Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 11, číslo 11/2009 **17. listopad 2009**

11/2009

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese

http://crypto-world.info

(1336 registrovaných odběratelů)

Obsah :

A. Soutěž v luštění 2009 skončila!

Soutěž v luštění 2009 (http://soutez2009.crypto-world.info/), která byla doprovázena fiktivním příběhem Václava Prokopce skončila. Možnost vkládat správné výsledky řešení jednotlivých úloh byla uzavřena 17. 11. 2009 v 18.00 hod.

Ceny (http://soutez2009.crypto-world.info/index.php?crypto=ceny) získali první tři řešitelé a dále tři řešitelé, kteří byli vylosování ze 46 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: 70

Celkem soutěžících: 89
Počet soutěžících, kteří vyřešili aspoň 1 úlohu: 83
Počet soutěžících zařazených do slosování: 47

Všechny úlohy letos vyřešilo celkem 16 soutěžících:
jmkollar, Jehova, kesy, ony, Bob, MD5Mir, koc, peddy, peta007, Tomik, Jahoda, Weber, Mirop, paulie, Snehurka, mim3

Pořadí na prvních třech místech:

1 jmkollar 70 13.11 (20:28)
2 Jehova 70 13.11 (20:33)
3 kesy 70 13.11 (21:12)

Vylosovaní soutežící:

11 Jahoda 70 13.11 (23:57
18 OldSuh 40 09.11 (08:32)
27 Prochor 36 10.11 (09:16))

Všem úspěšným řešitelům blahopřeji!

Sponzoři 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

Všechny postavy v tomto doprovodném příběhu jsou smyšlené a jakákoliv podobnost se skutečnými osobami je čistě náhodná. Příběh je zcela vymyšlen a nemá reálný podklad. Jediná opravdová reálie je šifrátor ŠD-2. Informace k tomuto šifrátoru můžete najít v e-zinu Crypto-World 78/2009 v článku Vojtěcha Brtníka: Rekonstrukce šifrovacího stroje ŠD-2.

B. JAK SE STAL VÁCLAV PROKOPEC VĚZNĚM

Ve dnech 13. až 25. ledna 1958 se u Státního soudu v Plzni konal proces s Václavem Prokopcem, zaměstnancem Zvláštní správy Ministerstva vnitra, ing. Ondřejem Sýkorou, jeho přímým nadřízeným a Karlem Weberem, synem statkáře, který byl v roce 1945 odsunut do Německa, ale v roce 1957 překročil zpět ilegálně hranice do své vlasti.

Velké procesy padesátých let již skončily, ale prokurátor v podobném duchu hřímal na celý sál:

„...ukázali se být sprostými zločinci, kteří se neštítí pomáhat připravovatelům nové světové války, dodávat jim špionážní zprávy a vyzývat je k válce proti našemu lidu… Chtěli oloupit náš lid o všechny svobody, kterých dobyl, chtěli jej dostat pod vládu statkářů a kapitalistů, chtěli jej zbavit státní samostatnosti.“

Na základě důkazů, které byly u soudu předloženy, byli uznáni všichni tři vinnými. Zaměstnanec Václav Prokopec byl odsouzen za trestný čin velezrady a vyzvědačství k 22 letům odnětí svobody, Karel Weber za stejný trestný čin na 20 let odnětí svobody. Zaměstnanec ing. Ondřej Sýkora byl odsouzen na 3 roky odnětí svobody za nedbalost a neplnění služebních povinností.

Václav Prokopec, který byl převezen k výkonu trestu do Mírova, uléhal na dřevěný tvrdý kavalec ke spánku. Takovýchto nocí strávil ve vězení celkem 8000. Na rozdíl od spoluodsouzených se na něj totiž nevztahovaly amnestie ani rehabilitační procesy, které proběhly v roce 1964-67. Bylo na něj vždy hleděno jako na skutečného špióna, který zradil svůj lid a stát a pro svůj čin nenašel pochopení a odpuštění.

Co vlastně provedl? Jak bylo u soudu prokázáno, vyzradil cizí (americké) rozvědce informace o organizování šifrové služby v Československu, o způsobu a provádění zácviku šifrérů a strukturu a jména osob, kteří na nově zřízené Zvláštní správě Ministerstva vnitra byli zaměstnáni. Tyto informace předával svému známému z dětství, agentu cizí rozvědky Karlu Weberovi. Společně s nimi byl ještě odsouzen také jeho nadřízený, který byl odsouzen za to, že neplnil dostatečně své povinnosti a svým nezodpovědným přístupem umožnil, aby se s těmito informacemi seznámil v rozsahu, který mu nenáležel a navíc i přes některé náznaky na jeho chování neupozornil.

Často, když takto večer uléhal, přemýšlel, proč se v rozsudku neobjevilo také jeho největší provinění, totiž to, že předal podrobné plány sovětského šifrovacího stroje CM-1, který nesl v ČR kódové označení ŠD-2. Říkal si, že asi jeho nadřízený kryptolog ing. Ondřej Sýkora se bál, aby mu nebylo ještě více přitíženo a vše, co se týkalo tohoto stroje, raději popřel a tvářil se, že k úniku nedošlo a nemohlo dojít.

Pravda byla však ještě o něco složitější. Vedení Zvláštní správy tušilo, že plány pravděpodobně opravdu unikly. Báli se však sovětské straně toto přiznat, a proto to raději nejen neoznámili, ale během vyšetřování o tom pomlčeli. Přesto provedli určitá opatření. I když kryptografický rozbor stroje neprokázal žádné slabiny, rozhodli se jej v ČR nenasadit. Zdůvodněno to bylo možnými problémy s domácí výrobou, zejména časovou zdlouhavostí, náročností s přepracováním technické a výrobní dokumentace, utajení vlastní výroby, vyškolení techniků a organizováním celého procesu. Možnost sériové výroby těchto šifrovacích strojů v SSSR bylo také nakonec odmítnuto s tím, že nabízená cena za jeden kus šifrátoru je pro náš stát příliš velká. ŠD-2 tak nakonec nebyl v Československu nikdy dále vyvíjen, či nasazen do praxe.

C. JAK SE STAL VÁCLAV PROKOPEC KRYPTOLOGEM

Když večer Václav Prokopec uléhal na svůj vězeňský kavalec, promítal si den po dni svůj život a přemýšlel nad tím, co se vlastně stalo.

Václav vzpomínal:

Bylo mi již 21 let, když jsem ostříhaný dohola 1. října 1952 narukoval k ženistům do starých Fučíkových kasáren v Táboře. Měl jsem absolvovanou měšťanku v Nečtinách a pokračovací školu v Manětíně a vyučen jsem byl jako strojní zámečník. Zde jsem absolvoval tzv. přijímač, složil vojenskou přísahu a začal poddůstojnickou školu. Jako syn partyzána jsem byl považován za spolehlivého a tak když byli hledáni vhodní adepti pro šifranty, byl jsem pozván na PVS, kde jsme dostali k vyplnění speciální testy. Vypadalo to, že zjišťují naši inteligenci. Vůbec jsme netušili, proč nám dávají k řešení tyto rébusy a ptají se nás, zda rádi luštíme křížovky, zda umíme šachy apod.

Pplk. ing. Ondřej Sýkora, který nám na PVS tyto testy rozdal a vedl s námi pohovor, pak vybral mne a ještě jednoho mého kolegu a oznámil nám, že budeme vycvičeni jako pracovníci vojenské šifrové služby. Proč ne? Zdálo se mi to zajímavé a navíc nám sliboval i velmi slušné zacházení a po vojně i práci a zajímavé finanční ohodnocení.

Viz příloha č.1: Úlohy z PVS

A tak jsem byl v březnu 1953 vyslán do Administrativního kurzu C v Tloskově u Neveklova, což byl krycí název čtyřměsíčního kurzu šifrantů - důstojníků v záloze. Tehdejším náčelníkem šifrové služby GŠ byl právě ing. pplk. Ondřej Sýkora, kterého jsem již znal z testů. Jeho oddělení čítalo asi 20 osob, bylo to důstojníci - učitelé. Já jsem byl zařazen do první čety, kde nám velel npor. ing. Prachař. V kurzu nás bylo na 300 absolventů ŠDZ (!) ode všech druhů vojsk. Seznámili nás s historií a rozvojem kryptologie (kryptografie), seznámili nás s jednouchými šifrovacími systémy a jejich luštěním, naučili nás šifrovat ručními prostředky za použití převodových tabulek a písmenkových heslových materiálů, ale také lehce zapamatovatelných klíčů, tvořit signální či hovorové tabulky, naučili nás používat německý diskový šifrovací stroj Enigma, který se stále v naší armádě používal a nakonec jako zvláštní tajemství nám ukázali i diskový šifrovací stroj ANNA,

etablovaný na dálnopisných stanicích svazků. Museli jsme se naučit užívat i polní spojovací prostředky včetně sovětské přenosné radiostanice A7b a německého dálnopisu Hell, který byl získaný ve velkém množství jako válečná kořist. Během kurzu byly pořádány tři jednodenní soutěže v luštění jednoduchých úloh (jednoduchá záměna, transpozice apod.). Soutěže se pořádaly vždy v pátek. Tři nejlepší měli za odměnu slíben opušťák na následující sobotu a neděli. Jaké bylo překvapení velitele mé čety a velitele kurzu, když všechny tři soutěže jsem vyhrál já! Kolegové mne dokonce podezírali, že znám výsledky, tak rychle jsem některé úlohy vyřešil…

Viz příloha č.2: Administrativní kurz C v Tloskově 1
Viz příloha č.3: Administrativní kurz C v Tloskově 2
Viz příloha č.4: Administrativní kurz C v Tloskově 3
Viz příloha č.5: Administrativní kurz C v Tloskově 4

Po absolvování kurzu jsem se stal armádním šifrérem. Jako strojař jsem neměl žádné problémy s obsluhou (někdy poněkud uživatelsky nevhodných) šifrovacích a spojovacích zařízení a i jinak jsem byl svými nadřízenými považován za spolehlivého, pilného a chytrého poddůstojníka.

V roce 1955 vznikla Zvláštní správa Ministerstva vnitra, která měla mimo jiné i gesci na vývoj a testování kryptografických prostředků. Vedoucím oddělení, které mělo na starosti vývoj a testování nových kryptografických prostředků, se stal můj „starý známý“ ing. pplk. Ondřej Sýkora. Když hledal vhodné zaměstnance - své podřízené, vzpomněl si na mne, protože si pamatoval, jak jsem v kurzu opakovaně vítězil v soutěžích v luštění jednoduchých šifer. Vyžádal si od mých současných nadřízených na mne reference, a protože jsem byl vylíčen jako oddaný, spolehlivý a schopný šifrér, rozhodl se, že mne zaměstná ve svém oddělení. Po vyřízení příslušných formalit jsem přešel z armády na Ministerstvo vnitra a stal se technickým pracovníkem v oddělení vývoje kryptografických zařízení Zvláštní správy.

Zde jsem zpočátku (během zkušební doby) nedělal nic zajímavého a byl jsem trochu zklamán. Měl jsem však mnohem více volného času než u armády a byl jsem v Praze. Toulal jsem se po tomto nádherném městě a bylo mi dobře. Cítil jsem se mladý, silný a měl život před sebou. Rád jsem si večer poseděl ve vinárně a postupně se ukázalo, že i když jsem měl velmi slušný příjem, stačil jsem jej v tom velkoměstě snadno rozházet. Nemít problémy s penězi, byl jsem dokonale šťastný.

V roce 1957, tedy v době, kdy jsem byl u Zvláštní správy již zaměstnán 2 roky, byla vládou ČSR požádána sovětská strana o pomoc při výrobě šifrátoru. Sovětská strana vyhověla a počátkem listopadu 1957 dodala do Československa k testování dva kusy stroje, které měly představovat vzor pro výrobu šifrátoru s označením ŠD-2. Jednalo se o modifikaci ruského šifrátoru CM-1.

Již jsem měl rok po zkušební době a mjr. Sýkora mne zařadil do týmu, který měl za úkol provést kryptograficko-technický rozbor zařízení. Všichni jsme podepsali speciální závazek mlčenlivosti, protože nejen, že toto zařízení bylo označeno jako přísně tajné, ale byl zde navíc zájem sovětské strany chránit toto tajemství specifickým způsobem, protože zařízení bylo v Sovětském svazu masově používáno.

D. JAK SE STAL VÁCLAV PROKOPEC ZRÁDCEM

Václav opět po těžkém dnu ve vězení uléhal znaven na svůj kavalec. Před usnutím vzpomínal na dny před svým zatčením. Jak se to vlastně stalo, že přišel o tak zajímavou a dobře placenou práci, že zradil sebe, důvěru a práci svých kolegů - soudruhů a svoji vlast.

Václav byl již druhý rok v Praze. Skončila mu zkušební lhůta a začal pracovat jako plnohodnotný člen kryptografického oddělení. Pro jeho schopnosti kombinovat a luštit jej ing. pplk. Ondřej Sýkora „půjčoval“ majoru Hádkovi z kryptoanalytického oddělení. Václav sice přesně nevěděl, co zde dělají. Pouze předpokládal, že luští zachycené dálnopisy a radiodepeše, ale co skutečně umí luštit a co ne, to nevěděl. Cítil se ve společnosti kryptoanalytiků důležitý. Nevadilo mu, že mu byla dávána jen pomocná práce, kterou nikdo z odborníků nechtěl dělat. Konkrétně mu vždy přinesli svazek dopisů, které byly zasílány na podezřelé vytipované adresy (většinou v cizině). On měl za úkol je přečíst, a pokud se mu zdály nějaké divné, kostrbatě gramaticky napsané apod., tak provést jejich analýzu. Ta spočívala v tom, že vypsal do připravených tabulek např. všechna prvá písmena vět v daném dopise, pak druhá atd., potom obdobně vypisoval poslední, předposlední písmena. Skutečně se stalo, že písmena dávala smysl a někdo (Václav ovšem nevěděl o tom kdo a komu) takto předával utajený text. Kolegové mu jednou prozradili, že mimo tento opravdu jednoduchý systém se používá i mnohem důmyslnější, kdy vypsaná písmena na dohodnutém místě vět tvoří souřadnice šifrovací tabulky.

Viz příloha č.6: Zvláštní správa - analýza dopisů

A tak ubíhal den za dnem. Večer pak Václav chodil do své oblíbené hospůdky na pivo, večeři a pivo a pivo, ale někdy si chtěl zahrát na někoho důležitějšího a to pak šel po městě a hledal nějakou lepší vinárnu. Není divu, že vždy desátého, kdy dostávali výplatu, již netrpělivě čekal u okénka soudružky Hromové, která jim peníze vyplácela.

Byl teplý květnový večer roku 1957. Václav se procházel po Kampě a pak zašel do vinárny u Dvou grošů. Objednal si dvě deci bílého vína a rozhlížel se znuděně po místnosti. V tom uviděl u protějšího stolu svého spolužáka z měšťanky v Nečtinách Karla Webera. Bylo mu to trochu divné, myslel si, že byl odsunut tak, jako ostatní Němci z vesnice Stvolny, kde Karlův otec měl velký statek. Byl však rád, že vidí někoho známého, a protože tam Karel seděl sám, vstal a přisedl k němu. Strávili spolu zajímavý večer, povídali si a vzpomínali na školu a své spolužáky a spolužačky. Řeč přišla i na spolužačku Evu, která se Václavovi tolik líbila. Václav nechtěl kazit ten hezký večer, ale pak si našel odvahu a zeptal se, jak je to možné, že zde Karel je. Byl přece odsunut. Karel se zasmál a řekl: „Neboj, jsem zde legálně. Ale nechce se mi o tom mluvit.“ Jenže vypili další sklenku, tedy přesněji další džbánek a Václav zase stočil řeč na jeho návrat.

