Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 14, číslo 1/2012 **15. leden**

1/2012

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1340 registrovaných odběratelů)

Obsah :

Soutež v luštění 2011: http://soutez2011.crypto-world.info/
Konference SOOM Hacking & Security konferenci http://www.soom.cz/

A. Informace redakce, PF 2012

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

Vážení čtenáři, e-ziny 11/2011 a 12/2011 v minulém roce nevyšly, protože hlavní protagonisté naší redakce byli zcela vytíženi jinými úkoly. I přes velkou snahu se nepodařilo tato čísla připravit.

Vynechání pravidelného vydání čísla e-zinu se stalo poprvé od září roku 1999, kdy jsem začal e-zin vydávat a rozesílat svým známým, kteří měli zájem o oblast, kterou se náš e-zin zabývá (popularizace kryptografie, elektronického podpisu, nekomerční informace o této problematice, soutěž v luštění).

Doufám, že v tomto roce nalezneme systém, který nám umožní obdobný výpadek minimalizovat. Vzhledem k vytíženosti mé a mých kolegů, kteří mi s jeho přípravou pomáhají, zvažujeme přejít na systém dvojčísel a e-zin vydávat pouze 1x za dva měsíce.

Omlouvám se za výpadek v závěru roku 2011 zejména účastníkům podzimní Soutěže 2011 v luštění. S velkým úsilím byla soutěž alespoň včas ukončena (poslední úkoly, vyhlášení vítězů). Celkový vítěz tak včas získal prvou cenu a mohl se zúčastnit Mikulášské kryptobesídky konané 1.-2.12.2011 v Praze (viz kapitoly Soutěž 2011 - Statistika soutěže, úspěšnost, řešitelé a Soutěž 2011 - Ceny a loga sponzorů).
Zveřejnění řešení jednotlivých úloh, které jsem původně plánoval do čísla 12/2011, se tak přesunulo až do tohoto čísla 1/2012. Děkuji za pochopení a za trpělivost !

Současně děkuji všem příznivcům za zaslané dotazy, kde jste zjišťovali, co se stalo a za váš zájem o pokračování e-zinu a nejrůznější nabídky pomoci. Velmi si jich vážím a je to velké povzbuzení v naší činnosti a podnět k zamyšlení, jak dále….

Závěrem mi dovolte, abych všem našim čtenářům popřál do roku 2012 pevné zdraví, klid na zajímavou práci, štěstí a úspěch v profesním životě.

Za redakci e-zinu Crypto-World a za kryptologickou sekci Jednoty českých matematiků a fyziků

Pavel Vondruška

B. Soutěž 2011 – Kompletní příběh včetně úloh, nápověd a jejich správného řešení

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

Úvodní příběh
Crypto-Wars

Vždy, když Dr. Peter Hayek nastoupil do časoprostorového výtahu a vložil do otvoru svoji kartu s nahranou stáží, se cítil velmi vzrušeně. I po dvaceti letech služby si stále nemohl zvyknout na to, že je vyslán do minulosti, aby zachránil svět. Přesněji, aby zachránil stabilitu světa a nedošlo ke změně, která by měla za následek zničení Ultima Paradise. Tedy světa, který byl vybudován jako stabilní svět v roce 9011 po narození Krista.

Pamatuje si stále velmi živě na svoji prvou cestu před dvaceti jedna lety, kdy nastoupil do výtahu ve společnosti toho „potrhlého matematika“, který jej vyhledal a nabídl mu velmi zajímavou práci, kde prý bude moci využít své schopnosti luštit klasické šifry. Matematik za ním přišel dva dny po té, co vyhrál prestižní světovou soutěž v luštění, aby mu nabídl zajímavou práci. Povečeřeli spolu a pak se od něj dozvěděl velké tajemství o cestování časem a o společenských fluktuacích v časoprostoru. Nejdříve přisuzoval jeho vyprávění jisté potrhlosti v jeho chování, které se projevovalo ve velké roztržitosti a neustálé roztěkanosti a velmi, velmi podivnému chování, kdy neustále sledoval okolí a před každou jednoduchou aktivitou přemýšlel, jakoby to pro něj bylo něco nového. Dále pak jeho vyprávění připisoval chutnému těžkému portskému vínu. V závěru večera, pravděpodobně pod vlivem toho, že v posledních měsících, kdy se mu vůbec nedařilo a stíhala jej jedna osudová rána za druhou (po smrti rodičů jej opustila jeho dívka) se rozhodl, že s ním zajde do hotelu, kde mu slíbil matematik předat přihlášku do nové práce.

