálka von Hatzfelda. Předá vám kontakty, které budete na své návštěvě v Rusku potřebovat. Zajistí vám pozvánku na velký ples, který pořádá carevna Kateřinu Velká pro přední šlechtice svého impéria na konci tohoto roku v Petrohradě. Dejte se na cestu proto ihned, abyste u jejího dvora byl již začátkem prosince. Detaily svého úkolu dostane před plesem. Zatím se soustředte na ruské šlechtice na dvoře carevny. Musíte si získat dvůr natolik, abyste dosáhl audience u carevny co nejdříve.

Přepis do mezinárodní abecedy

PRED ODJEZDEM Z BERLINA NAVSTIVTE MARSALKA VON HATZFELDA PRED
 VAM KONTAKTY KTERE BUDETE NA SVE NAVETEVE V RUSKU POTREBOVAT
 ZAJISTI VAM POZVANKU NA VELKY PLES KTERY PORADA CAREVNA
 KATERINU VELKA PRO PREDNI SLECHTICE SVEHO IMPERIA NA KONCI
 TOHOTO ROKU V PETROGRADE DEJTE SE NA CESTU PROTO IHNEDE ABYSTE U
 JEJIHO DVORA BYL JIZ ZACATKEM PROSINCE DETAILY SVEHO UKOLU
 DOSTANE PRED PLESEM ZATIM SE SOUSTREDTE NA RUSKE SLECHTICE NA
 DVORE CAREVNY MUSITE SI ZISKAT DVUR NATOLIK ABYSTE DOSAHL
 AUDIENCE U CAREVNY CO NEJDRIVE

Šifrování. Přepsáno to tabulky 36 x12 , doplněno X, transpozice podle klíče

Úloha č.7**Madam de Urfé****Šifrový text**

BMSQQ GSOYX EWJCA SCJKR GNNUM KSAPH CZLOC OEWWJ OCMHA KKSLO MJBFB IDOKA
 CGIOI VWPBO DVESL OMENB XCNDQ GUVFV DSAJQ NXDBF FOVDA WSIYB LGLAG AKTLK
 GHOLP NVEMD EIIQN XPCAK XQHZN BJCVA KCOZM KUWQU TWKKN NUMKM CQUHK LTJCP
 ACFIX VAKSO ZVOTA JNBCR GCUEG RUOTI NAAOL BJZEU SFRTC UJMUD VOXDT RJBVC
 QKAOY MJCAB FOUEG EGLKZ CMRBY XZFFV OCJVF XDUDD TJXKC SJOXB CFZCV VXGEJ
 LKGDY DLFVO OSTII UPKQO SPPQX LTNZC BPTUA GVDKM MMKKQ OWAPG GNRJQ QWZZW
 KPZRU NBSJG SKUQX KWNGZ GIDZU WWGOG JOPQK VZMDU FOOZP OMQVP ETXOE TBABC
 EDCDN VIOZS AYJYB DNPDS ZAZIQ AROLT PCRUI ACPFO ZMWFC DXRLM GUROB OVAPM

RVGMD OESOV VOXHN RTSPG TUUXO VJGMK UZULT NVOHD IJBHJ GLENT OCNVH XUKFZ
LAGGP QWAID IIPCN XPKFK WGUIN ZXAGO XZWAY GHQRF BKFKF NNVQN ABOCO PGYJH
NRUVZ PCOAE TEIXI TORAE KGOFF NRUQK SOFLS DNLWI HVCVD JBQKR KSRWP GRWJL
EWYNP BUDLP ZNXKP NDXXF IWPNF DSFRD MRAAH DXDOZ OFVWI USKIZ WAXLR CACUP
GBACO AKANN NHCTP FJBAB NGMJK ROABF ESBRO PNAJD ZHZOD AOZZB HYHPA KBOWY
ZFTSQ CDGAM OVDAA GUZGS ALHZK GNAMG JXZNS TSDRY MZQKV QKGAG OEOUW UCZMO
SKPGH PHNII VPBJT HOZUN TIIIV VFBI A WFZDJ OXPPG APBXU MCQTK KXJNS CEJFC
RYDDT NVSVR DRJQQ WZLZW ZOGNX NKROL VJXSW WNHXU IXFBN ZBKOB WJBUZ DXFPO
POJRJ QQWKX NTKDR LWQWA HAKSK ZDNUN XZDZP CFBSC ENBTZ OVELJ XSLRS AYMRO
RGYXK WENQB VYBQK VBSWN CASCY COXZW ZKQFP XCCVF WLKBB TBLQU KVVEJ CSTRK
SQUQG IKLBS PJBAG KROLV JXFGP GPNVP GBGLH ELFNH RWSVZ XNWOH NOQDC JXPFF
DSOCN JBRUD DFVKG NTCAC ZEESO AOXKZ JPXFL ALVWK PGRVA IWCBD VZVEW CNJIU
PWTKY XEWYW WYMHE SOVVO XNEIX IKGQK BALDR YJNCJ KOXFT UEEZG IFLGL DNFAK
FUAPU RKTKO BSDDV HXISV ZXJFA AXFLK GBKEB JPOBT NHNBL KCOFW HKPGH TSPQD
VZBSE ANPNZ KEZCK TEXNY JTIOB ZTFLS BNBSQ ATGBK UNYEA JIQMQ ODPYG XOFNX
NCJOS AVKGG WUMPB OWRKW UXQQZ JOQHP AKCOF GINQG MJKKO DCSCR UQBHY CDTVA
YMRVN NCJGO XNMKO YNQSC QKLKB UAKGN LNCHK RBNTB OYTBR JCWKK WOTOP FHCMH
GKFNE EZDTP TSPGO XZLST RLQBI EWSGB WOPNS WJZEM WZNVF OPUSQ QJKBH EWOCW
JPPMS XDWA OJWNB DCOED CNCPA HZNB OJAV VSTXA MJMQW IKYDS TNSPB CEWBK
VOFKS SCJGS KWALK HOFNO RDCWQ KZMKW OCMHN ECVXN WSCJN MGURB FAMDK MNEIP
URQRG YGLOF FNBBH OMGSK BGFOW JQPQQ GSWOP FJNTL CEIGU KTOFF PNZCD LKKAG
BNSAJ KCLZX AGIJJ HGKGR ORKUC KCDGM YMPDD WDQGB NUARQ HQJMF DZAFH HNKLO
LBJCY ERKWK HUMTK BUBKF JIQAH QRQVD ODREI XIPKT ACGIB DSCZN IMZWT EZKAJ
RJQQC VCZTS WRSJ MAHOX FVODH PNGWD EPUVK HOJVA PUPOL AMKYL WZJBF LQRKC
QXKGD CHCNK BHAKJ TJLWJ HCLKK AEZKA PRJQQ UAKCO HOENL NCRKA QFTSC RUMHS
YWIBJ CTNTC CGJCV FUYXS TNACI USOCQ OLBLD CGOQZ NDDJW DDTSA QWCZJ WZKND
TEARG SLFNP NUDTO FXRPU KQAKY CTVPO QCTZW YKQHX OSSMK DDCJV TKFES CFYVR
KVGQU YZIXZ KOTBJ DKNJE WUGQO KMJTU MJGAQ UKGRB JBSUG FYTNR OLGUK GBNVL
TJCDD OAOTT RCAPH YMPUW AYLNS QNACZ PNJHH GPFXX JQGIO BLOEX ESCQT WKKVK
GBNOA JBCDD FVVOB NEWOK LOLBN OHKJV PXSVM KBNTS WNAAG VZQPL NBSFN NNOQ

System: periodická šifra

Upřesnění:

Periodická šifra Beaufort cipher , NABUCODONOSOR

Inspirace:

Brian J.Winkel, Casanova and the Beaufort Cipher, Cryptologia, April/1978

<http://www.informaworld.com/smpp/content~db=all?content=10.1080/0161-117891852947>

heslo: NABUCODONOSOR

italsky: Nebuchadnezzar

Délka textu: 2279 znaků

Nápověda: Jméno kadeřníka

Správná odpověď: FIGURO

Body: 2

Otevřený text (Madame du Barry):

Moje milá, prosila jste mi, abych Vám napsala o svém životě. Vděčím vám za tolik a jsem tolik vděčná, že splnit toto Vaše přání je to nejmenší co mohu pro Vás za to, co jste pro mne vykonala udělat. Chtěla jste, abych byla ve svém dopise zcela otevřená. Slibuji, budu. Současně použiji šifru, kterou jste mne naučila, a použiji heslo, které jste mi svěřila. Věřím, že mé tajemství neprozradíte a zůstane navždy uchováno v tomto dopise.

Narodila jsem se před patnácti lety ve Vaucouleurs, malém městečku na dolním toku řeky Maasy. Má matka, švadlena, byla proslulá svým bujným poprsím. Pracovala čas od času pro klášter kajicníků třetího řádu svatého Františka ve městě a s jedním z bratrů Gomardem de Vaubernier, s řádovým jménem Ange počala dítě. To dítě z lásky jsem já.