„Ty ses vrátil, Karle?“ Karel se na něj podíval a pak po chvilce řekl: „No a proč ne?“ „Myslel jsem, že to nejde“, pokračoval Václav. „Ale jde“ řekl na to Karel a pak mu vyprávěl svoji smyšlenou legendu. Spočívala v tom, že jej v Německu vyhledala naše československá rozvědka a chtěla na něm nějakou službu. Když to udělal, bylo mu dovoleno za odměnu vrátit se zpět do vlasti. Skutečnost však byla úplně jiná.

V Německu se jemu ani otci příliš nedařilo. Nakonec se Karel Weber nechal naverbovat americkou rozvědnou službou a působil jako spojka – agent chodec. Již několikráte úspěšně přešel hranice do Československa a pak zpět do Německa. Teď byl v Praze a měl zde za úkol kontaktovat dr.Hromadu a vyzvednout od něj nějaký balíček, který měl co nejdříve přivézt zpět. Měl se s ním sejít právě dnes v této vinárně. Jenže z nějakého důvodu dr. Hromada nepřišel. Právě když chtěl odejít, přisedl k němu jeho bývalý spolužák Václav. Dost dobře se nemohl nechat zapřít a odejít, a tak teď s ním popíjel to mizerné a předražené víno a musel dělat, jak je rád, že jej potkal a poslouchat ty banální vzpomínky a příhody z měšťanky. Vymyslel si kvůli němu i docela slušnou legendu. Věděl, že se zde lidé bojí tajné služby a rozvědky a určitě se jej Václav už na nic více asi nebude vyptávat. Je dost možné, že s ním dokonce nebude chtít mít nic společného. Jenže najednou se přihodilo něco, co skutečně nečekal. Václav se k němu naklonil, podal mu ruku a řekl: „Vítej, tak to jsme skoro kolegové! Já jsem totiž zaměstnán u šifrové služby na Ministerstvu vnitra“. „To není možné!“ reagoval Karel. Pak mu to hned došlo, proboha to je náhoda! Potkat kamaráda, který mu důvěřuje a který má přístup k šifrám. To je prostě náhoda, která se agentovi jen tak nepřihodí. Pokud se mu podaří Václava přimět ke spolupráci, dostanou se jeho chlebodárci k těm nejcennějším tajemstvím a on se z obyčejného agenta – chodce, který neustále riskuje, že bude chycen, stane důležitým a oceňovaným vyzvědačem, kterého budou krýt a po splnění úkolu jej bude očekávat slušná odměna a poklidný život někde v Alpách, kde si s otcem zakoupí malý vysněný statek a zde v klidu stráví zbytek života …

Ten večer se mu podařilo Václava parádně opít. Odvedl jej domů. Ráno pak na něj před domem čekal a rychle mu vysvětlil, že by nebylo dobře, aby se o setkání svým kolegům zmiňoval nebo to dokonce hlásil. Karlovi nadřízení také nechtějí, aby se opíjel po večerech. Navíc, jak by zase Václav vysvětlil, že se schází ve vinárně s odsunutým Němcem, synem statkáře. A říci „pravdu“, že mu jeho dávný spolužák Karel prozradil, že pracuje pro rozvědku, také říci nesmí. Jak by to asi vypadalo, že Karel každému na potkání o tom vypráví. A tak si navzájem slíbili, že o setkání pomlčí.

Karel pak v následujících dnech Václava sledoval, a když zjistil, že chodí pravidelně do blízké hospody a v pátek a sobotu do nějaké vinárničky, nebylo pro něj těžké se s ním zase jakoby náhodou sejít. Setkání a vzájemných flámů přibývalo. Karel začal za Václava platit. Ten zpočátku nechtěl, ale když už mu došly peníze, rád pozvání od kamaráda zase přijal. „Vy teda na té rozvědce jste dobře placeni“ komentoval Václav, když jej Karel zase pozval na flám a když Karel zdůraznil, že to samozřejmě zaplatí.

Na jednom z flámů dokonce Karel hostil Václava i s jeho nadřízeným ing. Ondřejem Sýkorou. Ten flám se o pár měsíců později stal inženýru Sýkorovi osudným. Jeho nadřízení mu vyčítali, že se více nezajímal, s kým vlastně jeho podřízený tráví večery a navíc na něm ulpělo i vážné podezření, že snad věděl, kdo skutečně Karel je a že se nějak sám zapletl.

Vše vypadalo idylicky, ale jen do okamžiku, kdy Karel zcela chladně zaútočil na Václava. „Václave, dost té komedie. Nejsem člen československé rozvědky, ale naopak rozvědky americké!“

Když se Václav vzpamatoval z počátečního šoku, tak jej Karel začal zpracovávat dále. „Opovaž se někomu něco říc! Copak by ti někdo věřil, že jsi trávil tři měsíce po vinárnách se spolužákem, o kterém jsi věděl, že byl odsunut do Německa a nepojal jsi podezření, že zde asi není legálně? Jak bys svým nadřízeným vysvětlil, že jsi nehlásil takový podezřelý styk? A vůbec, chceš si přece užívat. Vol rozumem a místo nepříjemností a možná vězení, ber peníze. Jsem schopen ti zajistit spoustu peněz, a pokud budeš chtít si je užít v bezpečí, zajistím ti i odchod za hranice. Cena je malá. Řekneš mi vše, co o té vaší šifrové službě víš.“

Václav Prokopec váhal, ale nakonec podlehl. V následujících týdnech postupně vyzradil některé informace o službě, kde byl zaměstnán, jak je organizována, jména kolegů, názvy akcí, o kterých věděl, o prováděné kontrole dopisů, které se zúčastnil a také, jaké šifrátory se v armádě používají.

Shodou okolností zrovna v té době dorazila ze Sovětského svazu dodávka dvou šifrátorů CM-1, které dostaly na Zvláštní správě kódové označení ŠD-2 (šifrový dálnopis verze 2). Do týmu, který dostal za úkol provést jeho kryptologicko-technický rozbor, zařadil ing.Ondřej Sýkora i svého oblíbeného podřízeného Václava Prokopce.

Václav velmi brzy pochopil obrovský význam, jaký mají plány tohoto šifrátoru, který byl v Sovětském svazu používán. Kontaktoval Karla a o šifrátoru mu řekl. Slíbil, že plány překreslí a vše, co mu bude o zařízení známo, předá. Současně si však vymínil, že to bude ta poslední věc, co pro něj udělá. Žádá za to pak ihned zařízení přechodu do Německa a slušnou sumičku peněz. Karel vše do centrály ohlásil, počkal na pokyny a za týden se s Václavem opět sešel.

Viz příloha č.7: Zpráva centrále

Oznámil mu, že je vše zařízeno. „Přines plány a budeme se bavit, kdy a kde přejdeš.“ Václav Karla nečekaně překvapil. Plány již měl obkresleny a dokonce je přinesl na schůzku s sebou. Beze slova je teď vyndal a zabalené v Rudém Právu je dal Karlovi. Po chvilce mlčení překvapenému Karlovi pak řekl: „Jsme tedy domluveni, zajisti mi odchod a příští pátek mi řekni, kdy a kde!“ S tím se také ten večer rozloučili.

Jenže pak se to stalo. Tím, že byl Václav zařazen do týmu, kde se požadovala absolutní mlčenlivost, protože sovětská strana přikládala předaným podkladům velký význam, bylo rozhodnuto o speciální prověrce všech účastníků projektu. Všichni byli v tajnosti prolustrováni. Kontrarozvědka zjišťovala, s kým se stýkají, kdo se kolem nich pohybuje a jaký vedou život. Tím se samozřejmě dostala na stopu Karlovi Weberovi.

Pak již šlo vše ráz na ráz. Na schůzku do vinárny U dvou hrochů, kde se měli oba spiklenci sejít a domluvit konkrétní datum útěku z republiky, již Karel nepřišel. Místo něj však přišli na místo setkání dva příslušníci státní tajné bezpečnosti a Václava Prokopce zatkli.

Zatčen byl druhý den i jeho nadřízený, protože dle vyšetřovatelů nebylo možné, aby netušil, že se děje něco nepatřičného. Navíc bylo zjištěno, že se sám jedné ze schůzek dokonce zúčastnil a přitom nic podezřelého nenahlásil. Nezodpovědně dokonce zařadil Václava Prokopce na jeden z nejdůležitějších úkolů odboru. Mělo se

však všeobecně za to, že Václav Prokopec byl zatčen dříve, než se pořádně seznámil s plány šifrátoru a že nebylo možné, aby je stačil obkreslit a předat cestou Karla Webera cizí rozvědce. Ing. Ondřej Sýkora sice tušil, že to mohl stihnout, neboť mu umožnil, aby se s plány seznámil ještě dříve, než celý projekt oficiálně startoval, ale ve vlastním zájmu mlčel a ani u soudu se o tom on nebo Karel Weber nezmínil.

Možná i díky tomu, že předané informace byly vyhodnoceny jako sice přísně tajné, ale přece jen takového rázu, že nemohly zásadním způsobem poškodit šifrovou službu a bezpečnost státu a také možná proto, že již končila krutá padesátá léta, nebyl v následujícím soudním procesu Václav Prokopec odsouzen k trestu smrti, dokonce ani na doživotí.

E. JAK BYL PROLOMEN ŠIFROVÝ TEXT ZAŠIFROVANÝ POMOCÍ CM-1

Šifrátor CM-1 byl na svoji dobu velmi dobrým kryptografickým zařízením. Z šifrového textu nešlo ani při znalosti dokonalého popisu šifrátoru jej prolomit. Ovšem dokonalý popis stroje umožnil americké rozvědné službě postavit jeho funkční repliku. Pak již stačilo úkolovat agenty, aby získali nastavení šifrátoru na příslušný měsíc. Pokud se jim jej podařilo získat, pak již snadno rozvědka dešifrovala všechny zachycené texty, které byly pod tímto klíčem zaslány. Šifrátory tohoto typu se v Sovětském svazu používaly dlouhých třicet let od roku 1956 do roku 1986. Během této doby se podařilo americké rozvědce klíče získat relativně často. Zejména díky seržantu Kulikovovi, který je po celých 15 let pravidelně dodával, ale to je již zcela jiný příběh.

Viz příloha č.8 Dešifrace ŠD-2 / CM-1

Příloha č.1: Úlohy z PVS

Pplk. ing. Ondřej Sýkora, který na PVS rozdal vybraným vojákům testy, se procházel uličkou mezi stoly a díval se, jak jednotliví vojáci pracují. Většinou rychle a snadno vyřešili úlohu číslo jedna. Většina skončila u úlohy dva. Úlohu tři nevyřešil téměř nikdo. Z dvaceti posádek, kde již testy předkládal, vyřešili úlohu jen dva vojáci.

Úloha č.1

Šifrový text
AKCIPEC JEXELA YNARBO INDORAN RTSINIM EJ YNEZIRDAN ISSYVJEN JUM

Úloha č.2

Šifrový text
14 x 1 x 19 x 5 =
19 - 9 : 12 : 1=
10 + 5 =
22 !=
10 + 5 + 4 - 14 : 15 : 20 : 5 =
4 - 5 x 12 - 14 + 9 : 11 : 21=
1 ! =
18 - 15 x 12 x 14 : 9 : 11 - 21 =

Úloha č.3

Šifrový text

```
d v q O A r R t
s s L I e K K y
a n S w s M j A
w I Z d J k S S
x L m k A i A t
D T v o V E N E
O e O D E v a g
A A V i c b C f
```

Proto byl asi tak překvapen, když jsem po asi dvaceti minutách odložil tužku a papír s výsledky mu předložil. Podíval se na ně, pak zvedl oči a řekl: „ Výborně desátníku! Jak se jmenujete?“

Odpověděl jsem: „ Desátník Václav Prokopec!“

„Budu si vás pamatovat“, pokračoval podplukovník. „Zatím tyto úlohy tak rychle nikdo nevyřešil. Mimochodem, vy hrajete šachy, že?“

„Jak to víte?“ zeptal jsem se udiveně.

„No přece jste tu úlohu řešil tak, že jste si písmena složil do šachovnice 8x8 a pak jste je seřadil podle chodu jedné z šachových figur. Přitom jste správně odhadl, která písmena jsou bezvýznamná, a těmi jste se dále nezabýval. Výborná práce."

Přitakal jsem: „Ano, máte pravdu soudruhu podplukovníku."
V podstatě měl skutečně pravdu. Postupoval jsem podobně, jak řekl, ale spíše než ten šachový přístup, jsem použil prosté hledání k vybranému písmenu jiné vhodné písmeno tak, aby výsledek dával smysl. Teprve potom jsem si všiml, že výsledný text tvoří cestu jedné z figur po šachovnici…

Řešení úloh č.1,č.2 a č.3 - Úlohy z PVS

Úloha č.1

Otevřený text:
Můj nejvyšší nadřízený je ministr národní obrany Alexej Čepička.

Přepis do mezinárodní abecedy
MUJ NEJVYSSI NADRIZENY JE MINISTR NARODNI OBRANY ALEXEJ CEPICKA

Systém: Celý text napsaný pozpátku
Upřesnění: testovací příklad pro uživatele
Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Kdo?
Správná odpověď: CEPICKA
Body: 1

Šifrový text
AKCIPEC JEXELA YNARBO INDORAN RTSINIM EJ YNEZIRDAN ISSYVJEN JUM

Úloha č.2

Otevřený text:
Naše síla je v jednotě dělníků a rolníků!

Přepis do mezinárodní abecedy
NASE SILA JE V JEDNOTE DELNIKU A ROLNIKU

Systém: jednoduchá záměna
Upřesnění: záměna písmen za čísla, pořadí písmena v abecedě určuje za jaké číslo je písmeno zaměněno (A=1, B=2,…), znaménka početních operací (x - + :) oddělují jednotlivá písmena, konec slova označuje znak =
Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: Co?
Správná odpověď: SILA
Body: 1

Šifrový text
14 x 1 x 19 x 5 =
19 - 9 : 12 : 1=

10 + 5 =
22 !=
10 + 5 + 4 - 14 : 15 : 20 : 5 =
4 - 5 x 12 - 14 + 9 : 11 : 21=
1 ! =
18 - 15 x 12 x 14 : 9 : 11 - 21 =

Úloha č.3

Otevřený text:
Ať žije československá lidová armáda.

Přepis do mezinárodní abecedy
AT ZIJE CESKOSLOVENSKA LIDOVA ARMADA

Systém: bloudění šachového jezdce po šachovnici
Upřesnění: spojité bloudění šachového koně, pokud to jde se zachování pohybu jedním směrem, začátek pole a1, písmena otevřeného textu zapsána velkými písmeny, klamače malými písmeny
Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (4)
Správná odpověď: LIDOVA
Body: 3

Sestavení (cesta koně označena červeně a velkými písmeny)

d	v	q	O	A	r	R	T
s	s	L	I	e	K	K	Y
a	n	S	w	s	M	j	A
w	I	Z	d	J	k	S	S
x	L	m	k	A	i	A	T
D	T	v	o	V	E	N	E
O	e	O	D	E	v	a	G
A	A	V	I	c	b	C	F

Šifrový text

```
d v q O A r R t
s s L I e K K y
a n S w s M j A
w I Z d J k S S
x L m k A i A t
D T v o V E N E
O e O D E v a g
A A V i c b C f
```

Příloha č.2: Administrativní kurz C v Tloskově 1

Po třech týdnech výuky, kdy jsme se seznámili především s jednoduchými šifrovacími systémy a jejich luštěním, nám při čtvrtečním večerním nástupu naší čety oznámil velitel npor. ing. Prachař:

„Soudruzi, zítra se bude konat soutěž v luštění jednoduchých úloh. Bude se jednat o systémy, s nimiž jste se během výuky seznámili. Zejména se podívejte na luštění jednoduché záměny, transpozice a Cardanovy mřížky. Věřím, že naše četa dopadne ze všech čet nejlépe. Nejlepší tři vojáci z celého kurzu pak dostanou povolení ke krátkodobému opuštění posádky a to hned příští víkend. Konkrétně od pátku 16.00 hod. do neděle 24.00 hod. Doufám, že mne nezklamete a ukážete, že jste výtečně připraveni! Pohov! Rozchod na ubikace!“

Úloha č.4

Šifrový text

```
IQUEI EUJZG KJUJZ JTEDE ESRKJ DFMPJ
PDNSR RKJDN SSJMP CFIDJ KYSRL YUYUE
CUYMP JUOYM ESNJL NMBQU DJMNZ FBNMP
JUNDJ MNDJK EIDNO FZGFS DEMPG KFIDE
UFQTE LYUNP FZMPU NIFLD NSTFP KNIYJ
QMGFS RYOQI EUJPF LMTFG KJSFU FIEQT
ZFMNL FDNEI GEKQG EKJZF DFPKN IYJZD
EUQMF GEPUK ZQCFG EQSTJ ZFMUK ZFDNU
YTEKN MPEUJ PFLFM FDFMB NKQCN MFMUE
QGEKJ ZTEQJ MJRJC NTFTK JCDNB GKEMP
KFITQ BJOYM FZDEU QIEMP JLNTB ESNJZ
DEUQB ERLNU YMJUJ PGKJS QCNSN LNIIE
BJSNK FJTSF UYUNC NMUEQ GKEPN MPJPD
NSNDD EMPCJ TMFZF ZTQMF DEMPN IFDDF
GKFMU FISQC FBFUQ ZTFBM GECFD NMFZJ
RKJDN SDNKF JTSNJ PJTGK EPNGE TECDF
GKJSQ CNSNB QLNIQ TPFKY MGELQ MFMPJ
BNLNE DYLNI NDJSF LFBMU FPFMU EQGKJ
SNOEC QCFZJ BNKJG KEPNU JLSFM TQGND
JDFGK JPFLQ UDNPK MPJPQ NZJRK JDNSF
BNQMN LQCFU MFBNG KEMPK FITYE DJUKJ
PGJDM PUNUY TEKNM PEUJP FLQXX
```

Úloha č.5

Šifrový text

```
ANACA UOSRA BOTVI MTAZP HPIPE EKZBN
EIZAP INSJR AOAOR HHOEA JTLHD AEANJ
INEOI TEOEY CELIO LSUKD TIIOC JNENI
RYADI RNOON PETIA PSPOZ NRAIN ETYLA
KPLKK VISPA ADUIA NTPIS ECDNV NRINP
ENTTA PKNVE OSPON AEYEI SITIA LLCRN
RMJOU ENENE ADRHH NONKU CSIRZ ONROR
TIAMR XDAHC TZIIN EOZTB ZSRVM TRNIA
NSORN IMTPA SIRAC HTEBY NSNBA EPTID
ZOTCS VLPIN OREAS AERVO ARMRM DEPRI
PCAZR OIKIE NTTZA HLOSN IOYUR CISUS
NOTSA SAIUI IEAEI TNDAM ACNOA SRENU
UDISC EVREA UGRCK JAXUV RHDEL AIAVN
IYBNE EUNUA VRIIK OOTAE ONKKO JUOAJ
ASOTI INZRE ZYVAA HVMAG ABAIC SYIAS
SASVL OMLRD SSCLJ IOAZI PLTEV ESACT
YEORD UOKSN ASSTR RSESJ PDEMI CLKTJ
OOIBZ JHECM ISACC UHOOU CIRCE HDRAE
VOTIN OKIOG ARIOR OKMOH EUNEL VCEAE
NJIIT PTHUP RTVPH COIRR EIHC
```

Úloha č.6

Šifrový text
DVQCHLRAT
SSDIENOUY
ANHWSLJA
WIVDJKUP
XLMKAINT
OUCVOISRD
CEEACVAG
ISTICBEF
FRVUACEJ

V pátek po soutěži si mne zavolal velitel kurzu pplk. ing. Ondřej Sýkora k sobě do kanceláře. Zaklepal jsem, vstoupil a předpisově se zahlásil.
Podplukovník Sýkora se na mne přátelsky podíval a řekl. „Soudruhu, zavolal jsem si vás, protože jste ze všech soutěžících vyřešil poslední úlohu nejdříve a to o dvě hodiny dříve než vojín na druhém místě. Jak je to možné?“

Chvíli jsem přemýšlel, zda to mám říci, ale pak jsem odpověděl.
„Soudruhu podplukovníku, při přípravě na soutěž jsem si důkladně prohlížel všechny příklady, které jsme během výuky probírali, ale vrátil jsem se i k úlohám, které jsem řešil, než jsem byl sem na kurz vybrán. Zvlášť pozorně jsem si prohlížel tabulku s uschovaným textem, který jsme měli odhalit. Když jsem dnes řešil soutěžní úlohy, uvědomil jsem si, že se sice jedná o jiný systém, ale že mají něco společného. Ta původní měla velikost 8x8, ta dnešní 9x8 (pokud počítám písmena CH a OU jako jedno). To však není to podstatné. Pak mi to došlo a měl jsem výsledek ihned před sebou. Pro mne ta třetí úloha (Cardanova mřížka) byla tou úlohou nejlehčí!“

„Blahopřeji! Prokázal jste vynikající paměť, úsudek a kombinační schopnosti. Jen tak dále! Ten opušťák za odměnu si opravdu zasloužíte!“

Když jsem od velitele kurzu odcházel, byl jsem na sebe pyšný a sliboval si, že vyhraji i další soutěž, abych prokázal, že mé vítězství nebyla jen náhoda….

Příloha č.3: Administrativní kurz C v Tloskově 2

Před novou soutěží, na kterou jsem se právě připravoval, mne kontaktoval kolega z kurzu, desátník Jan Jenčík.

„Můžeš mi, prosím, prozradit, jak jsi řešil tu záměnu a transpozici? Byl jsi tak hrozně rychle hotov…“

Usmál jsem se. „Honzo, u té transpozice jsem postupoval trochu jinak, než nás učili. Využil jsem toho, že je to cvičný příklad a nebude obsahovat nějaké anomálie. Nejprve jsem si určil pravděpodobnou velikost tabulky. Vzhledem k délce textu 594 musí být rozměr vytvořen kombinací 11*3*3*3*2. Takže např. 27*22, 33*18 apod. apod. Nepoužíval jsem však naučený postup, kdy si stanovím všechny možné tabulky a počítám poměr samohlásek a souhlásek v řádku. Řekl jsem si, že nám dali

úlohu lehce řešitelnou a rozměr nebude příliš velký. Co třeba 11*54? Jak to potvrdit? Vzhledem k tomu, že nám říkali, že běžný způsob vyplnění tabulky na úplnou je buď pomocí X nebo abecedou (ABCD…), tak jsem se zkusil podívat na ta X. V textu jsou dvě X a to na pozicích 216 a 378. Obě čísla jsou dělitelná 54 (beze zbytku). Pokud by tedy tabulka měla rozměr 11*54, budou v tabulce na posledním řádku! Takže jsem zajásal a řekl jsem si, že mám správný rozměr. Navíc sloupky s písmenem X budou těmi posledními v tabulce a tedy jsem je přehodil na pozice 10 a 11. Zbytek pak už byl dílem chvilky – prostě jsem přehazoval sloupky 1 až 9 tak, aby vznikaly čitelné skupiny a slova … Snad jen doplním, že jsem samozřejmě viděl, že čísla 216 a 378 jsou dělitelná beze zbytku také číslem 27 a možný rozměr by ze stejných důvodů mohl být 27*22, ale nezdálo se mi to pravděpodobné, protože by tabulka byla moc „široká“ a řešení by bylo zdlouhavé a tedy pro školní soutěž těžké…“

Honza mi poděkoval a pak se mě ještě znovu zeptal na tu jednoduchou záměnu. Usmál jsem se. „Víš, Honzo, zde není potřeba nic moc vymýšlet. Statistika, bigramové vazby, oblíbená skupina souhlásek STR. Prostě klasika. Nicméně ani tady jsem nepočítal statistiky. Trvalo by mi to moc dlouho. Prostě jsem uhodl několik slov. Nečteš noviny? Určitě tam bude něco o míru, válce, socialismu, dělnické třídě apod. Zkusil jsem tam některé z těchto slov dosadit a ejhle už to jelo jako po másle …“

Takových hovorů jsem během kurzu vedl se svými kolegy bezpočet. Všichni mi lichotili, jak jsem nadaný a jak perfektně luštím. Jinými slovy jsem byl favorit i do soutěže, kterou jsme měli zítra absolvovat. Bál jsem se, že neuspěji, a tak jsem prolistovával sešity a učil se a učil. Co by tam mohli jen dát?

Trochu mne proto překvapilo a zaskočilo, když při čtvrtečním večerním nástupu naší čety oznámil velitel npor. ing. Prachař:
„Soudruzi, velitel kurzu rozhodl, že výsledky v minulém kole byly špatné. Nařídil nám oznámit v jednotlivých četách, že soutěž proběhne opět pouze ze základních šifrových systémů. Musíte se v nich polepšit. Kdo tentokráte v časovém limitu tří hodin dvě z předložených úloh nevyřeší, bude převelen do speciální čety, kde bude veden speciální doškolovací výcvik, tak aby tito frekventanti uspěli alespoň v poslední soutěži na závěr kurzu a aby tedy kurz zdárně absolvovali. Věřím, že nikdo z mé čety nezklame a zůstane v ní až do konce kurzu! Dnes jděte spát brzy. Zítra soutěž začíná již v 8.00 na jednotlivých učebnách. Tři nejlepší frekventanti kurzu získají opět jako uznání za svůj výkon volno k opuštění posádky na příští víkend. Pozor! Pohov! Rozchod!“

Řešení úloh č.4,č.5 a č.6 - Úlohy z kurzu v Tloskově 1

Úloha č.4

Otevřený text:
Důvodová zpráva. Zákon O ochraně státních hranic, část jedna.
Rychlý vývoj výstavby socialismu v naší zemi staví naši národní bezpečnost před nové úkoly. Vítězství dělnické třídy a úspěchy budovatelské práce vedou k zesílení odporu poražené třídy a znovu se potvrzuje poučka, že svržení vykořisťovatelé se nesmiřují se svou porážkou a sahají ke krajním prostředkům, aby se znovu dostali k moci a znovu mohli vysávat pracující lid. Domácí reakce vyvíjí svou protistátní činnost, jak se ze zkušeností denně přesvědčujeme, v úzkém spojení se zahraniční reakcí a tak proti pokojně pracujícímu lidu, který spolu se stami-

liony lidí na celém světě svou prací bojuje za mír a proti válce, skupina nepřátel uvnitř státu i za hranicemi usiluje všemi prostředky o návrat panství vykořisťovatelů.

Přepis do mezinárodní abecedy

DUVODOVA ZPRAVA ZAKON O OCHRANE STATNICH HRANIC CAST JEDNA RYCHLY VYVOJ VYSTAVBY SOCIALISMU V NASI ZEMI STAVI NASI NARODNI BEZPECNOST PRED NOVE UKOLY VITEZSTVI DELNICKE TRIDY A USPECHY BUDOVATELSKE PRACE VEDOU K ZESILENI ODPORU PORAZENE TRIDY A ZNOVU SE POTVRZUJE POUCKA ZE SVRZENI VYKORISTOVATELE SE NESMIRU-JI SE SVOU PORAZKOU A SAHAJI KE KRAJNIM PROSTREDKUM ABY SE ZNOVU DOSTALI K MOCI A ZNOVU MOHLI VYSAVAT PRACUJICI LID DOMACI REAKCE VYVIJI SVOU PROTISTATNI CINNOST JAK SE ZE ZKUSENOSTI DENNE PRE-SVEDCUJEME V UZKEM SPOJENI SE ZAHRANICNI REAKCI A TAK PROTI POKOJ-NE PRACUJICIMU LIDU KTERY SPOLU SE STAMILIONY LIDI NA CELEM SVETE SVOU PRACI BOJUJE ZA MIR A PROTI VALCE SKUPINA NEPRATEL UVNITR STATU I ZA HRANICEMI USILUJE VSEMI PROSTREDKY O NAVRAT PANSTVI VYKORISTOVATELU XX

Šifrový text

```
IQUEI EUJZG KJUJZ JTEDE ESRKJ DFMPJ
PDNSR RKJDN SSJMP CFIDJ KYSRL YUYUE
CUYMP JUOYM ESNJL NMBQU DJMNZ FBNMP
JUNDJ MNDJK EIDNO FZGFS DEMPG KFIDE
UFQTE LYUNP FZMPU NIFLD NSTFP KNIYJ
QMGFS RYOQI EUJPF LMTFG KJSFU FIEQT
ZFMNL FDNEI GEKQG EKJZF DFPKN IYJZD
EUQMF GEPUK ZQCFG EQSTJ ZFMUK ZFDNU
YTEKN MPEUJ PFLFM FDFMB NKQCN MFMUE
QGEKJ ZTEQJ MJRJC NTFTK JCDNB GKEMP
KFITQ BJOYM FZDEU QIEMP JLNTB ESNJZ
DEUQB ERLNU YMJUJ PGKJS QCNSN LNIIE
BJSNK FJTSF UYUNC NMUEQ GKEPN MPJPD
NSNDD EMPCJ TMFZF ZTQMF DEMPN IFDDF
GKFMU FISQC FBFUQ ZTFBM GECFD NMFZJ
RKJDN SDNKF JTSNJ PJTGK EPNGE TECDF
GKJSQ CNSNB QLNIQ TPFKY MGELQ MFMPJ
BNLNE DYLNI NDJSF LFBMU FPFMU EQGKJ
SNOEC QCFZJ BNKJG KEPNU JLSFM TQGND
JDFGK JPFLQ UDNPK MPJPQ NZJRK JDNSF
BNQMN LQCFU MFBNG KEMPK FITYE DJUKJ
PGJDM PUNUY TEKNM PEUJP FLQXX
```

Systém: Jednoduchá substituce

Upřesnění: heslo pro záměnnou tabulku je Josif Vissarionovic Stalin.