Moje maminka měla i dále četné milence a díky nim se dostala až do Paříže, kde působila jako kuchařka. Tam se také v provdala za Nicolase Ranona, vojenského skladníka nažloutlého a podobaného od neštovic. Mmmaince to nevadilo, chtěla a potřebovala počestného manžela. A právě díky tomuto nevlastnímu tatínkovi bylo rozhodnuto, že je třeba mne vzdělávat. A tak jsem se dostala do kláštera svaté Aury na předměstí Paříže. Zde jsem strávila celých devět let. Nevzpomínám na život zde ráda. Vadila mi přísná kázeň. Nesnášela jsem prosté bílé šaty s černým pláštěm a vadila mi věčná zima v klášterních ložnicích. Od matky, která se hezky strojila a parádila, jsem byla zvyklá na veselé prostředí a šaty a na toto spartánské prostředí v klášteře jsem si nemohla prostě přivyknout. Přišla jsem tam ale ke znalostem, které jsou i pro běžné ženy a to třeba i šlechtičny a to na královském dvoře přímo nevidané. Miluji četbu, kreslím a a zpívám a dostalo se mi v tomto směru výborné vzdělání. Jak víte tak má matka nemá v současnosti práci a tak jsme se musela po svém návratu z kláštera začít žít jako pouliční prodavačka. Myslím se, že ve svých patnácti letech jsem velmi krásná. Jsem vysoká, mám dokonalou postavu. Nosím své plavé vlasy, sčesané z vysokého čela. Mám krásné oči s dlouhými řasami a oválný obličej s malými pihami na tváři. Věřím, že se nyní vše změní. Jak víte, zamiloval se do mne váš kadeřník Figuro Lamet.

Mimo hodin lásky mne také vyučil tomuto krásnému kadeřnickému řemeslu.

Vymyslela jsem několik nových účesů, které jsem mimo Vás a vašich přítelkyň vyzkoušela i sama na sobě. U dvora prý měly velký úspěch. Nejvíce snad ten, který jsem udělala naposledy i Vám a to účes, v němž byly vlasy upraveny tak, aby z drdolu nedbale splývaly a působily, jako kdyby byly zvednuty neúmyslně a ve spěchu.

Žiji s Lametzem již pět měsíců. To se však nelíbí jeho matce. Vyčítala si mne na ulici. Hlasitě mne spílala a nazvala mne courou, děvkou a poběhlicí.

Velmi vám děkuji, že jste se mne zastala! Jste nejen krásná, ale i šlechtná!

Vaše navždy odaná Jeanne.

MOJE MILA PROSILA JSTE MI ABYCH VAM NAPSALA O SVEM ZIVOTE VDECIM VAM ZA TOLIK A JSEM TOLIK VDECNA ZE SPLNIT TOTO VASE PRANI JE TO NEJMENSI CO MOHU PRO VAS ZA TO CO JSTE PRO MNE VYKONALA UDELAT CHTELA JSTE ABYCH BYLA VE SVEM DOPISE ZCELA OTEVRENA SLIBUJI BUDU SOUCASNE POUZIJ SI FRU KTEROU JSTE MNE NAUCILA A POUZIJ HESLO KTERE JSTE MI SVERILA VERIM ZE ME TAJEMSTVI NEPROZRADITE A ZUSTANE NAVZDY UCHOVANO V TOMTO DOPISE NARODILA JSEM SE PRED PATNACTI LETY VE VAUCOULEURS MALEM MESTECKU NA DOLNIM TOKU REKY MAASY MA MATKA SVADLENA BYLA PROSLULA SVYM BUJNYM POPRSIM PRACOVALA CAS OD CASU PRO KLASTER KAJICNIKU TRETIHO RADU SVATEHO FRANTISKA VE MESTE A S JEDNIM Z BRATRU GOMARDEM DE VAUBERNIER S RADOVYM JMENEM ANGE POCALA DITE TO DITE Z LASKY JSEM JA MOJE MAMINKA MELA I DALE CETNE MILENCE A DIKY NIM SE DOSTALA AZ DO PARIZE KDE PUSOBILA JAKO KUCHARKA TAM SE TAKE V PROVDALA ZA NICOLASE RANONA VOJENSKÉHO SKLADNIKA NAZLOUTLEHO A PODOBANEHO OD NESTOVIC MMMAINCE TO NEVADILO CHTELA A POTREBOVALA POCESTNEHO MANZELA A PRAVE DIKY TOMUTO NEVLASTNIMU TATINKOVI BYLO ROZHODNUTO ZE JE TREBA MNE VZDELA VAT A TAK JSEM SE DOSTALA DO KLASTERA SVATE AURY NA PREDMESTI PARIZE ZDE JSEM STRAVILA CELYCH DEVET LET NEVZPOMINAM NA ZIVOT ZDE RADA VADILA MI PRISNA KAZEN NESNASELA JSEM PROSTE BILE SATY S CERNYM PLASTIKEM A VADILA MI VECNA ZIMA V KLASTERNICH LOZNICICH OD MATKY KTERA SE HEZKY STROJILA A PARADILA JSEM BYLA ZVYKLA NA VESELE PROSTREDI A SATY A NA TOTO SPARTANSKE PROSTREDI V KLASTERE JSEM SI NEMOHLA PROSTE PRIVYKNOUT PRISLA JSEM TAM ALE KE ZNALOSTEM KTERE JSOU I PRO BEZNE ZENY A TO TREBA I SLECHTICNY A TO NA KRALOVSKEM DVORE PRIMO

NEVIDANE MILUJI CETBU KRESLIM A A ZPIVAM A DOSTALO SE MI V TOMTO SMERU VYBORNE VZDELANI JAK VITE TAK MA MATKA NEMA V SOUCASNOSTI PRACI A TAK JSME SE MUSELA PO SVEM NAVRATU Z KLASTERA ZACIT ZIVIT JAKO POULICNI PRODAVACKA MYSLIM SE ZE VE SVYCH PATNACTI LETECH JSEM VELMI KRASNA JSEM VYSOKA MAM DOKONALOU POSTAVU NOSIM SVE PLAVE VLASY SCESANE Z VYSOKEHO CELA MAM KRASNE OCI S DLOUHYMI RASAMI A OVALNY OBLICEJ S MALYMI PIHAMI NA TVARI VERIM ZE SE NYNI VSE ZMENI JAK VITE ZAMILOVAL SE DO MNE VAS KADERNIK FIGURO LAMET MIMO HODIN LASKY MNE TAKE VYUCIL TOMUTO KRASNEMU KADERNICKEMU REMESLU VYMYSLELA JSEM NEKOLIK NOVYCH UCESU KTERE JSEM MIMO VAS A VASICH PRITELKYN VYZKOUSELA I SAMA NA SOBE U DVORA PRY MELY VELKY USPECH NEJVICE SNAD TEN KTERY JSEM UDELALA NAPOSLEDY I VAM A TO UCES V NEMZ BYLY VLASY UPRAVENY TAK ABY Z DRDOLU NEDBALE SPLYVALY A PUSOBILY JAKO KDYBY BYLY ZVEDNUTY NEUMYSLNE A VE SPECHU ZIJI S LAMETZEM JIZ PET MESICU TO SE VSAK NELIBI JEHO MATCE VYCIHALA SI MNE NA ULICI HLASITE MNE SPILALA A NAZVALA MNE COUROU DEVKOU A POBEHLICI VELMI VAM DEKUJI ZE JSTE SE MNE ZASTALA JSTE NEJEN KRASNA ALE I SLECHETNA VASE NAVZDY ODANA JEANNE

Šifrování/dešifrování/luštění: Substituce složitá - periodické heslo, srovnaná abeceda, Crypto-World 12/2000, str. 4-10

Úloha č.8

ISOCAMERON - písmo Megamikrů

Šifrový text

eeoiua xiua xue ea oe eoe eoe xue eox ui oox axaii xoxixo xoe xox au iou
 euo oiui ueu xixi exooa reo oeu kioe exuix uoioixioioioiixioixukeeee
 xoeu xaoxuuua axxaxiooixaeuoxexioox xuuoeo xoiu xeo oeuuio xaiex
 oxe xioeioo oxaxiuxooax xeuoiuuuoxiaaiioui xaoioe uxaiuxxoxeoe
 o xioixuou xaooiio uao xooeo xueia xoeia iuixaoioxiu xaiuxx
 ux eeo xaexiux xuu xaeiuxxoxioeouueeox xuiox xue xoiiiiexoxu x
 eoauxoxeiee iuxaiuxuo eooo aoiouxeiu xuixxooo xouooaeu xixoe
 oux xaeiixexioaai uiioe uoxaxexuixeiixxooe uouuxi xouioiixxie
 axoeu xuuaxi xioi iu xieaxoou aiiooa xouux xaeixouxoxio xioeueou iux
 i xuoouiooaou xaoiioea ueeu ueaer ioe uue xue xaexxu oioeoeoxoa ax
 euau xoeoouxi xioeieueou uex xooeo xoxe uuxiix xoxeouuee auoixioie
 ux eaaaixuxuxaeexu auoxauxi exuoxaeoouixuxeieu xaeuixuixixuuxux
 eeuxiueiee i xuxaxiioio xaeuxuoxu xxiou xua xuo xueeoxa xai xuo
 uxaxueea xxi xexiio u xauueuxi u xou xioioxiio u aieiooxi xou xoi
 io uouoixexouaax xaiexaeuxuixuoeoe i xiaou xieouaiioax xaiuxuxi
 ix xxiou xueeoaax xai eea xexiio xxaoo xeoau xuoexxiu xeeoe e
 oioe xueoxa xexeiauiux ooa iu xai oexeuioix xaeixoi xeaueuxio xuu
 euio xxiou xxi xexea xxeo xuoieo xea aoxi xoeiixou xauou uo iu
 oioauxeauxiooauxuieaex

Systém: Homofonní šifra (s dělbou na slova, mezera šifrována).

Upřesnění: Použita pravidla zápisu jazyka Megamikrů z knihy Icosameron
 6 samohlásek, a,e,i,o,u + x (nám neznámá), 7 výšek – zápis v souladu s knihou pomocí 7 ba-
 rev.

Jazyk Megamicromanů se v šifře nepoužívá (dále ještě využívá gesta, tanec, úsměvy), ale jsou použita pravidla k přepisu mezinárodní abecedy do jimi používaného zápisu a tím vznikne homofonní šifrový systém.

Na základě pravidel připravena tato převodová tabulka (* dále značí mezeru):

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

Přepsáno do tabulky / homofonní šifra.

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	*
e	x	a	u	o	i	e	a	x	u	o	i	E	o	u	a	a	e	i	i	o	x	u	x	a	e	x
i		a	o					u		e	i	O	u	x	a		e	i	o	u					x	

Jako mezera zvolen znak **x**. Tato barva použita pouze pro tento znak. V textu vzhledem ke své barvě znak zaniká a „zdá se, že tam není“. Má pomoci při hledání mezery...

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (-2)

Správná odpověď: ZPIVANEHO

Body: 5

Otevřený text:

Základy tohoto jazyka Megamikrů jsem popsal ve své knize: Historie Eduarda a Alžběty, kteří strávili jednaosmdesát let u Megamikrů, původních obyvatel Protokosmu v nitru naší zeměkoule. Hlavním tématem tohoto mého románu je smyšlená cesta do hlubin země, kde svítí věčné slunce, které nikdy nezapadá. K cestě do hlubin země využili moji hrdinové legendární vodní vír Malstrom u břehů Norska. Do hlubin země cestovali v olověné bedně. Pro osvěžení hrdla a ducha jsem je vybavil zásobu tekutin a to šesti lahvemi vody a šesti lahvemi pálenky. Moji hrdinové se seznámili s netušenými vynálezy jako např. strojem na výrobu elektřiny pomocí tření a se zařízeními, které umožňovali komunikaci na délku, rychlou dopravu pomocí strojů, přenos obrazu apod. Na svoji obranu dokázali obyvatelé vyrobit i velmi účinný otravný plyn. Jejich jazyk byl zvláštní. Používali jen šest samohlásek a to ještě jedna z nich byla pro nás neznámá. Tyto samohlásky vyslovovali v sedmi různých výškách a dále během řeči používali různá gesta, úsměvy. K zápisu těchto výšek museli vyrábět a používat inkoust v sedmi barvách. I tak nelze zachytit krásu tohoto ojedinělého zpívaného jazyka.

Přepis do mezinárodní abecedy

ZAKLADY TOHOTO JAZYKA MEGAMIKRU JSEM POPSAL VE SVE KNIZE HISTORIE EDUARDA A ALZBETY KTERI STRAVILI JEDNAOSMDESAT LET U MEGAMIKRU PUVODNICH OBYVATEL PROTOKOSMU V NITRU NASI ZEMEKOULE Hlavnim TEMATEM TOHOTO MEHO ROMANU JE SMYSLENA CESTA DO HLUBIN ZEME KDE SVITI VECNE SLUNCE KTERE NIKDY NEZAPADA K

CESTE DO HLUBIN ZEME VYUZILI MOJI HRDINOVE LEGENDARNI VODNI VIR MALSTROM U BREHU NORSKA DO HLUBIN ZEME CESTOVALI V OLOVENE BEDNE PRO OSVEZENI HRDLA A DUCHA JSEM JE VYBAVIL ZASOBU TEKUTIN A TO SESTI LAHVEMI VODY A SESTI LAHVEMI PALENKY MOJI HRDINOVE SE SEZNAMILI S NETUSENYMI VYNALEZY JAKO NAPR STROJEM NA VYROBU ELEKTRINY POMOCI TRENI A SE ZARIZENIMI KTERE UMOZNOVALI KOMUNIKACI NA DELKU RYCHLOU DOPRAVU POMOCI STROJU PRENOS OBRAZU APOD NA SVOJI OBRANU DOKAZALI OBYVATELE VYROBIT I VELMI UCINNY OTRAVNY PLYN JEJICH JAZYK BYL ZVLASTNI POUZIVALI JEN SEST SAMOHLASEK A TO JESTE JEDNA Z NICH BYLA PRO NAS NEZNAMA TYTO SAMOHLASKY VYSLOVOVALI V SEDMI RUZNYCH VYSKACH A DALE BEHEM RECI POUZIVALI RUZNA GESTA USMEVY K ZAPISU TECHTO VYSEK MUSELI VYRABET A POUZIVAT INKOUST V SEDMI BARVACH I TAK NELZE ZACHYTIT KRASU TOHOTO OJEDINELEHO ZPIVANEHO JAZYKA

Přepis podle tabulky homofonní záměny:

eeoiiua xiuxiu ueeaoe eoeoe xeeo uioo axaiiix xo ixo eoxeo auioeueo oiuiueu i
 xiexooa xeoeeu ioeeuix uoioixioioiixioix ueeeexoeu axuuuaa xxaxiooi ae
 uoxexioox xuueeo xoiu eooeeuio aioxoxe ioeiooo oxaxiu coax euoiuu uo ioaii
 oui xaoioe ux aiuxxo eoeo xio ixuou xoao iio uao oooeo uueia ooeiaiu ieraoii
 oxiu aiuxxu eoeo xaexiu oxuu aeiuuxx ioeouueeox xuiox xueoiiie xoxu xea
 xoxeiee xiu aiuxuo eoo aoiouxeiu x uiixooo xouoo aeu xixoeoux aeiii eioaa
 ixuioexuo xaxexuixeiixx ooeuouxixou ioiixieaxoeu xuaa i xioiu ieaxoou ai
 iooa xouux aeixouxo xioeueouixixuouiooacu xaoioea ueeu ueae ioeuuoe xue
 xaexxu oioeoe xoa xaxeuau oeeou ixio eieueouuex oooeo uoxeuuxiix oxeouueau
 oixioieux eaaaixu xaxaexu xou xau iie xuo xaeoouix ueieiu eaui xui xixuux uxeuu i
 ueiee ix uxaxiioio xaeuxuo u xoiou uaxuo a uoeexoa aiauuou xaa ueeae xai xexi
 iouu xauueuxiu uou xioio xiiouaieioo xou uoio uouoie ouaa xae aeu xui xue
 oeeixiaou ieoua iioa xaiiuxuxiix xioio u eoeoaaa xaeaaa e xiiio xaooxeoau
 auoexxiu xoeoe xioioe uieoxa xexiauiux oaa iu xai oxe uioix xaeixoi e auoexxi
 oxuueuio xxiouou xie xea x xoeo uoieo eaaa oxixoe iiu ouauou uuo iuuio iou au
 xiooau xieae x

Úloha č.9 Nová mise

Šifrový text

Pověda naše se vomíl
 as nebyvá Rdules pro
 akru ubál směchá kl
 opá na černí bolsta
 Peřili trab zrop sá
 tke očkon šilenci ve
 st prot věs skupena
 omuz a sotkka huvězt
 enemvro klasr havkaN
 po suv Mitéš dastym
 apol sšip prso daku
 yd novn paled omasto
 mír dras Fakot Mtěch

Havara Saša Neboľmik
 s tep vo Rmut sucha
 ok prut vosm proukaJ
 ote narč bli selk ad
 Pořtti vlakaz oprká
 trepič ontLip oclote
 slavnot běh slavene
 podzra sot baklava t
 e oaveb klikr padkon
 podrev vlšěm Dropke
 hal ladším prkot okl
 y ona nadar stom dus
 líko post ewvt dfěgě

Systém: Steganografie, Cardanova mřížka

Nápověda: Kde (2)

Správná odpověď: KRAKOVE

Body: 2

Otevřený text:

Vaše mise v Rusku skončila. Při zpáteční cestě se zastavte v Krakově. Další pokyn na místě.

Upřesnění šofrového systému:

Otevřený text je zapsán do následující mřížky:

		V			a			š			e			m	i		
	s			e			v		R		u			s			
		k				u				s						k	
o				n			č			i			l			a	
	P		ř			i					z			p		á	
t		e			č		n			í			c			e	
	s						t			ě		S			e		
			z		a		s		t			a			v		t
e				v				K				r		a		k	
		o				v				ě			D				
	a			l			š	í			p			o			k
y			n			n			a					m			
	í						s					t				ě	

Šifrování:

Znaky otevřeného textu v mřížce jsou zcela náhodně doplněny písmeny. Zaplněná tabulka tvoří prvou část šifrového textu.