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
J	O	S	I	F	V	A	R	N	C	T	L	B	D	E	G	H	K	M	P	Q	U	W	X	Y	Z
58	5	26	20	62	0	0	9	59	16	23	19	16	38	48	25	0	38	46	37	33	38	0	2	17	20

Frekvence jednotlivých písmen v šifrovém textu uvedeny ve třetím řádku tabulky. Tři nejfrekventnější odpovídají třem samohláskám otevřeného textu. Luštění by nemělo činit problém. V doprovodném textu ještě naznačeno, že lze v textu hledat slova politického charakteru tehdejší doby.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: slovo, které se v textu opakuje 3x
Správná odpověď: ZNOVU
Body: 2

Šifrový text

```
IQUEI EUJZG KJUJZ JTEDE ESRKJ DFMPJ
PDNSR RKJDN SSJMP CFIDJ KYSRL YUYUE
CUYMP JUOYM ESNJL NMBQU DJMNZ FBNMP
JUNDJ MNDJK EIDNO FZGFS DEMPG KFIDE
UFQTE LYUNP FZMPU NIFLD NSTFP KNIYJ
QMGFS RYOQI EUJPF LMTFG KJSFU FIEQT
ZFMNL FDNEI GEKQG EKJZF DFPKN IYJZD
EUQMF GEPUK ZQCFG EQSTJ ZFMUK ZFDNU
YTEKN MPEUJ PFLFM FDFMB NKQCN MFMUE
QGEKJ ZTEQJ MJRJC NTFTK JCDNB GKEMP
KFITQ BJOYM FZDEU QIEMP JLNTB ESNJZ
DEUQB ERLNU YMJUJ PGKJS QCNSN LNIIE
BJSNK FJTSF UYUNC NMUEQ GKEPN MPJPD
NSNDD EMPCJ TMFZF ZTQMF DEMPN IFDDF
GKFMU FISQC FBFUQ ZTFBM GECFD NMFZJ
RKJDN SDNKF JTSNJ PJTGK EPNGE TECDF
GKJSQ CNSNB QLNIQ TPFKY MGELQ MFMPJ
BNLNE DYLNI NDJSF LFBMU FPFMU EQGKJ
SNOEC QCFZJ BNKJG KEPNU JLSFM TQGND
JDFGK JPFLQ UDNPK MPJPQ NZJRK JDNSF
BNQMN LQCFU MFBNG KEMPK FITYE DJUKJ
PGJDM PUNUY TEKNM PEUJP FLQXX
```

Úloha č.5

Otevřený text:
Důvodová zpráva. Zákon O ochraně státních hranic, část dva.
Na naše území jsou vysíláni školení agenti, špioni a teroristé, aby organisovali sabotážní a teroristické sítě a aby spojovali zbylé příslušníky domácí reakce, kteří ve svém marném úsilí o zvrat našich poměrů spoléhají na válku proti vlastnímu národu. Je předním úkolem naší lidově demokratické národní bezpečnosti zabránit spojení domácích nepřátel s jejich spojenci za hranicemi a zneškodnit pronikání špionů, rozvratníků a jiných škůdců pracujícího lidu přes státní hranice. Je proto třeba věnovat zvýšenou pozornost ochraně státních hranic a prohloubit péči o orgány, které střežení hranic provádějí a které při tom již dosáhly řady úspěchů.

Přepis do mezinárodní abecedy
DUVODOVA ZPRAVA ZAKON O OCHRANE STATNICH HRANIC CAST DVA
NA NASE UZEMI JSOU VYSILANI SKOLENI AGENTI SPIONI A TERORISTE ABY ORGANISOVALI SABOTAZNI A TERORISTICKE SITE A ABY SPOJOVALI ZBYLE PRISLUSNIKY DOMACI REAKCE KTERI VE SVEM MARNEM USILI O ZVRAT NASICH POMERU SPOLEHAJI NA VALKU PROTI VLASTNIMU NARODU JE PREDNIM UKOLEM NASI LIDOVE DEMOKRATICKE NARODNI BEZPECNOSTI ZABRANIT SPOJENI DOMACICH NEPRATEL S JEJICH SPOJENCI ZA HRANICEMI A ZNESKODNIT PRONIKANI SPIONU ROZVRATNIKU A JINYCH SKUDCU PRACUJICIHO LIDU PRES STATNI HRANICE JE PROTO TREBA VENOVAT ZVYSENOU POZORNOST OCHRANE STATNICH HRANIC A PROHLOUBIT PECI O ORGANY KTERE STREZENI HRANIC PROVADEJI A KTERE PRI TOM JIZ DOSAHLY RADY USPECHU

Systém: Jednoduchá transpozice
Upřesnění: Úplná tabulka 54*11
Pořadí sloupců pro transpozici se získá vyčíslením hesla: JOSIFSTALIN
Klíč (po vyčíslení hesla): 5-8-9-3-2-10-11-1-6-4-7
Tabulka byla na úplnou doplněna pomocí X (dva znaky). Pomáhá při odhadu velikosti tabulky.
Dostatečná nápověda k řešení uvedena v doprovodném textu. Zejména je tam odhalena možná velikost tabulky a použití písmen X k doplnění na úplnou tabulku.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (1)
Správná odpověď: DUVODOVA
Body: 2

Šifrový text

```
ANACA UOSRA BOTVI MTAZP HPIPE EKZBN
EIZAP INSJR AOAOR HHOEA JTLHD AEANJ
INEOI TEOEY CELIO LSUKD TIIOC JNENI
RYADI RNOON PETIA PSPOZ NRAIN ETYLA
KPLKK VISPA ADUIA NTPIS ECDNV NRINP
ENTTA PKNVE OSPON AEYEI SITIA LLCRN
RMJOU ENENE ADRHH NONKU CSIRZ ONROR
TIAMR XDAHC TZIIN EOZTB ZSRVM TRNIA
NSORN IMTPA SIRAC HTEBY NSNBA EPTID
ZOTCS VLPIN OREAS AERVO ARMRM DEPRI
PCAZR OIKIE NTTZA HLOSN IOYUR CISUS
NOTSA SAIUI IEAEI TNDAM ACNOA SRENU
UDISC EVREA UGRCK JAXUV RHDEL AIAVN
IYBNE EUNUA VRIIK OOTAE ONKKO JUOAJ
ASOTI INZRE ZYVAA HVMAG ABAIC SYIAS
SASVL OMLRD SSCLJ IOAZI PLTEV ESACT
YEORD UOKSN ASSTR RSESJ PDEMI CLKTJ
OOIBZ JHECM ISACC UHOOU CIRCE HDRAE
VOTIN OKIOG ARIOR OKMOH EUNEL VCEAE
NJIIT PTHUP RTVPH COIRR EIHC
```

Úloha č.6

Otevřený text:
CHLADNOU HLAVU, PLANOUCÍ SRDCE A ČISTÉ RUCE

Přepis do mezinárodní abecedy
CHLADNOU HLAVU, PLANOUCÍ SRDCE A ČISTÉ RUCE

Systém: Cardanova mřížka
Upřesnění: mřížka odvozena z úlohy číslo 3

d	v	q	CH	L	r	A	T
s	s	D	I	e	N	OU	Y
a	n	H	w	s	L	j	A
w	I	V	d	J	k	U	P
x	L	m	k	A	i	N	T
OU	C	V	o	I	S	R	D
C	e	E	A	C	v	a	G
I	S	T	i	c	b	E	F
f	R	V	U	a	C	E	J

Na pozicích, které v úloze 3 byly součástí řešení (cesta koně) jsou umístěna písmena tvořící zprávu. K doplnění ostatních znaků byla použita nevýznamná písmena z úlohy 3. To že se jedná o stejná písmena, umožňuje nalézt řešení. Dostatečná nápověda k systému uvedena v doprovodném textu a to zejména odkaz na tabulku z úlohy 3.

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

Šifrový text
DVQCHLRAT
SSDIENOUY
ANHWSLJA
WIVDJKUP
XLMKAINT
OUCVOISRD
CEEACVAG
ISTICBEF
FRVUACEJ

Příloha č.4: Administrativní kurz C v Tloskově 3

I ve druhé soutěži jsem vyhrál. Úlohy byly opravdu lehké. No lehké, alespoň mně se to zdálo.

Úloha č.7

Šifrový text
```
ZQMJK JPJWX CVUDN OMVND YGJNO MVNDY
GJFJH PIDNH PIZXC ONZOM ZNJPK VIPED
XDOMD YTKMZ YFJHP IDNOD XFJPM ZQJGP
XDKMJ GZOVM DIZHV EDQID XJUOM VODOG
ZYVNQ ZJFJQ TYJWT OHJCJ PXZGZ CJNQZ
OVKMJ GZOVM DQNZX CUZHD NKJEO ZNZXX
```

Úloha č.8

Šifrový text
```
WORZX BMHBN PNRBS EZNKB DWWFL KADQQ
DHKZU HFBSX CXWLV LBRKM VLVVU BNLBB
LHSEZ NKBDW WFWLP ZRVDR VDMPZ GYXWP
FHSEQ FLTRP MIJHP JXNHX ZTKNJ FEEBR
JGINP VYNIK WGXKA YKBMS SEQES WIVIY
GOETV REXCE QCGEI NIWLB KOMWW HPZHV
UGIDB ESGAV BRJTB JVRTR LLAIQ FIGTN
VGOFK VEBOO XHJVI GGXJB CPVNB TKZSB
ENNTA GAVKL SQWCE ZXBRB CYQFL KAYIX
LXRLJ LGIEE XBLNP YWHNR TVCXG FUYQF
ENNPD ZWMLL DRLOA CRNCI OVZBC HVPRF
AFOAW MAVNT SHEMA VQFNR MCMNC VNTUB
VIUCK HESTP BBRDU DMAGL TTDLH EYGIQ
NHJTS BENNT AZMLJ PRVRN ZYIIS GVDMZ
AXVCW CKDYX QZGVN ZAGEB ZLUBU CEDDE
```

```
UAOGI AQVAD IOQDO XCAAL TPWGW ORPVR
HKEOK RDRMD DRLXM GGYGS IWQFN XNLHB
JRSGM PAEEL AIWLN LPLSI RZBVT TCSWE
CTMZA GJTST LYWDO XCAAL MFXBK MAGQY
AFAYQ SWLTD BESGY DIZWI RZBBK XVWWA
VRNPA UJHML HQAEI VWZMG IDBRF XJCCM
FXJDQ PZGAC WQFHS EQNKX PDIYA MEYBB
ETNTN RKMJP VMMOE CMWFB VUIMQ DULVT
DBCVM ZXKAY KBMSS VMZFX MPKXW FIEIY
KDEXD YSFSV MZSWA YAXWF
```

Úloha č.9

Šifrový text

```
NNSUE ISUYI AIKLN AETSI NAEOI TAYRA IOAIA OANAE OITCE IEAYP JVLZY ERSUN
KDMCR ACKEI EVMAN MSLOV ANSCP MRSOE AIAAK POILS NMNRD UOAUI TAVTR ULVNJ
HLPUE OHIAT RZIIU ERMES VRTEK EIAOY ISLIP LBIAO OSBAT SKISR RTIZT BSLVS
NGOBE SRRTI OPING IEOSN LSVOJ MZEAA
```

Hned na první úloze jsem získal časový náskok. Jak se totiž ukázalo, tak většina frekventantů úlohu řešila jako jednoduchou záměnu. To sice také vede k cíli, ale já jsem objevil cestu elegantnější a byl jsem hotov během několika minut i s přepsáním celého textu. Klasika je klasika … Druhá úloha byla, tak jak jsem očekával, na periodické heslo. Byl to můj oblíbený systém. Protože text byl dostatečně dlouhý a heslo krátké, tak nebyl problém získat z opakování velikost periody a příslušné abecedy (srovnané). Prostě Kasiského metoda vedla bezpečně k cíli. Třetí úloha mne trochu potrápila. Nejprve jsem nemohl rozpoznat systém. Bylo mi však jasné, že je to zase nějaká transpozice. Důvodem byla charakteristika šifrového textu. Jak jsem si s textem hrál, pochopil jsem, že to sice transpozice je, ale systém, který jsme se neučili. Není to totiž klasická šifra, ale spíše rébus. Asi jej do testu zařadili, aby zjistili, nakolik jsme všímaví a vzhledem k tomu, jak je to lehké, tak možná i proto, aby test splnilo co nejvíce účastníků.

Řešení úloh č.7,č.8 a č.9 - Úlohy z kurzu v Tloskově 3

Úloha č.7

Otevřený text:
Evropou obchází strašidlo - strašidlo komunismu - Nechť se třesou panující třídy před komunistickou revolucí! Proletáři nemají v ní co ztratit, leda své okovy. Dobýt mohou celého světa. Proletáři všech zemí, spojte se!

Přepis do mezinárodní abecedy
EVROPOU OBCHAZI STRASIDLO STRASIDLO KOMUNISMU NECHT SE TRESOU PANUJICI TRIDY PRED KOMUNISTICKOU REVOLUCI PROLETARI NEMAJI V NI CO ZTRATIT LEDA SVE OKOVY DOBYT MOHOU CELEHO SVETA PROLETARI VSECH ZEMI SPOJTE SE

Systém: Jednoduchá záměna, varianta na Caesarovu šifru

Upřesnění: posun abecedy o 5

```
Otevřená abeceda:  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
Šifrová abeceda:   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
```

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (3)
Správná odpověď: STRASIDLO
Body: 1

Šifrový text

```
ZQMJK JPJWX CVUDN OMVND YGJNO MVNDY
GJFJH PIDNH PIZXC ONZOM ZNJPK VIPED
XDOMD YTKMZ YFJHP IDNOD XFJPM ZQJGP
XDKMJ GZOVM DIZHV EDQID XJUOM VODOG
ZYVNQ ZJFJQ TYJWT OHJCJ PXZGZ CJNQZ
OVKMJ GZOVM DQNZX CUZHD NKJEO ZNZXX
```

Úloha č.8

Otevřený text:
Evropou obchází strašidlo – strašidlo komunismu. Ke svaté štvanici na toto strašidlo se spojily všechny mocnosti staré Evropy – papež i car, Metternich i Guizot, francouzští radikálové i němečtí policajti. Kde je opoziční strana, která by nebyla svými vládnoucími odpůrci vykřičena jako komunistická, kde je opoziční strana, která by opět potupnou výtku komunismu nevmetla ve tvář jak pokrokovějším opozičníkům, tak i svým reakčním odpůrcům? Z této zkušenosti vyplývá dvojí. Komunismus je již uznáván všemi evropskými mocnostmi za moc. Je svrchovaný čas, aby komunisté otevřeně před celým světem vyložili své názory, své cíle a své snahy a proti báchorkám o strašidle komunismu postavili manifest strany samé. Proto se v Londýně shromáždili komunisté nejrůznějších národností a sepsali tento manifest, jenž uveřejní v jazyku anglickém, francouzském, německém, italském, vlámském a dánském.

Přepis do mezinárodní abecedy
EVROPOU OBCHAZI STRASIDLO STRASIDLO KOMUNISMU KE SVATE STVANICI NA TOTO STRASIDLO SE SPOJILY VSECHNY MOCNOSTI STARE EVROPY PAPEZ I CAR METTERNICH I GUIZOT FRANCOUZSTI RADIKALOVE I NEMECTI POLICAJTI KDE JE OPOZICNI STRANA KTERA BY NEBYLA SVYMI VLADNOUCIMI ODPURCI VYKRICENA JAKO KOMUNISTICKA KDE JE OPOZICNI STRANA KTERA BY OPET POTUPNOU VYTKU KOMUNISMU NEVMETLA VE TVAR JAK POKROKOVEJSIM OPOZICNIKUM TAK I SVYM REAKCNIM ODPURCUM Z TETO ZKUSENOSTI VYPLYVA DVOJI KOMUNISMUS JE JIZ UZNAVAN VSEMI EVROPSKYMI MOCNOSTMI ZA MOC JE SVRCHOVANY CAS ABY KOMUNISTE OTEVRENE PRED CELYM SVETEM VYLOZILI SVE NAZORY SVE CILE A SVE SNAHY A PROTI BACHORKAM O STRASIDLE KOMUNISMU POSTAVILI MANIFEST STRANY SAME PROTO SE V LONDYNE SHROMAZDILI KOMUNISTE NEJRUZNEJSICH NARODNOSTI A SEPSALI TENTO MANIFEST JENZ UVEREJNI V JAZYKU ANGLICKEM FRANCOUZSKEM NEMECKEM ITALSKEM VLAMSKEM A DANSKEM

Systém: `periodické heslo, systém` Vigenerova šifra, délka textu 740

Upřesnění: periodické heslo STALIN
V doprovodném textu uvedena systém. Délka textu je dostatečná. Při malé délce periody (hesla) by nemělo dělat řešitelům řešení problém.