Stejná tabulka znovu naplněna stejným textem a opět náhodně vyplněna. Tato zaplněná tabulka tvoří druhou část šifrového textu.

Tento postup byl skutečně kdysi praktikován. Důvodem bylo, že přiložení tabulky na ručně psaný text nemuselo dávat zcela jasně výsledný text (vzhledem k tomu, že písmena se nezobrazila ve vystřížených okénkách tabulky zcela přesně/ jednoznančně). Zajišťovalo se tak to, že příjemce našel uschovaný text bez velkých problémů. Vedlejší efekt této praktiky však byl, že relativně bezpečný systém byl degradován na velmi lehce řešitelnou šifru.

Úloha č.10
Mise v Polsku

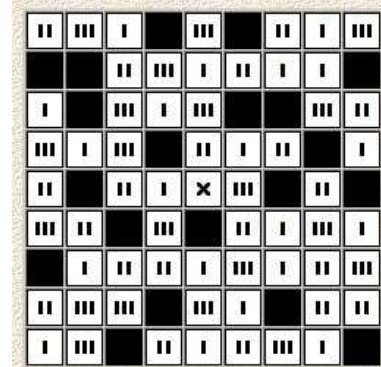
Šifrový text

MEEVJ YBTCV OREEA MFLRE KAAJT VNANS EITCS
IKOIS XVUMB ENOLJ EKES MZAXA ABOID MHEWR
JTENA ERJAE B

Systém: transpozice, Fleissnerova mřížka

Upřesnění: 9x9 , 80 znaků+X (střed), mřížka viz obrázek.

Fleissnerova mřížka



Poznámka: obrázek a zašifrování vytvořeno aplikací dostupnou na:
<http://www.musilek.eu/michal/sifry-krizovka.html?menu=cc>

Nápověda: Co ?

Správná odpověď: ODMENA

Body: 4

Otevřený text:

Vyvolejte souboj s hrabětem Františkem Xawerem Branickim. Nezabijte jej. Čeká Vás velká odměna.

VYVOLEJTE SOUBOJ S HRABETEM FRANTISKEM XAWEREM BRANICKIM
NEZABIJTE JEJ CEKA VAS VELKA ODMENA

VYVOLEJTESOUBOJSHRABETEMFRANTISKEMXAWEREMBRANICKIMNEZABIJT
EJEJCEKAVASVELKAODMENA

Úloha č.11 Jan Josef Kittel

Šifrový text

PBPHG FYHVX FLEEO SEJLB PVIJM GUPBQ EROAH NFLER DPPVB XDDVP
INRPX SSWGK SD

Systém: záměna - postupný posun písmen

Upřesnění: posun o 0,1,2,3,....

Použitá abeceda je uspořádána cyklicky (mod 26)

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluští: P3

Správná odpověď: PORADKU

Body: 2

Otevřený text:

Pane Casanova, s radostí vám mohu oznámit, že vaše paže je již skoro v pořádku.

Přepis do mezinárodní abecedy

PANE CASANOVA S RADOSTI VAM MOHU OZNAMIT ZE VASE PAZE JE JIZ SKO-
RO V PORADKU

Úloha č.12 Stíny hraběte Branického

Šifrový text

Moi drodzy.

Mam nadzieję, że ręka jest wyleczona.

Modlę się za was.

Twoja Hali

System: Text napsaný pozpátku „neviditelným tajným písmem“

Upřesnění:

Šifrová zpráva je napsána skoro bíle na bílém podkladu.

Text lze vyvolat např. tak, že v aplikaci Malování (součást Windows) se naleje na plochu jiná barva. Podklad se změní, ale písmena zůstanou bílá.



Samotný text je napsán polsky a to obráceně odzadu.

Nápověda: (14 CZ)

Správná odpověď: ZABIT

Body: 2

Otevřený text:

Klamač (bezvýznamový text):

Můj milý. Doufám, že se ti ruka již zahojila. Modlím se za Tebe. Tvoje Halina

Moi drodzy. Mam nadzieję, że ręka jest wyleczona. Modlę się za was. Twoja Hali

Otevřený text, který má být utajen:

Nevracej se zpět do Krakowa. Přátelé hraběte Branického přísahali, že se Ti pomstí! Chtějí tě zabít.

Polsky:

Nie wracaj do Krakowa. Przyjaciele hrabiego Branickiego przysięgł pomścić Ciebie! Oni chcą cię zabić.

Zašifrováno (pozpátku):

ćibaz ęc ąhc ino eibeic ćicśmop łgąisyzrp branickego ogeibarh eleicajyzrp awokark od jacarw ein

Úloha č.13 - Adelaide de Gueidan podruhé

Šifrový text

63 2 3 64 21 91 28 659 6 303 122 614 32 56 47 313 314 129 4 309 216 658 111
 404 52 73 662 651 148 657 301 49 73 88 601 29 60 77 78 410 82 26 30 203 72
 123 145 505 138 611 39 413 506 615 511 652 524 135 217 303 520 129 217 98
 222 307 669 11 56 34 212 602 140 78 515 216 131 514 127 658 49 317 318 315
 49 55 76 512 655 101 9 29 304 305 28 501 418 143 619 613 620 611 619 616
 612 617 620 611 524 502 514 522 521 413 505 305 507 418 506 309 219 137 322
 139 99 324 203 85 94 117 214 25 91 106 417 625 614 150 149 127 659 518 77
 307 72 602 56 660 206 419 410 607 501 415 302 143 95 43 662 64 111 223 25
 401 86 306 602 17 106 317 44 422 215 39 57 201 80 4 2 13 70 301 59 658 615
 201 100 501 4 115 87 306 84 304 209 417 210 78 111 15 74 311 202 93 224 56
 106 83 19 517 103 317 312 91 213 99 26 316 112 313 88 94 72 129 101 657 96
 140 71 85 144 517 95 317 218 311 105 324 78 127 668 119 81 411 108 652 215

Systém: Knižní šifra

Použita varianta, kdy jsou písmena v oběma stranám známém textu očíslována a tato čísla jsou pak využita jako substituce písmen v otevřeném textu.

Zde použit předchozí dopis Adelaidy Giacomovi.

Markantem k nalezení správného referenčního textu je jednak to, že tento text je znám oběma stranám (a luštitelům) a jednak na něj ukazuje délka. V šifrovém textu není použito větší číslo, než je délka referenčního dopisu.

Upřesnění: (referenční dopis z roku 1749)

Muj drahokame ma lasko Pisi ti protoze mi schazis a takto mam pocit ze jsi se mnou Chci se Ti pochlubit Sestavila jsem si podle tve sifrovaci tabulky kterou jsi mi dal radeji svoji vlastni Hned jak se se mnou setkas tak Ti dam její opis Vim ze se nebudeš moc dockat az si pomoci teto me tabuky v klidu dopis prelozis Urcite jsi zvedavy co v nem pisi Ale na nasem setkani ti to nereknu Stydela bych se Takto to zustane navzdy bezpecne zasifrovane a nikdo nepovolany si to neprecte Coze to tak tajneho Ti chci naspas Jestli jsi prelozil dopis az sem tak se ptam Tuisis to Tak tedy ano Rozhodla jsem se ze Tvuj navrh prijmu a prvnii riiijnovou nedeli prijedu za Tebou na lovecky zamecek tveho pritele Zustanu tam s Tebou pres noc Ale slib mi ze nikmu a nikdy o tom nebudeš nic vypravet Milacku moc se tesim Lasko moje Tva holubicka

Nápověda: Kde (2)

Správná odpověď: NEBI

Body: 3

Očíslování písmen v referenčním dopise:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
0	M	U	J	D	R	A	H	O	K	A	M	E	M	A	L	A	S	K	O	P	I	S	I	T	I	0
25	P	R	O	T	O	Z	E	M	I	S	C	H	A	Z	I	S	A	T	A	K	T	O	M	A	M	25
50	P	O	C	I	T	Z	E	J	S	I	S	E	M	N	O	U	C	H	C	I	S	E	T	I	P	50
75	O	C	H	L	U	B	I	T	S	E	S	T	A	V	I	L	A	J	S	E	M	S	I	P	O	75
100	D	L	E	T	V	E	S	I	F	R	O	V	A	C	I	T	A	B	U	L	K	Y	K	T	E	100
125	R	O	U	J	S	I	M	I	D	A	L	R	A	D	E	J	I	S	V	O	J	I	V	L	A	125
150	S	T	N	I	H	N	E	D	J	A	K	S	E	S	E	M	N	O	U	S	E	T	K	A	S	150
175	T	A	K	T	I	D	A	M	J	E	J	I	O	P	I	S	V	I	M	Z	E	S	E	N	E	175
200	B	U	D	E	S	M	O	C	D	O	C	K	A	T	A	Z	S	I	P	O	M	O	C	I	T	200
225	E	T	O	M	E	T	A	B	U	K	Y	V	K	L	I	D	U	D	O	P	I	S	P	R	E	225
250	L	O	Z	I	S	U	R	C	I	T	E	J	S	I	Z	V	E	D	A	V	Y	C	O	V	N	250
275	E	M	P	I	S	I	A	L	E	N	A	N	A	S	E	M	S	E	T	K	A	N	I	T	I	275
300	T	O	N	E	R	E	K	N	U	S	T	Y	D	E	L	A	B	Y	C	H	S	E	T	A	K	300
325	T	O	T	O	Z	U	S	T	A	N	E	N	A	V	Z	D	Y	B	E	Z	P	E	C	N	E	325
350	Z	A	S	I	F	R	O	V	A	N	E	A	N	I	K	D	O	N	E	P	O	V	O	L	A	350
375	N	Y	S	I	T	O	N	E	P	R	E	C	T	E	C	O	Z	E	T	O	T	A	K	T	A	375
400	J	N	E	H	O	T	I	C	H	C	I	N	A	S	P	A	T	J	E	S	T	L	I	J	S	400
425	I	P	R	E	L	O	Z	I	L	D	O	P	I	S	A	Z	S	E	M	T	A	K	S	E	P	425
450	T	A	M	T	U	S	I	S	T	O	T	A	K	T	E	D	Y	A	N	O	R	O	Z	H	O	450
475	D	L	A	J	S	E	M	S	E	Z	E	T	V	U	J	N	A	V	R	H	P	R	I	J	M	475
500	U	A	P	R	V	N	I	R	I	I	J	N	O	V	O	U	N	E	D	E	L	I	P	R	I	500
525	J	E	D	U	Z	A	T	E	B	O	U	N	A	L	O	V	E	C	K	Y	Z	A	M	E	C	525
550	E	K	T	V	E	H	O	P	R	I	T	E	L	E	Z	U	S	T	A	N	U	T	A	M	S	550
575	T	E	B	O	U	P	R	E	S	N	O	C	A	L	E	S	L	I	B	M	I	Z	E	N	I	575
600	K	M	U	A	N	I	K	D	Y	O	T	O	M	N	E	B	U	D	E	S	N	I	C	V	Y	600
625	P	R	A	V	E	T	M	I	L	A	C	K	U	M	O	C	S	E	T	E	S	I	M	L	A	625
650	S	K	O	M	O	J	E	T	V	A	H	O	L	U	B	I	C	K	A							650
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

chybí: **G Q W X**

Otevřený text:

Můj milovaný. Než odejdu z tohoto světa, tak Ti chci poděkovat za nejkrásnější okamžik mého života. Byla to noc, kterou jsem s Tebou strávila v říjnu před padesáti lety na loveckém zámečku. Po této noci jsem se bála, že budu mít s Tebou dítě. Teď toho lituji, že to nebyla pravda. Sejdeme se v nebi. Tva holubička.

Mezinárodní abeceda:

MUJ MILOVANY. NEZ ODEJDU Z TOHOTO SVETA TAK TI CHCI PODEKOVAT ZA NEJKRASNEJSI OKAMZIK MEHO ZIVOTA. BYLA TO NOC, KTEROU JSEM S TEBOU STRAVILA V RIJNU PRED PADESATI LETY NA LOVECKEM ZAMECKU. PO TETO NOCI JSEM SE BALA, ZE BUDU MIT S TEBOU DITE. TED TOHO LITUJI, ZE TO NEBYLA PRAVDA. SEJDEME SE V NEBI. TVA HOLUBICKA.

Šifrování: písmeno otevřeného textu je náhodně nalezeno v referenčním textu a je nahrazeno číslem, které odpovídá jeho pořadí v referenčním textu. Úmyslně použity znaky z konce textu, aby byla vidět jeho délka. Použita opakování více než bylo potřeba.

Úloha č.14 Zednářská lóže 3

Šifrový text

Nakonec obnos puvab trochu rodopis relief rezba Glasgow. Nerv venku houf pivo svab drama elf ruze kyvadlo. Slib prepis pucet zapal postup. Tetrev Q krokus zpusob duvod hoboj. Dabel venku trumf jas Jakob. Rtut trumf objev dolozit ucitel zjev dvou. Relief odchod fiasko rozvoj. W ocenit puvab podzim slib dragoun. Dostup dav vsechno chlap W. Elf zad berni kongres pohyb. Potesen kov Q. Obrys krab premena dokazat azyl elf. Narizen Q vas Glasgow sidlo. Konvoj rameno relief vule trumf. Album carodej konzul W. Tarif cloveku kouzlo sestup W. Nakup priliv W relief. Predtim shon nastroj tajnost cemu Eros. W houf datum orloj sokol elf. Islam biskup laska trumf Q. Prinos hrob schuzka adresat kristal relief.

System: kombinovaná šifra: steganografie + Augustova šifra

Upřesnění:

poslední písmena dávají šifrový text, který se dešifruje pomocí posunu o 1 znak vlevo (Augustova šifra)

Nápověda: (2)

Správná odpověď: ZVU

Body: 4

Otevřený text:

Braťe, zvu tě na zednářskou práci, která se uskuteční v Šalamounově chrámu pražském první neděli květnovou. Velmistr veliké lóže pražské.

Příprava textu / mezinárodní abeceda:

BRATRE ZVU TE NA ZEDNARSKOU PRACI KTERA SE USKUTECNI V SALAMOUNOVE CHRAMU PRAZSKEM PRVNI NEDELI KVETNOVOU VELMISTR VELIKE LOZE PRAZSKE

Augustova šifra / posun o 1 znak vpravo (A/B, B/C, ... Z/A)

CSBUSF AWV UF OB AFEOSTLTPV QSDJ LUFBS TF VTLVUFDOJ W TBMBNPVOPWF DISBNV QSBATLFN QSWOJ OFEFMJ LWFUOPWPV WFMNJTUS WFMJLF MPAF QSBATLF

Steganografické zakrytí šifrového textu. Text tvoří poslední písmena. Slova náhodně doplněna. Použita taková, která odkazují na alchymii a případné kontakty Zednářů.

Nakonec obnos puvab trochu rodopis relief rezba Glasgow. Nerv venku houf pivo svab drama elf ruze kyvadlo. Slib prepis pucet zapal postup. Tetrev Q krokus zpusob duvod hoboj. Dabel venku trumf jas Jakob. Rtut trumf objev dolozit ucitel zjev dvou. Relief odchod fiasko rozvoj. W ocenit puvab podzim slib dragoun. Dostup dav vsechno chlap W. Elf zad berni kongres pohyb. Potesen kov Q. Obrys krab premena dokazat azyl elf. Narizen Q vas Glasgow sidlo. Konvoj rameno relief vule trumf. Album carodej konzul W. Tarif cloveku kouzlo sestup W. Nakup priliv W relief. Predtim shon nastroj tajnost cemu Eros. W houf datum orloj sokol elf. Islam biskup laska trumf Q. Prinos hrob schuzka adresat kristal relief.

D. Ohlasy, připomínky a komentáře soutěžících

D.1 Termíny zveřejnění soutěžních úloh

Dobrý den,
chtěl bych se zeptat, kdy je možné očekávat další úlohy v soutěži Crypto-World. Časová prodleva mi už připadá dlouhá ... :).

Dobry den,
rad bych se zeptal, na kdy se planuje finalni uloha/posledni varka uloh.
Primlouvam se hlavne za to, aby se nekryla s kvalifikaci a hlavne samotnou Tmou (3. 10. respektive 5. - 6. 11. 2010). (obecne s termíny sifrovacek)

Co se týká termínů zveřejňování úloh, asi to nemáte jednoduché. Tento a následující víkend se pro změnu koná Deskohraní; myslím, že si ho část řešitelů soutěže rozhodně nenechá ujít. Pokud je to možné, poprosil bych o odložení alespoň závěrečné úlohy o týden (nebo dva) dále.

S tym terminom finale zverejnenym v CW to myslite vazne, alebo to je preklep?

Prosim, prosim, je mozne posunout na libovolny den v tydnu. Urcite bude vice soutezicich na vikendu a ...

Dobrý den,
myslím, že není moc dobrý nápad zveřejnit úlohy, které rozhodnou o celkovém umístění v dlouhodobější soutěži, večer před všedním dnem (viz CW 10/2010). Lidé, kteří pracují všední dny od rána (to bude velmi pravděpodobně většina řešitelů), tak v podstatě ztrácí šanci na dobré umístění v soutěži. (Kdyby byl termín znám s dostatečným předstihem, mohli by si případně zajistit volno, to však není tento případ :).)

Nikdy se nepodaří najít termín, který bude vyhovovat všem. Doporučoval bych tedy alespoň to, aby po zveřejnění úloh následoval nějaký volný čas během víkendu. Jako rozumné mi přijdou (obecně) termíny pátek večer, sobota (kdykoli) nebo případně neděle. (Pokud preferujete negativní reakce, pak tedy Po večer rozhodně ne, Út večer rozhodně ne :).)

Vsedni den je super.

Dekuji za tu anketu. Alespon mam pocit, ze je ted termin stanoven tak, ze poskodi co nejmene mych konkurentu..

Bezva, beru zpet, ted je termin stanoven spravedlive. Dekuji.