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

Šifrový text

```
WORZX BMHBN PNRBS EZNKB DWWFL KADQQ
DHKZU HFBSX CXWLV LBRKM VLVVU BNLBB
LHSEZ NKBDW WFWLP ZRVDR VDMPZ GYXWP
FHSEQ FLTRP MIJHP JXNHX ZTKNJ FEEBR
JGINP VYNIK WGXKA YKBMS SEQES WIVIY
GOETV REXCE QCGEI NIWLB KOMWW HPZHV
UGIDB ESGAV BRJTB JVRTR LLAIQ FIGTN
VGOFK VEBOO XHJVI GGXJB CPVNB TKZSB
ENNTA GAVKL SQWCE ZXBRB CYQFL KAYIX
LXRLJ LGIEE XBLNP YWHNR TVCXG FUYQF
ENNPD ZWMLL DRLOA CRNCI OVZBC HVPRF
AFOAW MAVNT SHEMA VQFNR MCMNC VNTUB
VIUCK HESTP BBRDU DMAGL TTDLH EYGIQ
NHJTS BENNT AZMLJ PRVRN ZYIIS GVDMZ
AXVCW CKDYX QZGVN ZAGEB ZLUBU CEDDE
UAOGI AQVAD IOQDO XCAAL TPWGW ORPVR
HKEOK RDRMD DRLXM GGYGS IWQFN XNLHB
JRSGM PAEEL AIWLN LPLSI RZBVT TCSWE
CTMZA GJTST LYWDO XCAAL MFXBK MAGQY
AFAYQ SWLTD BESGY DIZWI RZBBK XVWWA
VRNPA UJHML HQAEI VWZMG IDBRF XJCCM
FXJDQ PZGAC WQFHS EQNKX PDIYA MEYBB
ETNTN RKMJP VMMOE CMWFB VUIMQ DULVT
DBCVM ZXKAY KBMSS VMZFX MPKXW FIEIY
KDEXD YSFSV MZSWA YAXWF
```

Úloha č.9

Otevřený text:
Na naše území jsou vysíláni školení agenti, špioni a teroristé, aby organisovali sabotážní a teroristické sítě a aby spojovali zbylé příslušníky domácí reakce, kteří ve svém marném úsilí o zvrat našich poměrů spoléhají na válku proti vlastnímu národu.

Přepis do mezinárodní abecedy
NA NASE UZEMI JSOU VYSILANI SKOLENI AGENTI SPIONI A TERORISTE ABY ORGANISOVALI SABOTAZNI A TERORISTICKE SITE A ABY SPOJOVALI ZBYLE PRISLUSNIKY DOMACI REAKCE KTERI VE SVEM MARNEM USILI O ZVRAT NA-SICH POMERU SPOLEHAJI NA VALKU PROTI VLASTNIMU NARODU

Systém: transpozice zvaná „zepředu zezadu“
Upřesnění: střídavě se písmena otevřeného textu zapisují zepředu a zezadu čímž vznikne šifrový text
Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (3)
Správná odpověď: UZEMI
Body: 2

Šifrový text

```
NNSUE ISUYI AIKLN AETSI NAEOI TAYRA IOAIA OANAE OITCE IEAYP JVLZY ERSUN
KDMCR ACKEI EVMAN MSLOV ANSCP MRSOE AIAAK POILS NMNRD UOAUI TAVTR ULVNJ
HLPUE OHIAT RZIIU ERMES VRTEK EIAOY ISLIP LBIAO OSBAT SKISR RTIZT BSLVS
NGOBE SRRTI OPING IEOSN LSVOJ MZEAA
```

Příloha č.5: Administrativní kurz C v Tloskově 4

Náš čtyřměsíční kurz v Tloskově se blížil ke svému závěru. Ještě nás čekala poslední soutěž, závěrečné ústní zkoušky a pak slavnostní vyřazení.

Očekával jsem, že poslední soutěž bude významně těžší než dvě předchozí. Pilně jsem se učil všechny systémy, o kterých se naši přednášející zmínili. Díval jsem se na postup řešení takových systémů jako ÜBCHI, ADFGX, ADFGVX, PlayFair, BIFID, Fleisnerova mřížka, dvojitá transpozice apod. Pravda, systémy jsou náročné na luštění a tedy i na čas a dalo se předpokládat, že v soutěži nebudou, ale chtěl jsem být připraven.

Nakonec mne příklady trochu zklamaly. Dvě úlohy byly opravdu velmi lehké. Jednalo se o jednoduchou záměnu s převrácenou abecedou a druhá úloha byla zase obyčejná úplná transpozice a to dokonce v tabulce 23x23. Toto spočetla většina frekventantů. Ani jsem si ty příklady na památku, na rozdíl od všech ostatních, které jsem během svého kurzu řešil, nezaznamenal. Zajímavější byla pouze třetí ze soutěžních úloh tohoto kola.

Úloha č.10

```
98787 32971 26672 39694 96243 48672
69694 27915 38675 69469 19878 74862
42746 39186 87721 96946 53753 26651
57919 84542 73921 87329 78726 46919
87876 95747 64274 32727 15768 76263
96234 94778 76454 27244 57975 62786
21862 97388 73362 24512 38457 87341
96737 24579 49697 24667 53266 51987
38791 98787 48624 27463 53297 64697
23962 27867 27486 87351 53265 38218
33696 85432 15734 26854 12978 69427
34245 75692 46687 37378 74945 46263
96235 32973 87343 53227 91297 35126
86692 76348 66756 94675 69665 27686
68412 97274 96224 68515 71873 29787
26851 39491 95738 34268 57868 51984
54273 84937 56962 75397 86724 57942
78794 86219 12653 23869 62352 49493
42749 78744 93753 94919 87845 75653
23263 68876 47383 76753 57465 32973
88767 53265 32375 69466 51987 87486
24274 63651 98454 27756 26946 85191
52734 96227 23278 62182 79424 57915
46532 34945 46396 97276 56845 72394
6851
```

Tuto úlohu jsem vyřešil jako jediný. Pravda, s malou nápovědou. Jak jsem se však pak dozvěděl, tuto nápovědu měli na pokyn velitele k dispozici ve všech učebnách.

Náš velitel čety npor. ing. Prachař, který na nás jako vždy při soutěži dohlížel, napsal na tabuli bez jakéhokoliv vysvětlení podivnou sekvenci čísel 26532 6. Pak si sedl a chvílemi vyťukával prsty do desky stolu .../---/.../, tedy S O S. Jen jsem ze začátku nevěděl, zda SOS znamená pomoc jako takovou nebo snad přímo tu sekvenci na tabuli. Šifra se mi moc líbila. Ještě jsem o takovém systému neslyšel. O to více jsem si svého výsledku vážil.

Mimochodem ve vedlejší třídě velitel čety nápovědu dokonce ještě více rozšířil. Na tabuli napsal 26532 67245 721 a prsty do desky stolu vyklepával SOS SOS, pak udělal přestávku a zase vyťukal uvedená dvě slova SOS SOS (.../---/..././/.../---/..././/) .

Soutěž nakonec dopadla tak, jak jsem si přál. Předložené úlohy jsem opět vyřešil nejdříve ze všech frekventantů a tak jsem byl opět ze všech 300 účastníků nejlepší.

Při slavnostním vyřazení mne velitel kurzu ing. pplk. Ondřej Sýkora nechal předstoupit před všechny přítomné a poblahopřál mi za vynikající výkon.
Odpověděl jsem „Sloužím lidu!“ a zařadil se mezi ostatní frekventanty.

Následně jsem byl převelen do Tábora, kde jsem se stal armádním šifrérem.
To bylo těsně po měnové reformě roku 1953 …

Řešení úlohy č.10 - Úlohy z kurzu v Tloskově 4

Úloha č.10

Otevřený text:

Právě se vracím z Hradu od pana prezidenta. Dnes ráno jsem mu podal návrh na přijetí demise ministrů, kteří odstoupili 20. února t. r., a současně jsem panu prezidentovi navrhl seznam osob, kterými má být vláda doplněna a rekonstruována. Mohu vám sdělit, že pan prezident všechny mé návrhy, tak jak byly podány, přijal. Soudruzi a soudružky, dekrety jak propouštěcí, tak i jmenovací jsou panem prezidentem podepsány a za chvíli budou mnou kontrasignovány.

Přepis do mezinárodní abecedy

PRAVE SE VRACIM Z HRADU OD PANA PREZIDENTA DNES RANO JSEM MU PODAL NAVRH NA PRIJETI DEMISE MINISTRU KTERI ODSTOUPILI DVACATEHO UNORA T R A SOUCASNE JSEM PANU PREZIDENTOVI NAVRHL SEZNAM OSOB KTERYMI MA BYT VLADA DOPLNENA A REKONSTRUOVANA MOHU VAM SDELIT ZE PAN PREZIDENT VSECHNY ME NAVRHY TAK JAK BYLY PODANY PRIJAL SOUDRUZI A SOUDRUZKY DEKRETY JAK PROPOUSTECI TAK I JMENOVACI JSOU PANEM PREZIDENTEM PODEPSANY A ZA CHVILI BUDOU MNOU KONTRASIGNOVANY

Systém: zlomkový šifrový systém Morbit (text převedený do morseovky a následně rozdělený na dvojice znaků včetně dělících znaků a potom provedena záměna za čísla)

Upřesnění: klíč vyčíslení slova 'DVOULETKA'.

2 = ..	9 = .-	6 = .X
8 = -.	5 = --	3 = -X
7 = X.	4 = X-	1 = XX

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

Přepis otevřeného textu do Morseovky

```
.--./.-./.-/...-/.//..././/...-/.-./.-/-.-./../--//--..//..../.-

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

../!!-/.-/-.-//..//.---/--/./-./---/.../.-/-.-./../!.---/.../---

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

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

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

./--./-./---/.../.-/-./-.--//
```

Šifrový text (záměna dvojic znaků moreseovky dle klíče)

```
98787 32971 26672 39694 96243 48672
69694 27915 38675 69469 19878 74862
42746 39186 87721 96946 53753 26651
57919 84542 73921 87329 78726 46919
87876 95747 64274 32727 15768 76263
96234 94778 76454 27244 57975 62786
21862 97388 73362 24512 38457 87341
96737 24579 49697 24667 53266 51987
38791 98787 48624 27463 53297 64697
23962 27867 27486 87351 53265 38218
33696 85432 15734 26854 12978 69427
34245 75692 46687 37378 74945 46263
96235 32973 87343 53227 91297 35126
86692 76348 66756 94675 69665 27686
68412 97274 96224 68515 71873 29787
26851 39491 95738 34268 57868 51984
```

```
54273 84937 56962 75397 86724 57942
78794 86219 12653 23869 62352 49493
42749 78744 93753 94919 87845 75653
23263 68876 47383 76753 57465 32973
88767 53265 32375 69466 51987 87486
24274 63651 98454 27756 26946 85191
52734 96227 23278 62182 79424 57915
46532 34945 46396 97276 56845 72394
6851
```

Příloha č.6: Zvláštní správa - analýza dopisů

Když mi v roce 1956 skončila jednoletá zkušební lhůta na Zvláštní správě, začal jsem se pomalu zapracovávat. Naše oddělení mělo pravděpodobně trochu více volna, a proto mi ing. pplk. Ondřej Sýkora povolil drobnou stáž u majora Hádka na kryptoanalytickém oddělení.
Konkrétně jsem zde dělal na analýze tzv. dopisů. Jednalo se o dopisy, které byly zasílány na podezřelé vytipované, pravděpodobně krycí adresy (většinou v Německu nebo Rakousku). Měl jsem za úkol je přečíst, a pokud se mi zdály nějaké divné, kostrbatě gramaticky napsané apod., tak provést jejich analýzu.
Úplně první dopis, který jsem zachytil, byl tento. Z textu mi bylo na první pohled jasné, že se jedná o typ dopisu, který jsem hledal.

DOPIS č. 1 (úloha č.11)

```
Ahoj Romane.
Bývalý spolužák se chtěl se mnou sejít. Sjednat schůzku s ním a Marií bylo
lehké. Halenku si vzala na schůzku úplně novou. Vtipný jsem byl celý večer.
Potit jsem se však nepřestával. Pletl jsem se při oslovení Marie, to byl
trapas. Vylíčit jsem musel, proč. Motal jsem to. Perlou pak byl můj omyl.
Opil ses, zeptal se spolužák? Vrcholem bylo, když jsem musel odběhnout na
WC. Placení proběhlo dobře. Setkání pomalu končilo. Pletený svetr byl tep-
lý. Pohorky taky. Zbojnik byl vedle mne elegán. Množství alkoholu udělalo
své. Beseda probíhala otevřeně. Dotaz stíhal dotaz. Marné to však bylo.
Tkaloun u boty jsem si pořád přišlapával. Dovozel jsem Marii domů taxíkem.
Despota jsi, mně vyčetla. Hukot odjíždějícího taxíku nebylo slyšet. Adept
na cenu debila jsem byl jen já. Jehněčí povahu jsem nikdy neměl. Stokrát
jsem si to vyčítal. Tábor byl večer hežčí než Praha. Stichla překvapením.
Kategoricky však chtěla, abych odešel. Obejít se beze mne však nedokázala.
Osvětlení pokoje bylo docela slabé. Vlněné šaty měla na sobě úplně těsně.
Při tom ji slušely. Bohatší zážitky už jsem dlouho neměl. Chodit s Marií
jsem však příliš nechtěl. Volba by to nebyla dobrá. Obecně vzato by mi to
však možná nevadilo. Zato jí asi jo. Vlez mi na záda. Pecivále! Poklesla mi
překvapením brada. Elegantně jsem asi nevypadal. Piha na nose se jí chvěla.
Zlost se mnou lomcovala. Soptil jsem hněvem. Volíš divná slova! Touha mnou
najednou začala lomcovat. Krk měla odhalený. Vkusná blůzka byla napnuta na
jejích ňadrech. Zabavit se mi ji chtělo. Zbylo tu něco k pití? Zklamaně
řekla – NE. Tajemně jsem se usmál. Zaměstnat fantazii by bylo dobré. Obejít
se bez alkoholu? Fantasticky se začala bavit. Sbohem mi však řekla. Zdvihl
jsem se. Kradmo jsem se na ni podíval. Nenasytné rty měla sevřeny. Suma su-
márum, mám jít? Baječný večer, že? Herec jsi dobrý, řekla. Sotva jsem to
uslyšel. Krok jsem k ní udělal. Katastrofa se blížila. Pohovka se prohnula.
Sem tam, sem tam. Stichli jsme na chvíli. Muckali jsme se pak dále. Ach,
vykřikla! Kvas skončil. Melodie lásky mi ještě zněla v uších.
Příště Romane napíši, jak se náš vztah vyvíjí dále. Franta
```

Odhalit v textu uschovanou zprávu byla pro mne lahůdka. Ostatně by to asi velmi rychle zvládl každý, kdo znal, jak vypadají tyto klasické dopisní agenturní systémy. Stačilo provést klasickou analýzu znaků a byl jsem hotov.