Akceptujem, ale zaroven koncim. Nema zmysel zucastnovat sa sutaze, v ktorej vopred nemam sancu uspriet... To je zbytocne zabijanie cas, aj ked tie ulohy ma bavia a riesil som ich rad.

Na Vaši soutěž určitě nezanevřu. Úlohy se pokusím dořešit, i když to bude možná s časovým odstupem :).

Uvědomuji si, kolik práce se za soutěží v luštění šifrových textů skrývá. Myslím, že jako autor máte právo stanovit si vlastní pravidla (i v případě, že některým řešitelům nemusí tato pravidla nutně připadat objektivní).

D.2 Úlohy a ohlasy

Dobry den,

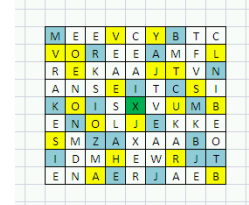
diky za zatim peknou soutez, kde clovek obcas musi namahat mozek. Mel bych malou prosbu, zda by slo psat pribeh tak, aby nebyl tak navodny.

V drivejsich rocnicich jsem podle bodoveho ohodnoceni premyslel o typu sifry a hledal nejdrive typ sifry a nasledne pak reseni (pravda, obcas pozdeji pomohla napoveda, kde byl nazev sifry pripadne její popis).

Letosni rocnik mi trosku prijde, ze neni az tak o napadu/analyze, ale spis o tom, kdo umi lepe zachazet s excelem pripadne kdo ma lepsi solver na dany typ sifry.

Dobrý den,

udělátka, která jsem připravil, se osvědčují. Například Fleissnerovu mřížku jsem řešil nejprve ručně vybarvováním políček a když jsem "chytil" dva úseky textu, které vypadaly rozumně, nechal jsem "dřinu" s otáčením mřížky o 90° p řipravenému skriptu



Diky znalosti typu sifer slo posledni 3 sifry lustit opravdu rychle (me to zabralo cca 2 hodiny) Bez znalosti typu sifry se tento cas mohl o dost protahnout. I kdyz Fleissnerova mrizka by byla rozhodne jasny kandidat (pocet pismen dava ctverec a "uprostred" je X).

Berte tu pripominku spis jako stesk souteziciho, ktery ma prozatim "hotovo" a musi cekat min dalsi tyden na nove sifry

S pozdravem

O tych Icosameronoch som si to nasiel na internete. Hned bolo jasne, ze sa jedna o homofonnu sifru. Na tej ulohe bol extremne neprijemny zapis. Skoro 2 hodiny mi trvala priprava textu na analyzu!!! Cize skoro 2 hodiny som roznofarebne pismenka substituoval na normalne pismena a cifry (spolu 36 znakov). To bolo nieco hrozne. Potom uz samotne lustenie zabralo cca 15 minut. Uz sa tesim na dalsie ulohy.

Nepřipadá mi však, že by úlohy byly pracné. Jako pracná mi v podstatě přišla pouze prozatím poslední úloha (písmo Megamikrů) - od začátku bylo jasné, o co se jedná, šlo pouze o to řešení dotáhnout do konce (zakódovat nějak znaky jejich písma, provést frekvenční analýzu a potom správně přiřadit jednotlivým znakům písma naší abecedy). Vlastně jediná netriviální věc v této úloze byla uvědomit si, že jedním ze znaků je mezera ...:)

Ta sutaz je pre mna cosi ako droga. Nedokazem sa odputat ani ked chcem. Aj minuly rok ma dost dlho nicil MORBIT a x-krat som si vtedy povedal, ze s tym musim skoncit a nedokazal som.

Jinak letošní úlohy mi celkově připadají obtížnější než v předchozích ročnících. (Některé úlohy za pouhé dva body už byly poměrně zapeklité :).) Je to jenom můj pocit nebo jde o úmysl a máte třeba podobné reakce i od dalších řešitelů?

Dobrý den,

musím konstatovat, že úlohy 12 a 13 mají pro mne velmi rozdílnou náročnost. Zatímco první z nich jsem měl vyluštěnou během pěti minut, asi proto, že jsem se steganografií v obrázcích dělal už předtím sám různé pokusy, "nešťastná" třináctka mi dává zabrat. Podle použití jedno, dvou a trojčiferných čísel a podle celkového počtu použitých čísel (několikrát větší než počet písmen mezinárodní abecedy) soudím, že se jedná o knižní šifru. Klasická knižní šifra znamená, že očísloji slova v nějakém textu a při dešifrování pak píšu první písmena příslušných slov. Zkoušel jsem zatím průvodní texty příběhu k soutěži (Historie de ma vie, Úkoly ze šuplíku - Adelaide de Gueidan), ale text, který by dával smysl nevychází. Tak nevím, jestli jdu správným směrem. Jedná se o knižní šifru? Mám hledat i jiná písmena než ta první? Každopádně jsou obě úlohy zajímavé a jiné než ty předchozí. Umíte umístit laťku do správné výšky. Člověk doufá, že když napne všechny síly, mohl by přeskočit, ale

jednoduché a samozřejmé to nebude ...

Nešťastná 13.. Pak mne to došlo. Stačilo se podívat kolik písmen mají texty, které přicházejí v uvahu. Pak už to bylo za chvíli...

Bylo mi jasné, že jde o knižní šifru. Jaký text byl použit jsem se dohadoval. Nejpravděpodobnější byl předchozí dopis od stejné milény. Délka textu odpovídala nejvyššímu číslu v šifře. Proto jsem se po této stopě pustil, text napsal do tabulky vytiskl a pak jsem aktivoval místo počítání manželku. Já hlásil čísla a ona odpovídala písmenem, který v tabulce našel. Nastěsti hned od počátku bylo vidět, že jsem se trefil. Manželka na závěr řekla, že toho blbce, který to vymyslel mám pozdravovat... Tak jsem suse poznáměl, že jsi to byl ty a vyrizují...

Mimochodem nejvíc mi dala zabrat úloha č. 13 (kódová kniha). Poté, co jsem si udělal graf rozložení četnosti (viz příloha), tak jsem si byl naprosto jistý, že ty shluky po pětadvaceti nemohou znamenat nic jiného, než nějaký druh substituce. Stačí je akorát správně namapovat. "Hm, prostě modulo 25 nefunguje, tak to bude určitě složitější vzoreček..." Az této fixace mě dostala až nápověda. Povedený chyták, to byl záměr?

Poslední dvojice úloh mi v praxi ukázala, že složení několika relativně jednoduchých systémů může dát dohromady poměrně těžce rozluštitelnou šifru. I tady pro mě byla náročnost obou úloh rozdílná. U č. 14 jsem správně odhadl použitý systém a kombinoval jsem agenturní systém s různými jednoduchými záměnami. Protože jsem neměl moc času stihl jsem do zveřejnění nápovědy vyzkoušet, první písmena, druhá písmena a třetí písmena všech slov, přičemž jsem je kombinoval s šifrou Atbaš a se všemi 25 možnými posuny abecedy (včetně Albam), pak mě napadlo jít na poslední písmena slov. Trochu mě mátlá ta sólo písmena W a Q, ale tuhle šifru bych určitě vyluštil i bez nápovědy.

Co se týká úlohy číslo 14, v šifrovém textu byla patrná značná redundance. Bylo zřejmé, že je potřeba "vzít pouze něco" :). Osobně jsem vsadil na poslední písmena slov (první písmena mě odradila opakujícími se písmeny r) a jednoduchou záměnu (potud to bylo v podstatě správně :)), ale řešení se mi nějak nedařilo najít. Tak jsem potom začal zkoušet šifru Vigenere ... :(.

Po nápovědě, že se jedná o velmi jednoduchou klasickou šifru, jsem vyzkoušel ještě Caesarovu šifru a bylo to :).

Finálová úloha č.15

Dobrý večer,

určitě Vás zajímá, na čem se v současné době trápí soutěžící. Tak vězte, že já jsem ještě neobjevil dopis Karla Ungara hraběti Valdštejnovi.

Text "Predpokladam, ze ji vsak snadno objavite." v zadání úlohy mě začíná trochu dráždit. Už jsem to přečetl alespoň desetkrát. :-)

Zjistil jsem, že Casanovy rukopisy nedávno získala BNF a digitalizuje je [1]. To je ale asi něco jiného, než zmiňovaný dopis.

Navíc pochybuju, že by se BNF aktivně účastnila této soutěže :-)

[1] http://www.bnf.fr/en/bnf/anx_bnf_en/a.bnf_manuscrits_casanova_en.html

Tak to bylo mistrně ukryté. Bez toho zvýraznění bych na to určitě nepřišel. A i tak jsem to otevřel a nejdřív si myslel, že je to ten starý obrázek, že mám to pdf určitě nakešované v browseru. No ale pak už to byla hračka. Přesně, jak praví text: "Fotografie je dostatečně návodná".

Mimochodem jsem hledal i na takových místech, jako <http://soutez2010.crypto-world.info/place/Duchcov.pdf>, přestože v zadání bylo jasně řečeno, že v Duchcově to není.