Pamatuji si také na jeden dopis, který byl, pokud jde o styl, opět typický pro agenturní dopisní systémy. Jenže již zde ležel týden a nikdo z oddělení jej dosud nedešifroval. Půjčil jsem si jej a začal jej analyzovat. Tentokrát to bylo mnohem složitější. Především byla porušena „nepsaná“ zásada těchto typů dopisů, totiž že se ukrývalo v nějakém slově podle určitého předpisu jedno písmeno. Navíc zde ten předpis byl dynamický. Již to nebylo ono klasické prvé písmeno ve větě nebo poslední písmeno v každé větě… Nicméně to neodolalo a já ukrytou zprávu odhalil. Za odhalení této zprávy jsem dokonce dostal zvláštní peněžní odměnu. Nutno říci, že mi hodně pomohlo si všímat chyb a atypických slov. Určitě bych pro zprávu, která zde byla ukryta, dokázal napsat dopis tak, aby při letmé kontrole nikdo nepřišel na to, že obsahuje vloženou zprávu a ne takto hloupě jako v tomto případě…

DOPIS č. 2 (úloha č.12)

```
Ahoj Josefe,
Jak asi víš, přestěhoval jsem se do Plzně.
Ale na ten nový byt si nemohu zvyknout.
Tomáš mi půjčil na stěhování své auto.
Den mi trvalo, než jsem všechno přivezl.
Stejně se mi chtělo brečet, když jsem ten náš domeček opouštěl.
Vždyť se mnou jsi tam taky strávil tolik let!
Čekal jsem, že si v Plzni zvyknu na nový byt rychleji.
Stačilo ke stažení hrdla si jen vzpomenout na rodný domeček.
A byl jte se tam vůbec podívat?
Nás to ani nenapadlo.
Snad za pár let zapomenu.
Pokud však mě zdraví dovolí, pak bych se tam na důchod vrátil.
Síc to jinak žalem nevydržím!
Zatím se však trápit zbytečně nebudu.
V tom dmé si nemohu zvyknout.
Hodiny sedím a přemýšlím, zda jsem musel opravdu z naší rodné vesnice ode-
jít.
Snad družstvo nebyl tak špatný záměr.
Říkám si žte, jsem nemusel hned nesouhlasit a počkat, jak to dopadne.
Pak si zase říkám, ale co.
Vpů lce života se již jeho styl mění velmi těžce.
Tak zatím Ota
```

Řešení úloh č.11 a č.12 - Zvláštní správa - analýza dopisů

Úloha č.11

Otevřený text:
Velitel třicátého ostravského bitevního leteckého pluku byl jmenovám mjr. Toth Michal.

Upřesnění: Text je uschován v dopise tak, že se k zápisu otevřeného textu použije třetí písmeno v prvním slově každé věty. Dostatečná nápověda uvedena v doprovodném textu, kde je uveden klasický postup při analýze a hledání textu uschovaného v dopise.

Nápověda pro výběr slova dokazujícího, ze řešitel úlohu vyluštil: (3)
Správná odpověď: OSTRAVSKEHO
Body: 2

Šifrový text

```
Ahoj Romane.
Bývalý spolužák se chtěl se mnou sejít. Sjednat schůzku s ním a Marií bylo
lehké. Halenku si vzala na schůzku úplně novou. Vtipný jsem byl celý večer.
Potit jsem se však nepřestával. Pletl jsem se při oslovení Marie, to byl
trapas. Vylíčit jsem musel, proč. Motal jsem to. Perlou pak byl můj omyl.
Opil ses, zeptal se spolužák? Vrcholem bylo, když jsem musel odběhnout na
WC. Placení proběhlo dobře. Setkání pomalu končilo. Pletený svetr byl tep-
lý. Pohorky taky. Zbojnik byl vedle mne elegán. Množství alkoholu udělalo
své. Beseda probíhala otevřeně. Dotaz stíhal dotaz. Marné to však bylo.
Tkaloun u boty jsem si pořád přišlapával. Dovozel jsem Marii domů taxíkem.
Despota jsi, mně vyčetla. Hukot odjíždějícího taxíku nebylo slyšet. Adept
na cenu debila jsem byl jen já. Jehněčí povahu jsem nikdy neměl. Stokrát
jsem si to vyčítal. Tábor byl večer hežčí než Praha. Stichla překvapením.
Kategoricky však chtěla, abych odešel. Obejít se beze mne však nedokázala.
Osvětlení pokoje bylo docela slabé. Vlněné šaty měla na sobě úplně těsně.
Při tom ji slušely. Bohatší zážitky už jsem dlouho neměl. Chodit s Marií
jsem však příliš nechtěl. Volba by to nebyla dobrá. Obecně vzato by mi to
však možná nevadilo. Zato jí asi jo. Vlez mi na záda. Pecivále! Poklesla mi
překvapením brada. Elegantně jsem asi nevypadal. Piha na nose se jí chvěla.
Zlost se mnou lomcovala. Soptil jsem hněvem. Volíš divná slova! Touha mnou
najednou začala lomcovat. Krk měla odhalený. Vkusná blůzka byla napnuta na
jejích ňadrech. Zabavit se mi ji chtělo. Zbylo tu něco k pití? Zklamaně
řekla – NE. Tajemně jsem se usmál. Zaměstnat fantazii by bylo dobré. Obejít
se bez alkoholu? Fantasticky se začala bavit. Sbohem mi však řekla. Zdvihl
jsem se. Kradmo jsem se na ni podíval. Nenasytné rty měla sevřeny. Suma su-
márum, mám jít? Baječný večer, že? Herec jsi dobrý, řekla. Sotva jsem to
uslyšel. Krok jsem k ní udělal. Katastrofa se blížila. Pohovka se prohnula.
Sem tam, sem tam. Stichli jsme na chvíli. Muckali jsme se pak dále. Ach,
vykřikla! Kvas skončil. Melodie lásky mi ještě zněla v uších.
Příště Romane napíši, jak se náš vztah vyvíjí dále. Franta
```

Úloha č.12

Otevřený text:
Jana půjde se mnou. Čekejte nás za měsíc sedmého. Držte palce. Ota

Upřesnění: Opět se jedná o agenturní systém, kdy se otevřený text steganograficky ukryje do dopisu. Tentokráte se využívají postupně prvé slabiky slov ve větách a to v pořadí slabika prvního slova ve větě, slabika druhého slovo v následující větě a nakonec slabika ve třetím slově ve větě. Systém se pak dále periodicky opakuje.
Nápověda uvedena v doprovodném textu, kde je uvedeno, že text je uschován nikoliv rozdělený na jednotlivá písmena (běžný postup), ale na celé slabiky. Luštitel je upozorněn, že se má všímat zejména podezřelých slov.

Nápověda pro výběr slova dokazujícího, ze řešitel úlohu vyluštil: Kdy?
Správná odpověď: SEDMEHO
Body: 4

Sifrový text

```
Ahoj Josefe,
Jak asi víš, přestěhoval jsem se do Plzně.
Ale na ten nový byt si nemohu zvyknout.
Tomáš mi půjčil na stěhování své auto.
Den mi trvalo, než jsem všechno přivezl.
Stejně se mi chtělo brečet, když jsem ten náš domeček opouštěl.
Vždyť se mnou jsi tam taky strávil tolik let!
Čekal jsem, že si v Plzni zvyknu na nový byt rychleji.
Stačilo ke stažení hrdla si jen vzpomenout na rodný domeček.
A byl jte se tam vůbec podívat?
Nás to ani nenapadlo.
Snad za pár let zapomenu.
Pokud však mě zdraví dovolí, pak bych se tam na důchod vrátil.
Síc to jinak žalem nevydržím!
Zatím se však trápit zbytečně nebudu.
V tom dmé si nemohu zvyknout.
Hodiny sedím a přemýšlím, zda jsem musel opravdu z naší rodné vesnice ode-
jít.
Snad družstvo nebyl tak špatný záměr.
Říkám si žte, jsem nemusel hned nesouhlasit a počkat, jak to dopadne.
Pak si zase říkám, ale co.
Vpů lce života se již jeho styl mění velmi těžce.
Tak zatím Ota
```

Příloha č.7: Zpráva centrále

Během vyšetřování bylo prokázáno, že Karel Weber komunikoval s centrálou pomocí šifrového spojení. Za tím účelem byl vybaven následující převodovou tabulkou a bločkem hesel. Tabulka i bloček byly přiloženy jako přílohy k vyšetřujícímu spisu.

	0	**1**	**2**	**4**	**6**	**7**	**8**	**9**		
-	D	E	I	N	S	T	A	R	Weber	57130 19
3	B	C	F	G	H	K	L	M	Heslo	34089 23
5	O	P	Q/J	U	V	W	X/Y	Z	šifra	81119 32

Obžalovaný Weber tvrdil, že žádnou zprávu nestačil odeslat. Zpravodajské službě se také žádný telegram, který by odpovídal této šifře, nepodařilo zachytit. Bloček s heslovým materiálem (http://soutez2009.crypto-world.info/pribeh/blocek.txt) byl neporušený. Vyšetřovatelům byl znám pokyn, že heslové skupiny, které byly použity k vytvoření šifrového textu, mají být ihned zničeny, a proto uvěřili, že Weber žádnou zprávu centrále neodeslal. I to byl jeden z důvodů, proč se předpokládalo, že informace o analyzovaném šifrátoru ŠD-2 / CM-1 nebyly předány cizí rozvědce.

Skutečnost však byla jiná. Weber centrále pravidelně zprávy zasílal. Informoval v nich o naverbování Václava Prokopce a zaslal do centrály vše, co se od něj dozvěděl. Z bločku však spotřebovaná hesla nevytrhával. Vždy si pouze zapamatoval, kde skončil a při přípravě nové zprávy začal s pěticí na novém řádku. Tím si zajistil, že heslo nebylo nikdy použito dvakrát. Ze školení, kterým prošel, věděl, že v takovém případě nelze z šifrového textu zprávu vyluštit, a proto mu vytrhávání hesel připadalo nadbytečné. Heslový materiál mu zbýval ještě na několik zpráv.

Poslední zpráva, kterou odeslal, byla tato:

```
68576 77942 06114 43386 56023 74203 22741 66582 02226 13131 15890 66109
96557 20241 42904 12392 12984 70271 69657 78286 29296 00944 79991 19559
02306 94898 73939 34036 80892 35887 69559 31457 97026 13827 88962 80230
76938 94373 84895 78410 92618 94152 62805 91699 01170 62473 21551 37649
17124 18980 36924 89892 20370 25273 68133 02387 70637 66963 53819 88797
02705 51891 50361 67559 17921 14809 42001 68270 83314 91067 31520 82976
```

Před zatčením se mu podařilo uschovat rozbor a plán šifrátoru do mrtvé schránky, kde byly kurýrem cizí rozvědky vyzvednuty a odvezeny do centrály. Tajemství šifrátoru ŠD-2 / CM-1 tak bylo vyzrazeno a to umožnilo americké rozvědné službě postavit jeho funkční repliku. V následujících letech se pak rozvědce opakovaně podařilo získat klíčový materiál a dešifrovat řadu důležitých zpráv.

Řešení úlohy č.13 - Zpráva centrále

Úloha č.13

Otevřený text:
Desátého října. Objekt má pracovat na rozboru sovětského šifrátoru CM jedna. Slíbil předat kompletní plány a rozbor. Setkám se s ním opět za týden. Po předání již nechce zůstat, žádá o zajištění přechodu do Německa a vysokou odměnu. Plány uložím v mrtvé schránce na hřbitově. Zajistěte vyzvednutí. Weber

Převod do mezinárodní abecedy
DESATEHO RIJNA OBJEKT MA PRACOVAT NA ROZBORU SOVETSKEHO SIFRATORU CM JEDNA SLIBIL PREDAT KOMPLETNI PLANY A ROZBOR SETKAM SE S NIM OPET ZA TYDEN PO PREDANI JIZ NECHCE ZUSTAT ZADA O ZAJISTENI PRECHODU DO NEMECKA A VYSOKOU ODMENU PLANY ULOZIM V MRTVE SCHRANCE NA HRBITOVE ZAJISTETE VYZVEDNUTI WEBER X

Upřesnění:
Jedná se o skutečný agenturní šifrový systém, který agenti německé rozvědky BND využívali na území bývalého NDR, PLR a Československa.
Otevřený text se nejprve převedl pomocí jedno-dvoumístné číselné záměny. K tomu se používala zde uvedená tabulka, nazývána DEIN STAR. Následně se k získanému textu přičetlo jednorázové heslo. Získaný šifrový text je z hlediska luštění absolutně bezpečný, pokud byla dodržena příslušná pravidla (heslo použitou pouze jednou, heslo zničeno, heslo náhodné a stejně pravděpodobné a nepredikovatelné).

	0	1	2	4	6	7	8	9		
-	D	E	I	N	S	T	A	R	Weber	57130 19
3	B	C	F	G	H	K	L	M	Heslo	34089 23
5	O	P	Q/J	U	V	W	X/Y	Z	šifra	81119 32

Algoritmus systému je zcela zřejmý z tabulky, kde je uveden drobný příklad. Vzhledem k tomu, že řešitelé si mohli stáhnout bloček s hesly, znamená to, že se vlastně jedná o jednoduchou úlohu dešifrace. Na šifrový text se postupně aplikují hesla v bločku. Pokud by vyšel možný text (některé kombinace nejsou vzhledem k převodové tabulce možné) je

potřeba se podívat, zda je výstup čitelný – pokud ANO – jedná se o řešení. V tomto případě řešitel musel prokázat, že je schopen sestavit takovýto jednoduchý program, protože hesel v bločku bylo uvedeno hodně a manuální zkoušení by bylo velmi, velmi pracné.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (3)
Správná odpověď: OBJEKT
Body: 12

Aplikace převodové tabulky DEIN STAR
0168713650 925248 5030521377 398 519831505687 48 950593050954 650561763713650 623298750954 3139 521048 638230238 5191087 37503951381742 51388458 8 9505930509 61737839 61 6 4239 505117 598 758014 5150 51910842 52259 413136311 59546787 59808 50 59852267142 5191313650054 050 4139131378 8 5658650375054 500391454 51388458 54385059239 56 3997561 63136984311 48 369302750561 59852267171 565859561045472 5713019 58

Rozdělení do pětic

```
01687 13650 92524 85030 52137 73985 19831 50568 74895 05930 50954 65056
17637 13650 62329 87509 54313 95210 48638 23023 85191 08737 50395 13817
42513 88458 89505 93050 96173 78396 16423 95051 17598 75801 45150 51910
84252 25941 31363 11595 46787 59808 50598 52267 14251 91313 65005 40504
13913 13788 56586 50375 05450 03914 54513 88458 54385 05923 95639 97561
63136 98431 14836 93027 50561 59852 26717 15658 59561 04547 25713 01958
```

VYBRANÉ HESLO Z BLOČKU:

```
67999 64392 14690 68356 04996 01328 13910 16024 38431 18201 65946 01153
89920 17691 80685 35893 68671 85061 21029 55263 44105 02217 29606 06742
60893 16440 94434 41086 94729 67591 53136 46406 80538 48026 43812 39320
92786 79432 53532 67925 56931 45354 12317 49432 97929 71160 66556 97145
04211 05202 80448 39527 25920 22369 14620 24939 26352 61040 68280 91236
49679 63460 46535 74532 67460 65057 26394 53622 34853 97520 16817 81028
```

```
Součet = Šifrový text:
68576 77942 06114 43386 56023 74203 22741 66582 02226 13131 15890 66109
96557 20241 42904 12392 12984 70271 69657 78286 29296 00944 79991 19559
02306 94898 73939 34036 80892 35887 69559 31457 97026 13827 88962 80230
76938 94373 84895 78410 92618 94152 62805 91699 01170 62473 21551 37649
17124 18980 36924 89892 20370 25273 68133 02387 70637 66963 53819 88797
02705 51891 50361 67559 17921 14809 42001 68270 83314 91067 31520 82976
```