Ja jsem cul nějakou zradu ve smyslu steganografie takže jsem prohledaval web cryptoworldu a ty fotky jsem prohlizel vsechny, nahodou jsem si vsiml te zmeny,

Na hradecke veze koukam, 0321 vidim, 49 pismen vidim i mrizku 7x7 vidim ale precist se to neda :-)) Pouziju 0321 pro otoceni znaku (zkousel jsem otacet proti i po směru ručiček) prevedu na pismena a dam do mrizky a jsem v pytlí :-)

Zato u šifry č. 15 jsem si připravil pěknou slepou uličku. Číselné heslo 0321 jsem považoval za posuny v polyalfabetické substituci s periodickým heslem a dešifrováním zednářského kříže jsem proto začínal, nikoliv končil. Za nápovědu jsem byl vděčný, s ní byla šifra náhle zcela jasná, takže jsem ji dešifroval bez jediného zaváhání. Zato bez nápovědy nevím, nevím. Upřímně blahopřeji soupeřům, kteří to zvládli.

Ale tohle byla asi nejslozitejsi poslední uloha co pamatuju.

Dobrý den,
tak jsem to včera vydržel někdy k půlnoci a ráno už je konec. Sice poslední úlohu vůbec nevím, ale každopádně chválím, člověk se mohl alespoň docela dlouho kochat nadějí :-)
Jsem rád, že ta poslední úloha byla opravdu těžká (zjevně nejen pro mě), je to takhle zajímavější :-)

Po soutěži

Dobrý večer,
tak nakonec se mi podařilo všechny úlohy letošní soutěže vyřešit. Ale dalo mi to pěkně zabrat :).

Smekám před všemi, kterým se to podařilo bez Vaší poslední nápovědy. (Ono zpětně je řešení vlastně zřejmé, většinu věcí uvedených v nápovědě člověk stejně věděl nebo alespoň tušil, ... ale doplnit si chybějící kousky skládačky a celé to dát dohromady během pár hodin, to je obdivuhodné.)

Dekuji za zpestreni podzimu.

Tradičně Vám však musím poděkovat za úžasnou zábavu. Na Vaši soutěž se těším celý rok. A je to rok od roku lepší a lepší.

Obdivuji to kolik casu soutezi venujete a jak nam ji po kapkach ordinujete. Mate pravdu jsem nemocny. Musim se lecit ... (lustenim). Kdy dostanu dalsi davku, zase az na podzim?

Děkuji za letošní luštitelskou soutěž. Strávil jsem s ní příjemné chvíle.

Díky moc za Váš čas, který věnujete přípravě soutěže, já už bych si bez toho podzim ani nemohl představit

Ten proces hladania, ci uz ide o sifry, matematicke ulohy, alebo cokolvek ine, je ten najlepší:

Soutez byla letos opravdu vyborna a díky za ni. Prite vyhraju ☺

Taky jsem zvědav, kdo bude příští rok, Casanovu bude těžké překonat :-)

Obdivuji vase napady. Je prijemne lustit stále něco noveho. Obdivuji, ze jste se ještě nevyčerpal (doslova a prenesene).

A díky za tradicni podzimni zabavu...

D.3 Kde se všude luštilo

(poznámka PV – e-mail s fotografií, která odstartoval rubriku „Kde se všude luštilo“)

Dobry vecer,
lustilo se i v meste Brasilia v Brazilii...
S pozdravem

(poznámka PV – následující e-mail přišel do rubriky „Kde se všude luštilo“ s fotkami z Mongolska, obsah e-mailu samozřejmě berte s rezervou ☺, autorovi za fotografie a kouzelný doprovodný e-mail velice děkuji):

Dobry den,
při procházce Ulánbátarem mě zaujala jedna zcela nenápadná jurta – snad tím, že se z ní ozývalo nezřetelné mumlání, jásavé výkřiky a zklamané povzdechy.
Věc byla rázem jasná – je to jurta luštitelského oddělení II. odboru GŠ armády MoR.
Bohužel, ani po silném klepání na dveře nikdo neotvíral, jen z komínku stoupal stále hustší a hustší kouř, patrně ve chvatu pálili citlivé materiály.
Na druhou návštěvu jsem se již lépe připravil – z protokolárních důvodů jsem oblékl tradiční mongolský kabát zvaný „deel“.
Po několikaminutovém „významném“ šustění papíry už náčelník nevydržel a vyšel ven.
Na mé jadrné „NAZDAR“ odpověděl též neméně jadrně -nazdar a pak ...Češi?
/pozn. V Mongolsku je prý přes 20. tisíc Mongolů/lek, co se domluví česky/.
Nad předloženými ukázkami úloh jen uznale pokyvoval hlavou a pídil se po dalších informacích, tak jsem mu doporučil Vaši knihu. Dovnitř do jurty mě opět nepozval, ozývalo se jen horečné cvakání kuliček sčotů, patrně probíhal nějaký složitý výpočet....
Cca po půlhodině plodného rozhovoru ve stylu ... hm ha huh u ... a dalších zvuků jsme se rozešli, bezpochyby oba naplněni silným zážitkem.

V popředí je vidět nejmodernější mongolský šifrátor, maskovaný jako sekačka.
S pozdravem

(poznámka PV: reakce)

Je příjemné vidět, že se jedná o opravdu mezinárodní soutěž ... :).

Připadá mi, že soutěž je dost známá. Lidé si ji najdou ať jsou kdekoliv.... kde je internet. Jsem zvědav, když jste teď odstartoval novou minisoutěž, která místa ještě přibudou. Ja sám jsem však v Praze a Praha je nuda. Ale možná bych udělal nějakou kompozici s Hradem, když nám tu teď tak pěkně svítí sluníčko.

(poznámka PV: autor fotografie z HK netušil, jak mne jejím zasláním inspiroval a opravdu nevěděl, že ji využiji pro zakomponování do soutěže a uschování 15té úlohy..., dodatečně jsem se mu omluvil za její editaci bez jeho vědomí.

Zasláný originál – viz Crypto-World 10/2010, editovaná soutěžní verze zůstala na stránce soutěže a je uvedené v tomto e-zinu).

Vážený pane kolego,
posílám fotografii do rubriky "Kde se všude luští" z dnešního dne (14.10.2010). Protože Hradec Králové není tak exotický jako předchozí dvě místa, zpestřil jsem obrázek šifrovaným pozdravem. Fotografie je snad dostatečně návodná, takže prozradí nejen použitý systém, ale dokonce i klíč pro dešifrování.

(poznámka PV: A na úplný závěr fotografie od celkového vítěze)

Posílám slíbené foto :-). kdo by nevěděl kde to je, v exifu jsou souřadnice :-)
Zdraví

E. Mikulášská kryptobesídka / SantaCrypt 2010 / Program

<http://mkb.buslab.org/>

Pořádá TNS, a.s., a BUSLab za podpory / Organized by TNS, a.s. and BUSLab with support of



Program den první

2. prosince 2010 (čtvrtek) / December 2, 2010 (Thursday)

- 8:45 – *Registrace / Registration*
- 9:30 – 9:40 *Zahájení workshopu / Workshop opening*
- 9:40 – 10:40 *Keynote*
Danilo Gligoroski – Why narrow-pipe cryptographic hash functions are not a match to wide-pipe cryptographic hash functions?
- 10:40 – 11:40 *Keynote*
Paul Leyland – Experiences with GPUs for Cryptography
- 11:40 – 12:25 Michal Rjaško, Martin Stanek – On Designated Verifier Signature Schemes
- 12:30 – 13:30 *Oběd / Lunch*
- 13:30 – 14:30 *Keynote*
Dan Cvrček – Thoughts On Cryptography in Banking
- 14:30 – 15:00 *KEYMAKER I*
Kamil Malinka – Evaluation of Flash VEP Usability as Behavioural Characteristics for Biometric Authentication
- 15:00 – 15:30 *Přestávka na kávu a čaj / Coffee & tea break*
- 15:30 – 17:00 *KEYMAKER II*
Bedřich Hovorka – Search for S-boxes with evolutionary computing
Peter Vagánek – Alternative elliptic curves for cryptography
Tobiáš Smolka – Strengthening applications by automatic transformations

17:00 – 17:25 *Rump session*

17:30 – *Večeře / Dinner*

Následují neformální diskuze v prostorách vyhrazených pouze pro účastníky kryptobesídky. /
Followed by informal discussions in the hall available only to the workshop participants.

Program den druhý

3. prosince 2010 (pátek) / December 3, 2010 (Friday)

8:55 – 9:00 *Zahájení druhého dne workshopu / Opening of the second day of the workshop*

9:00 – 10:00 *Keynote*
Tomáš Rosa – Unleashing EMV Cards for Security Research

10:00 – 10:30 *Přestávka na kávu a čaj / Coffee & tea break*

10:30 – 11:30 *Keynote*
Petr Hanáček, Petr Švenda – Cryptography for Resource-limited Network Nodes

11:30 – 12:10 *KEYMAKER III*
Eugen Antal – Porovnanie rotorových šifrátorov Enigma a Fialka M-125
Juraj Varga, Eugen Antal – Zodiac

12:11 – *Mikuláš / Santa*

Závěr workshopu... / Workshop ends...



F. O čem jsme psali v listopadu 2000 – 2009

Crypto-World 11/1999

A.	Jak je to s bezpečností eliptických kryptosystémů ? (Ing. Pinkava)	2-4
B.	Známý problém přístupu k zabezpečeným serverům pomocí protokolu https s aplikací Internet Explorer 5 v systému Windows NT 4.0 s aktualizací SP4	4-5
C.	Y2Kcount.exe - Trojský kůň v počítačích	5
D.	Matematické principy informační bezpečnosti (Dr. Souček)	6
E.	Letem šifrovým světem	6-8
F.	E-mail spojení	8
G.	Trocha zábavy na závěr (malované křížovky)	9

Crypto-World 11/2000

A.	Soutěž! Část III. - Jednoduchá transpozice	2 - 6
B.	Působnost zákona o elektronickém podpisu a výklad hlavních pojmů - Informace o přednášce	7 - 9
C.	Rozjímání nad ZoEP, zvláště pak nad § 11 (P. Vondruška)	10-13
D.	Kryptografie a normy III. (PKCS #5) (J. Pinkava)	14-17
E.	Letem šifrovým světem	18-19
F.	Závěrečné informace	19

Crypto-World 11/2001

A.	Soutěž 2001, III.část (Asymetrická kryptografie - RSA)	2 - 7
B.	NESSIE, A Status Report (Bart Preneel)	8 - 11
C.	Dostupnost informací o ukončení platnosti, zneplatnění a zrušení kvalifikovaného certifikátu (P.Vondruška)	12-16
D.	Odpovědnost a přechod odpovědnosti ve smyslu zákona o elektronickém podpisu (J.Hobza)	17-19
E.	Eliptické křivky a kryptografie (J.Pinkava)	20-22
F.	Mikulášská kryptobesídka (V.Matyáš,Z.Říha)	23
G.	Letem šifrovým světem	24-25
H.	Závěrečné informace	26

Crypto-World 11/2002

A.	Topologie certifikačních autorit (P.Vondruška)	2 - 9
B.	Srovnání výkonosti hašovacích algoritmů SHA-1, SHA-256, SHA-384 a SHA-512 (M.Kumpošt)	10-16
C.	Informace z aktuálních kryptografických konferencí (J.Pinkava)	
-	Konference ECC2002	17-18
-	Konference CHES 2002	18-20
-	CRYPTO 2002	20-21
D.	The RSA Challenge Numbers	22-23
E.	Letem šifrovým světem	24-25
F.	Závěrečné informace	26

Crypto-World 11/2003

A.	Soutěž 2003 – průběžná zpráva (P.Vondruška)	2
B.	Mikulášská kryptobesídka – Program	3
C.	Cesta kryptologie do nového tisíciletí IV. (Od NESSIE ke kvantovému počítači) (P.Vondruška)	4– 7
D.	Kryptografie a normy. Politika pro vydávání atributových certifikátů, část 2. (J.Pinkava)	8 –11
E.	Archivace elektronických dokumentů (J.Pinkava)	12-16
F.	Unifikace procesů a normy v EU (J.Hrubý)	17-27
G.	Letem šifrovým světem	27-29
H.	Závěrečné informace	30

Crypto-World 11/2004

A.	Soutěž 2004 – úlohy závěrečného kola! (P.Vondruška)	2-4
B.	Jedno-dvoumístná záměna (P.Vondruška)	5-6
C.	Fleissnerova otočná mřížka (P.Vondruška)	7-8
D.	Formáty elektronických podpisů (J.Pinkava)	9-13
E.	Elektronická faktúra a elektronické daňové priznanie aj bez zaručeného elektronického podpisu. (R.Rexa)	14
F.	Nedůvěřujte kryptologům (V.Klíma)	15
G.	O čem jsme psali v listopadu 1999-2003	16
H.	Závěrečné informace	17

Příloha : Crypto-World 11/2004 – speciál (24 stran)

(V.Klíma : Nedůvěřujte kryptologům, ke stažení na adrese :

<http://crypto-world.info/index2.php?vyber=casop6>)

Crypto-World 11/2005

A.	Soutěž v luštění 2005 – přehled úkolů III. kola (P.Vondruška)	2-7
B.	Hardening GNU/Linux, Komplexnější prostředky pro lokální hardening OS Linux, část 3.(J.Kadlec)	8-12
C.	Může biometrie sloužit ke kryptografii? (Martin Dražanský, Filip Orság)	13-18
D.	Mikulášská kryptobesídka 2005 (D.Cvrček)	19-21
E.	Konference IT SECURITY GigaCon (P.Vondruška)	22
F.	O čem jsme psali v listopadu 1999-2004	22-23
G.	Závěrečné informace	24

Crypto-World 11/2006

A.	Soutěž v luštění 2006 skončila (P. Vondruška)	2
B.	Nový koncept hašovacích funkcí SNMAC s využitím speciální blokové šifry a konstrukcí NMAC/HMAC (V. Klíma)	3-16
C.	Elektronické cestovní doklady, část 2 (L. Rašek)	17-24
D.	Počítačová (ne)bezpečnost (J. Pinkava)	25-31
E.	Mikulášská kryptobesídka (D. Cvrček)	32-33
F.	O čem jsme psali v listopadu 1999-2005	34-35
G.	Závěrečné informace	36

Crypto-World 11/2007

A.	Soutěž v luštění 2007 skončila (P.Vondruška)	2
B.	Z dějin československé kryptografie, část IV., Československé šifrovací stroje z období 1955 – 1960. Šifrovací stroj ŠD – 1 (K.Šklíba)	3-5
C.	Testy obrazové kvality snímačů otisků prstů Suprema (M.Drahanský, O.Nezhyba)	6-11
D.	Možnosti odposlechu optických vláken (J.Dušátko)	12-30
E.	Mikulášská kryptobesídka 2007 – Program (V.Matyáš)	31-32
F.	Konference EOIF GigaCon (A.Ušcińska)	33
G.	O čem jsme psali v listopadu 2000-2006	33-35
H.	Závěrečné informace	36
	Příloha: Příběh Štěpána Schmidta (všechny 4 části ve formátu doc) pribeh.doc	

Crypto-World 11/2008

A.	Podzimní Soutěž v luštění 2008 skončila! (P. Vondruška)	2-4
B.	KYBERNETICKÉ ÚTOKY: RUSKO? – GRUZIE a SVĚT (T.Sekera)	5-11
C.	Kvantový šumátor ve Společné laboratoři optiky UP a Fyzikálního ústavu AV ČR (J. Hrubý)	12-17
D.	Mikulášská kryptobesídka 2008 / SantaCrypt 2008	18-19
E.	O čem jsme psali v listopadu 1999-2007	20-21
F.	Závěrečné informace	22

Crypto-World 11/2009

A.	Soutěž v luštění 2009 skončila!	2
B.	JAK SE STAL VÁCLAV PROKOPEC VĚZNĚM	3-4
C.	JAK SE STAL VÁCLAV PROKOPEC KRYPTOLOGEM	4-5
D.	JAK SE STAL VÁCLAV PROKOPEC ZRÁDCEM	6-9
E.	JAK BYL PROLOMEN ŠIFROVÝ TEXT ZAŠIFROVANÝ POMOCÍ CM-1	9
F.	Příloha č.1: Úlohy z PVS	10-11
G.	Řešení úloh č.1,č.2 a č.3 - Úlohy z PVS	11-12
H.	Příloha č.2: Administrativní kurz C v Tloskově 1	12-14
I.	Příloha č.3: Administrativní kurz C v Tloskově 2	14-15
J.	Řešení úloh č.4,č.5 a č.6- Administrativní kurz C v Tloskově 1,2	15-19
K.	Příloha č.4: Administrativní kurz C v Tloskově 3	19-20
L.	Řešení úloh č.7,č.8 a č.9 - Administrativní kurz C v Tloskově 3	20-23
M.	Příloha č.5: Administrativní kurz C v Tloskově 4	23-24
N.	Řešení úloh č.10 - Administrativní kurz C v Tloskově 4	24-26
O.	Příloha č.6: Zvláštní správa - analýza dopisů	26-27
P.	Řešení úloh č.11 a č.12 - Zvláštní správa - analýza dopisů	27-29
Q.	Příloha č.7: Zpráva centrále	29-30
R.	Řešení úlohy č.13 - Zpráva centrále	30-32
S.	Příloha č.8: Dešifrace ŠD-2 / CM-1	32-33
T.	Řešení úloh č. 14 a č.15 - Dešifrace ŠD-2 / CM-1	34-37
U.	Ohlasy a komentáře soutěživých	38-39
V.	O čem jsme psali v listopadu 1999-2008	40-41
W.	Závěrečné informace	42

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 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 e-ziny, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály: <http://crypto-world.info>

Všechna práva vyhrazena. Tato publikace ani žádná její část nesmí být reprodukována nebo šířena v žádné formě, elektronické nebo mechanické, včetně fotokopií, bez písemného souhlasu vydavatele.

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:	Vlastimil Klíma Pavel Vondruška
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS (výběr příspěvků, komentáře a vkládání na web)	Jaroslav Pinkava Vlastimil Klíma Pavel Vondruška Tomáš Rosa
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@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.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