Bloček: (ukázka 39 řádek, modře vyznačené vybrané heslo, soutěžní bloček měl 1421 řádek) http://soutez2009.crypto-world.info/pribeh/blocek.txt

```
61798 20831 40657 23475 61325 35232
19804 47629 36508 27565 80686 63289
72623 62085 06532 71382 57680 28663
29559 23596 90401 69604 47502 85938
39123 55672 01508 84206 16239 61826
36316 92012 19867 89967 80596 93810
88167 94260 21279 92725 36475 74417
12513 99976 24176 19028 96049 59897
14520 11672 17269 71913 88604 68092
27916 05860 58326 67526 36982 72404
51786 15091 06285 36262 13962 75639
67999 64392 14690 68356 04996 01328
```

```
13910 16024 38431 18201 65946 01153
89920 17691 80685 35893 68671 85061
21029 55263 44105 02217 29606 06742
60893 16440 94434 41086 94729 67591
53136 46406 80538 48026 43812 39320
92786 79432 53532 67925 56931 45354
12317 49432 97929 71160 66556 97145
04211 05202 80448 39527 25920 22369
14620 24939 26352 61040 68280 91236
49679 63460 46535 74532 67460 65057
26394 53622 34853 97520 16817 81028
87666 74112 34068 87402 50443 81172
35610 16328 76869 78642 56054 82043
29931 97920 89561 20562 13629 75955
06920 18820 48321 34385 06508 36922
60595 91938 64434 06389 25059 83292
74549 38061 80824 53664 32293 93605
22756 04981 39817 48567 16283 62601
64535 40675 47959 17539 42351 17242
40465 74972 41088 93664 47990 87243
56657 99236 11352 84017 62553 66343
65396 45782 38481 31210 56325 74479
89839 50413 19253 69938 25135 40201
43959 32422 04810 62631 88974 76358
43649 01355 11799 23841 74482 35906
68538 46092 55667 91939 69764 36890
52438 09791 08386 68062 97498 13857
```

Příloha č.8 : Dešifrace ŠD-2 / CM-1

Šifrátor ŠD-2, který byl v Sovětském svazu znám pod krycím jménem CM-1, byl velmi dobrým kryptografickým zařízením. Ze zachycených šifrových textů nešlo ani při znalosti dokonalého popisu šifrátoru získat luštěním otevřený text. To potvrdily i současné kryptografické rozbory (např. Brtník, V. : Rekonstrukce šifrovacího stroje ŠD-2, Crypto-World 7-8/2009).

Prokopcem předaný popis stroje umožnil americké rozvědné službě postavit jeho funkční repliku. Také se jim podařilo získat ke spolupráci seržanta Kulikova, který byl armádním šifrérem a stroj obsluhoval. Spolupráce se jim dařila celých dlouhých 15 let tajit a on jim pravidelně dodával nastavení šifrátoru. Pak již nebylo pro centrálu obtížné dešifrovat zachycené telegramy, které byly pod tímto nastavením zašifrovány.

Seržant Kulikov nastavení šifrátoru vždy dohodnutým způsobem zformátoval a částečně zašifroval. Pak toto nastavení ponechal v mrtvé schránce, odkud jej vyzvedl jiný agent a zajistil jeho předání centrále. Zde je příklad, který dokladuje, jak takovéto zprávy vypadaly. Toto je nastavení na listopad a prosinec roku 1965:

```
BEGIN1
PHIMB ADHJX UAZAJ YMTNM JTMKX NAJAS
BMTHB VNMDA JTHPM IMPBH JANXC ZMJAD
MUOXK IHUDV KXNXU SHBUM TVTXN THYBM
TXJXC HUUVT MTAHN SADDA NEJXT BHKNM
```

```
CHUUV TMTAH NSADD ANEMN EDXJF HINHT
MCAJX DHIOX INXIH OXIXN MCTAO XVBCX
NMPBX ICFHZ AUAPB KNAUA OXIXN MCTAP
BXIMN GUAFX JDGPH YVIOX NXUMT XJCFH
KMNGJ TMCAJ PBMKN XBHZD VJTAT UXPBX
ICFHZ AZPBM KGOXI NMMZO XIXNM CTPBX
KHIHK MTMWV DYMTX THJAS BGOXO MYHHW
KGYDX NMJTM KXNAC HUUVT MTHBV IKHOA
CXUAU HTMWV DYVOJ HVVKX IXNGK CMJTA
IKXAE HBYVD AYHK
END1
BEGIN2
Q=Q W=L X=R Z=Z
1 00000000000000000000000000
5 11000001000001100001001000
3 00010000000001000011010000
4 00010001010010000000000100
2 01010001000000000001000010
R 00000000000000000000000000
SADDA NE 123456
IAJCM NEDXJ 7891011
END2
```

Díky replice šifrátoru a získaným klíčům dešifrovala rozvědka celou řadu důležitých telegramů. Jako ukázka je uveden přísně tajný telegram, který byl poslán z pražské ambasády do Moskvy a informuje se v něm o velmi závažném rozhodnutí.

```
SUPPM IPFKI RBKRU PXKOJ BYAOV MUEOB XYHGD UQFQW PFBQU JTDRU IMTNA BWRQO
DUBJR XQIOQ ISBWC YCENW MDBXW BOBFY DIWCR MPPYM LIZMA YDPYV DYUYI EBCOW
KTJUF JMQDE WHUVF RANFX WBVIS FZDTQ MORHD QEROE NRIKV NEPOC MKRVB ZQAKQ
EKWID BYMIU XMWKC VYZHQ XHXNE ZBPKS TTVVK XNCEF ALXUF HDMAG XRECX UXRHJ
NCHQD GAENS CBXVP TADPY OCEOV XTXRP UEGTK TTKXL TYFCV WQBIP IGXEY SQKOD
GQZSP NZBVS OGYBK YJWAC VWNVN ALMYX ZXETI DUFJA THERE TZJTH IVGRN DAXZP
NBLKK WUSDE LOCZA RRWOH WJQLA KQXMZ YBRVP XPIVA XINXO VWPGO KRBEQ AQSAZ
FEGEH ZMJLF CDFLL MUIRP HEMRZ LZVRT RQKSA EHPLF HJYST HUZBE KXPIU PAYYU
PURKX OVOAN MMUOI VJCKW LHIRM QDHQS EROQC NRAER PNQRX GKGKG MWBTH GYUPL
BMRKF NNLVG PITVC OGCZE KUEAY HOEXV XSTPE RXZES PUJLS LJHUH WKWYJ GKVYF
TRNVC OAWXV WQBIE AXVHN KVQHE ZQYEM BXBCI RNOGB IRYDC TQPZZ QQYND MFLVF
QOZYU IVKYC RNIDZ WIDDA TLSSK ONBPK EHIBW YOMZS QSSAZ EKDVE EFMFS SUMXS
LXKRD MIAKD LJSLU YORYK DFNCG ABAOW FLKDT QEYMZ GZMJQ RBHHR HYIOQ GXKTD
JWLNM JIOZG ECTTK AHQXC DLMNB XPFEL TOKZD XQBXH GWXLQ FGHEK XMHGP SIWDD
LYGZJ SURDL PCSYT SSOGO QTNPO WGOQD AFGBD AKEPZ FHWFK QDOXQ VLRTR HFEBA
JAESJ WELPX DDHIZ HNTKH MWSBY IKFDY JKDES KGZKL NMBJH ALJSV TMBDU KDBSI
VDZEF UXFBL KVVRC GZOWC LTUHA YJVHK ZLXLA AZHMR DESAA QRUWW HQCAW ONBLT
CXXLR CBLIL TLSTM GDIIU YPQLN EMEWX PKEQQ ORSKB QDIAZ DASJJ WQ
```

Řešení úloh č.14 a č.15 - Dešifrace ŠD-2 / CM-1

Úloha č.14 Nastavení

Otevřený text:

BEGIN1
PODARILO SE MI ZISKAT NASTAVENI SIFRATORU NA LISTOPAD A PROSINEC
ZASILAM JE V DOMLUVENEM FORMATU TENTOKRATE SE COMMUTATION FILLING SET ROV-
NA COMMUTATION FILLING ANGLES
HODNOTA CISEL OD JEDNE DO JEDENACTI JE URCENA PREDCHOZIMI PRVNIMI JEDENACTI
PREDANYMI HESLY
POKUD JE NEMATE SCHOVANY STACI SPRAVNE ROZLUSTIT ME PREDCHOZI ZPRAVY JEDNA
AZ JEDENACT
PREVODOVA TABULKA TETO SIFRY JE JAKO OBVYKLE NASTAVENI COMMUTATORU DVOJICE
MIMO TABULKU JSOU UVEDENY V CASTI DVE
IGOR KULIKOV
END1

BEGIN2
Q=Q W=L X=R Z=Z
1 00000000000000000000000000
5 11000001000001100001001000
3 00010000000001000011010000
4 00010001010010000000000100
2 01010001000000000001000010
R 00000000000000000000000000
filling 123456
disc angles 7891011
END2

Systém:
V doprovodném textu uvedeno, že pro předání nastavení šifrátoru použil Kulikov speciální formátování.
Byla použita jednoduchá substituce pro zašifrování otevřeného textu podle této tabulky:
Otevřená abeceda: 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
Šifrová abeceda: M W C I X S E F A O Y D U N H P Q B J T V K L R G Z

V části dvě jsou nejprve uvedeny dvojice znaků z převodové tabulky, které se v doprovodném textu nevyskytly. Potom je uvedeno pořadí kol (první sloupek) a vždy k danému kolu nastavení pinů. Následuje vybrané nastavení.
Čísla 1-11 v nastavení (filling) šifrátoru jsou počáteční písmena hesel získaných řešením úkolů v soutěži (počáteční písmeno slova, kterým se prokazovalo přes webové rozhraní, že řešitel úlohu vyřešil, např. 1.úloha měla řešení CEPICKA, takže 1=C atd.)
1 2 3 4 5 6 7 8 9 10 11 = C S L Z D C S D U H O
Text v této části zašifrován opět stejnou jednoduchou záměnou.

Poslední použité drobnosti pro získání celého nastavení byly:
Tabulka jednoduché záměny je současně propojení komutátoru (Commutator Settings).
Nastaveni (filling) pro Commutation filling Angels a Commutation filling Settings jsou shodné. Obojí je však zmíněno v otevřeném textu.

Při klasickém (frekvenčním) řešení jednoduché záměny mohou mít řešitelé problém, protože je použita angličtina a čeština najednou a charakteristika nevychází.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (4)
Správná odpověď: ZISKAT
Body: 5

Šifrový text

```
BEGIN1
PHIMB ADHJX UAZAJ YMTNM JTMKX NAJAS
BMTHB VNMDA JTHPM IMPBH JANXC ZMJAD
MUOXK IHUDV KXNXU SHBUM TVTXN THYBM
TXJXC HUUVT MTAHN SADDA NEJXT BHKNM
CHUUV TMTAH NSADD ANEMN EDXJF HINHT
MCAJX DHIOX INXIH OXIXN MCTAO XVBCX
NMPBX ICFHZ AUAPB KNAUA OXIXN MCTAP
BXIMN GUAFX JDGPH YVIOX NXUMT XJCFH
KMNGJ TMCAJ PBMKN XBHZD VJTAT UXPBX
ICFHZ AZPBM KGOXI NMMZO XIXNM CTPBX
KHIHK MTMWV DYMTX THJAS BGOXO MYHHW
KGYDX NMJTM KXNAC HUUVT MTHBV IKHOA
CXUAU HTMWV DYVOJ HVVKX IXNGK CMJTA
IKXAE HBYVD AYHK
END1
BEGIN2
Q=Q W=L X=R Z=Z
1 00000000000000000000000000
5 11000001000001100001001000
3 00010000000001000011010000
4 00010001010010000000000100
2 01010001000000000001000010
R 00000000000000000000000000
SADDA NE 123456
IAJCM NEDXJ 7891011
END2
```

Úloha č.15 Šifra ŠD-2 / CM-1

Otevřený text:

```
Praha, patnáctého prosince tisíc devětset šedesát pět. Přísně tajné.
Oznamuji, že sovětský ministr obrany Rodion Jakovlevič Malinovskij podepsal
se svým československým protějškem Bohumírem Lomským Dohodu mezi vládou
SSSR a vládou ČSSR o opatřeních ke zvýšení bojové pohotovosti raketových
vojsk. K tomuto úkonu Lomského zmocnil prezident Antonín Novotný již
v listopadu. Ve smlouvě zůstaly všechny hlavní zájmové body. Schváleno bylo
vybudování tří speciálních jaderných depotů na československém území v rám-
ci akcí Javor. Výstavba objektů bude oficiálně evidována jako spojovací ka-
belové útvary. Výstavbu bude finacovat československá strana. Termín ukon-
čení byl dohodnut na konec roku tisíc devět set šedesát sedm. Potom je pře-
vezmou do své výlučné kontroly naše speciální jednotky. Pro vybudování de-
potů byly schváleny námi vybráné tři lokality: Bělá pod Bezdězem, vzdálená
přibližně deset kilometrů od Mladé Boleslavi, Míšov třicet kilometrů od
Plzně, a Bílina, ležící dvacetpět kilometrů vzdušnou čarou od Ústí nad La-
bem. Smlouva byla dle našeho návrhu uzavřena na deset let a její platnost
se automaticky prodlužuje na další období, pokud ji nevypoví jedna ze zú-
častněných stran jeden rok před uplynutím její splatnosti. Detailni infor-
mace se připravuje. Kovaljov.
```

Převod do mezinárodní abecedy

PRAHA PATNACTEHO PROSINCE TISIC DEVETSET SEDESAT PET PRISNE TAJNE OZNAMUJI ZE SOVETSKY MINISTR OBRANY RODION JAKOVLEVIC MALINOVSKIJ PODEPSAL SE SVYM CESKOSLOVENSKYM PROTEJSKEM BOHUMIREM LOMSKYM DOHODU MEZI VLADOU SSSR A VLADOU CSSR O OPATRENICH KE ZVYSENI BOJOVE POHOTOVOSTI RAKETOVYCH VOJSK K TOMUTO UKONU LOMSKEHO ZMOCNIL PREZIDENT ANTONIN NOVOTNY JIZ V LISTOPADU VE SMLOUVE ZUSTALY VSECHNY HLAVNI ZAJMOVE BODY SCHVALENO BYLO VYBUDOVANI TRI SPECIALNICH JADERNYCH DEPOTU NA CESKOSLOVENSKEM UZEMI V RAMCI AKCI JAVOR VYSTAVBA OBJEKTU BUDE OFICIALNE EVIDOVANA JAKO SPOJOVACI KABELOVE UTVARY VYSTAVBU BUDE FINACOVAT CESKOSLOVENSKA STRANA TERMIN UKONCENI BYL DOHODNUT NA KONEC ROKU TISIC DEVET SET SEDESAT SEDM POTOM JE PREVEZMOU DO SVE VYLUCNE KONTROLY NASE SPECIALNI JEDNOTKY PRO VYBUDOVANI DEPOTU BYLY SCHVALENY NAMI VYBRANE TRI LOKALITY: BELA POD BEZDEZEM VZDALENA PRIBLIZNE DESET KILOMETRU OD MLADE BOLESLAVI MISOV TRICET KILOMETRU OD PLZNE A BILINA LEZICI DVACETPET KILOMETRU VZDUSNOU CAROU OD USTI NAD LABEM SMLOUVA BYLA DLE NASEHO NAVRHU UZAVRENA NA DESET LET A JEJI PLATNOST SE AUTOMATICKY PRODLUZUJE NA DALSI OBDOBI POKUD JI NEVYPOVI JEDNA ZE ZUCASTNENYCH STRAN JEDEN ROK PRED UPLYNUTIM JEJI SPLATNOSTI DETAILNI INFORMACE SE PRIPRAVUJE KOVALJOV

Systém:

Zašifrováno pomocí šifrátoru ŠD-2

Softwarový simulátor http://soutez2009.crypto-world.info/sd2/cti.txt

Nastavení: přesné nastavení šifrátoru viz úloha č.14, nastavení simulátoru viz pohled na *správné nastavení šifrátoru*

Po vyřešení předchozí úlohy a pochopení uvedených informací již není problém v simulátoru nastavit směnné klíče a text dešifrovat.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (za ČR podepsal?)

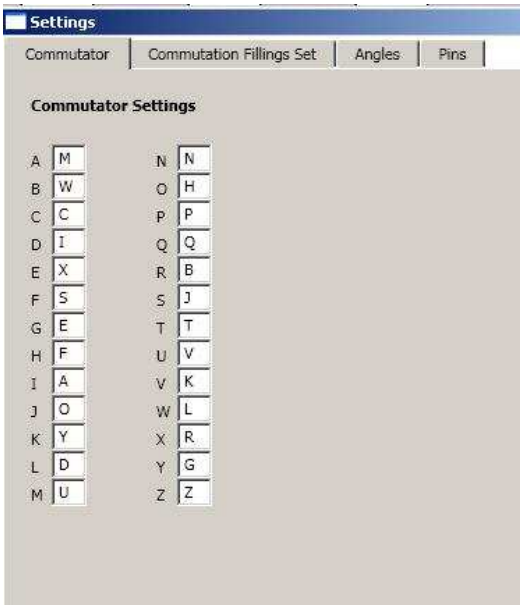
Správná odpověď: LOMSKY

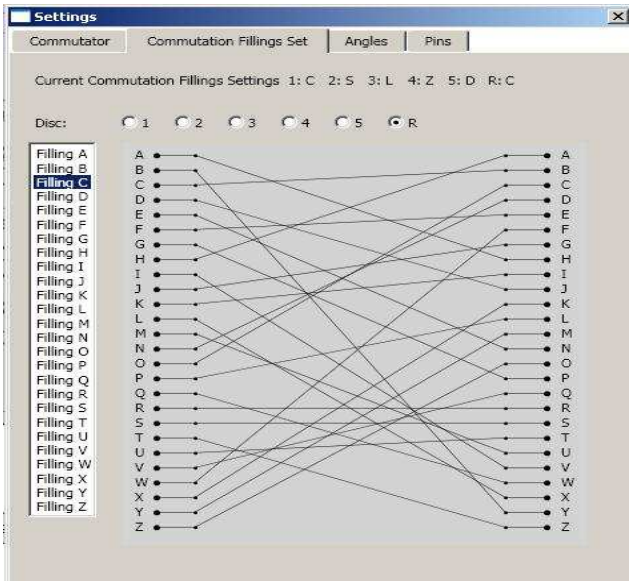
Body: 25

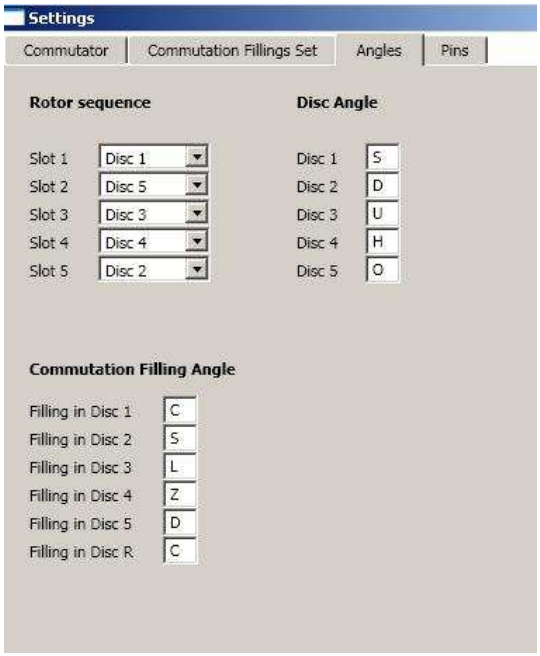
Šifrový text

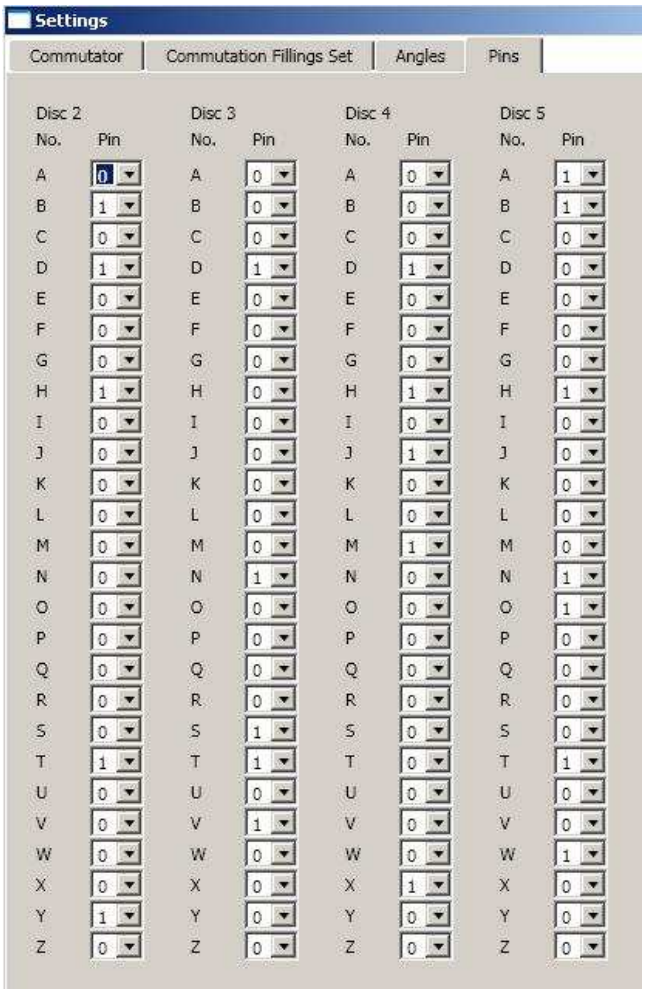
SUPPM IPFKI RBKRU PXKOJ BYAOV MUEOB XYHGD UQFQW PFBQU JTDRU IMTNA BWRQO
DUBJR XQIOQ ISBWC YCENW MDBXW BOBFY DIWCR MPPYM LIZMA YDPYV DYUYI EBCOW
KTJUF JMQDE WHUVF RANFX WBVIS FZDTQ MORHD QEROE NRIKV NEPOC MKRVB ZQAKQ
EKWID BYMIU XMWKC VYZHQ XHXNE ZBPKS TTVVK XNCEF ALXUF HDMAG XRECX UXRHJ
NCHQD GAENS CBXVP TADPY OCEOV XTXRP UEGTK TTKXL TYFCV WQBIP IGXEY SQKOD
GQZSP NZBVS OGYBK YJWAC VWNVN ALMYX ZXETI DUFJA THERE TZJTH IVGRN DAXZP
NBLKK WUSDE LOCZA RRWOH WJQLA KQXMZ YBRVP XPIVA XINXO VWPGO KRBEQ AQSAZ
FEGEH ZMJLF CDFLL MUIRP HEMRZ LZVRT RQKSA EHPLF HJYST HUZBE KXPIU PAYYU
PURKX OVOAN MMUOI VJCKW LHIRM QDHQS EROQC NRAER PNQRX GKGKG MWBTH GYUPL
BMRKF NNLVG PITVC OGCZE KUEAY HOEXV XSTPE RXZES PUJLS LJHUH WKWYJ GKVYF
TRNVC OAWXV WQBIE AXVHN KVQHE ZQYEM BXBCI RNOGB IRYDC TQPZZ QQYND MFLVF
QOZYU IVKYC RNIDZ WIDDA TLSSK ONBPK EHIBW YOMZS QSSAZ EKDVE EFMFS SUMXS
LXKRD MIAKD LJSLU YORYK DFNCG ABAOW FLKDT QEYMZ GZMJQ RBHHR HYIOQ GXKTD
JWLNM JIOZG ECTTK AHQXC DLMNB XPFEL TOKZD XQBXH GWXLQ FGHEK XMHGP SIWDD
LYGZJ SURDL PCSYT SSOGO QTNPO WGOQD AFGBD AKEPZ FHWFK QDOXQ VLRTR HFEBA
JAESJ WELPX DDHIZ HNTKH MWSBY IKFDY JKDES KGZKL NMBJH ALJSV TMBDU KDBSI
VDZEF UXFBL KVVRC GZOWC LTUHA YJVHK ZLXLA AZHMR DESAA QRUWW HQCAW ONBLT
CXXLR CBLIL TLSTM GDIIU YPQLN EMEWX PKEQQ ORSKB QDIAZ DASJJ WQ

Pohled na správné nastevní šifrátoru SD-2 , úloha č.15









U. Ohlasy a komentáře soutěžících

Diky. Super. Ta úloha s koněm mi připadla lehká, ale bažil sem se tím, jak muj kolega, který také soutěží ne a ne úlohu vyřešit...

Děkuji, příště zkusím úlohy vyřešit trochu dříve :), tentokrát jsem kolem pátku třináctého neměl úplně ideální podmínky.

U úlohy čtrnáct mne trochu zmátla poslední pasáž (od slova SADDA do konce šifrového textu). Hledal jsem v ní usilovně nějaký smysl, nakonec však k úspěšnému řešení nebyla vůbec potřeba ... :).

Moc děkuji za letošní soutěž. Bylo to příjemné zpestření podzimních dní.

Dakujem a velmi dakujem aj za sutaz ako taku. Sice 10. uloha mi dala velmi zabrat a uz som to chvilu aj chcel vzdat, ale sutaz ako taka sa mi velmi pacila a som za nu vdacny.

> Ta desátá úloha byla založena na málo známé šifře jménem MORBIT.
> Patří mezi třídu zlomkových čifer (Bifit, DalleStelle) apod.

No, to uz viem od minuleho piatku. Trvalo mi to 10 dni :-) Po 4. napovede (slovo NAPOVEDA) som definitivne prisiel na to, ze je to sifra zalozena na morzeovke. Dovtedy som si to neuvedomoval, pretoze tu morzeovku v sprievodnom texte som chapal len ako "prozu", t.j. ze v danej situacii velitel vojakom vyklepaval morzeovku... bez akehokolvek dalsieho skryteho vyznamu. V dalsej napovede (SKLO a PRST) morzeovka nebola, takze som to vypustil z hlavy a isiel som uplne zlou cestou. Bol som z toho zufaly a cele noci som nemohol spavat, pretoze aj ked som nechcel, tak stale som na tu ulohu myslel a premielalo sa mi to v hlave. Aj som chcel nechat celu sutaz tak, ale nedokazal som sa odputat od tej ulohy. Potom prisla ta NAPOVEDA a znova tam bola morzeovka, ale uz teraz bola pouzita sposobom, ktory jasne hovoril o tom, ze to ma cosi spolocne so sifrou. Skusal som vsetko mozne, ako napr. kodovanie morzeovky v trojkovej sustave a nasledny prevod do dekadickej, rozne sposoby kodovania binarne a pod.
Nakoniec som bol bezradny do tej miery, ze som sadol k pocitacu a v Googli som len tak bezcielne hladal sifry suvisiace s morzeovkou. No a natrafil som na Morbit - bol tam priklad a struktura tej sifry mi hned pripomenula 10. ulohu. Tak som to skusil a sadlo to. Ale bolo to strasnych 10 dni...

Dobry den,
v prvom rade sa chcem podakovat za krasnu a miestami aj pomerne narocnu sutaz. Nie kazdy si najde cas na organizovanie takychto aktivit. Mozem povedat, ze sa som sa pri sutazi velmi dobre bavil, a o to v konecnom dosledku ide.

Dobrý den,
děkuji za výbornou soutěž, těším se na další rok.

Mám spíš menší poznámku, která se týká poslední úlohy. Ta pro mě nebyla o luštění šifer, ale místo toho byla o boji s windows, kterým jsem strávil asi 3 hodiny! Zjištění konfigurace stroje nebyl po rozluštění 14. úlohy problém.
Jako linuxový uživatel jsem byl poněkud roztrpčen nutností použít program, který běží pouze pod windows.

Takže jsem byl nucen restartovat počítač a nabootovat windows xp.

Pro mne byly problematicke ulohy 3,6,9,10 . U 3,6 slo jen o napad, ale ten ne a ne prijit. Jakmile jsem to „uvidel“, zacal jsem si trhat vlasy z hlavy. Jo desitka byle jine kafe. Nastesti to po NAPOVEDE bylo jasne (tedy skoro jasne).

Podobne aj ta uloha s blockom. Napisanie programu mi zabralo neuveritelnych 90 minut, aj ked algoritmus som vedel okamzite. Vyslo to asi az na sty pokus, po odhaleni vsetkych chyb a preklepov v programe a zatial ma predbehlo 9 ludi :-)

Letos se mi pribeh libil mnohem vice nez v minulych letech. Hlavne se mi libilo, jak ulohy byly zasazeny do deje. Asi je tezke vse takto predem vymyslet a zkloubit. Dekuji a tesim se na pristi rok.

Jsem zase letos nejelpsi resitelka zena? Neslo by udelat lustitelske kategorie? Napr. zeny, studenti a prednasejici. Vim (tedy od Vas), ze se souteze zucastnili nejmene tri prednasejici informatiky a to je nefer! I v boxu jsou váhove kategorie …

Moc Vám děkuji za soutěž, je naprosto super. Úlohy i příběh jsou moc zajímavé. Dostal jsem se k Vašemu časopisu zajímavou náhodou…
Dělá mi problém jednoduchá záměna, asi se projevují mé malé zkušenosti. Úloha č. 4 mi dala pořádně zabrat. Stejně tak se teď nemůžu dostat přes 1. část úlohy č. 14 - viz soubor v příloze.

Bezva soutez. Mel jsem však letos velky problem rozchodut simulator. Ten lonsky byl mnohem pritulnejsi a prehlednejsi a hlavne nemel chyby. Při ulozeni nastaveni se neuolozilo, při sifrovani a desifrovani se neobjevilo, ze se kola otocila atd. Nicmene neberte to jako stiznost. Vim, ze vsichni jsme měli stejne podminky a ja to bnimam tak, ze replika nebyla dokonala.

To nemala byt z mojej strany staznost :-) Mna tie ulohy velmi bavili a na kazdu jednu som sa vopred tesil. To len bol moj pocit o ich obtiaznosti. Ale uznavam, ze pre ludi ktori sa po prvy raz zapajaju do sutaze boli tie ulohy (az na 10.) dobre volene.

Odhadl jsem, že CHUUV TMTAH NSADD ANE znamená COMMU TATIO NFILL ING a doluštění už nebyl žádný problém.

Chtel jsem si koupit vasi knizku. Jenze jsem ji opravdu zde v Decine nemohl sehnat. Koupit přes internet jsem si ji nechtel, a tak jsem si řekl ze si ji jednoduse vyhraji. Jak však vidite chybelo mi k tomu par hodin ...

Dekuji za jiz tradicne zajimavou soutez. Zda se však, ze jiz tradicne jsem na horsim a horsim miste. Tak tedy zase priste!

V. O čem jsme psali v listopadu 2000 – 2008

Crypto-World 11/2004

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

Crypto-World 11/2006

Crypto-World 11/2007

Crypto-World 11/2008

W. 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/