V hotelu Alcron prošli společně kolem recepce, vstoupili do běžného výtahu a když se dveře zavřely, vytáhl jeho podivný průvodce nějaký balíček, který připevnil na stěnu výtahu a pak vyndal ze své náprsní kapsy kartu a přiložil ji k balíčku. Proboha snad to není bomba! Jenže výbuch nenastal, ale stalo se něco jiného. Vnitřek výtahu se jako mávnutím kouzelného proutku změnil a najednou se octli v prostoru, který výtah připomínal, ale byl jiný než ten, do kterého vstoupili. Změnil se materiál, vše bylo z nějakého zvláštního plastu. Původní panel s tlačítky zmizel a místo něj se objevil displej velikosti asi 10x10 cm, ve kterém bylo číslo 2011 a pod ním další dlouhá řada čísel. Jeho průvodce se k němu obrátil a řekl: „Milý Petře, vím, že budeš s novou prací souhlasit, a proto tě odvezu přímo do naší centrály, která leží daleko v budoucnosti a je uzavřena ve speciálním časoprostorovém vaku.“ Pak vyndal z kapsy jinou čipovou kartu a přiložil ji k displeji. Na displeji se začala rychle měnit čísla 2011 / 2012 / 2013/ ..... Čísla v druhém řádku se měnila tak rychle, že prakticky tvořila jen světelnou čárku. Po několika málo minutách se „výtah“ zastavil a najednou se objevily dveře. Oba z výtahu vystoupili a ocitli se v místnosti se skleněnou kopulí a se spoustou zelených velkých rostlin. Vnímal, že se kolem pohybují lidé, kteří jsou oblečeni do šatů ze zvláštní přiléhavé, lesklé látky. Zmateně se kolem sebe rozhlížel a hledal vysvětlení toho, co se to vlastně stalo? Přece nebude věřit těm povídačkám svého podnapilého průvodce, že se ocitli v daleké budoucnosti!

Ale bylo to tak. Petr se dostal do výcvikového střediska SGW (ochránců světa). Trvalo to asi 3 měsíce, než se částečně vyrovnal s tím, co se stalo a než pochopil a vstřebal základní

informace. Petr měl možnost se ptát a ptát a na své dotazy dostával odpovědi. Byl ve výcviku a bylo potřeba, aby byl připraven. Základní důraz výcviku byl kladen právě na to, aby nový adept na strážce pochopil, kdo je, co je jeho úkolem, proč vzniklo toto výcvikové středisko, proč instituce Strážců světa vznikla, proč byl vybrán, co bude dělat, proč to nejde dělat jinak, paradoxy času a prostoru.

Petr si postupně sestavoval mozaiku informací, která mu měla pomoci vše pochopit. Zpočátku si při své pečlivosti a také ze strachu, zda nešílí nebo již nezešílel, řadu věcí psal, aby se k nim mohl vracet a hledal v tom, zda to má nějaký smysl.

Ze všech poznámek se mu postupně vyklubal tento nový pohled na svět:
Cestování časem a časoprostorem je možné. Vše se děje najednou. Tak jako chodíme dveřmi z místnosti do místnosti, tak můžeme vstupovat z jednoho bodu v čase a prostoru do jiného. Omezení je dáno pouze energií. Zatímco cestování časem ve stejném bodě prostoru je energeticky zvládnutelné, tak cestování v prostoru ve stejném čase je energeticky náročné. Lidé se mění, ale povahově jsou to pořád zvířata. Pro své ego, moc a majetek jsou ochotni udělat cokoliv a to i tehdy, když tím poruší obecný princip morálky. Jak běžela staletí a tisíciletí (pardon jak běží vedle sebe), tak se stalo, že v jednom bodě časoprostoru přišli na způsob, jak ovládnout pohyb v čase. To však mělo za následek, že se našla skupina lidí, která se rozhodla toto využít ve svůj přímý či nepřímý prospěch a lidé ze skupiny začali cestovat v čase za účelem změny minulosti. To, co nastalo, byl tak hrozný zmatek, že vyústil v neustálé změny dějin, které měly za následek změnu budoucnosti a to zcela nepředvídanou, vedlo to však k tomu, že kolem roku 9000 se skupina lidí rozhodla, že taková anarchie není možná a hlavně může vést k definitivnímu zničení lidstva bez možnosti nápravy. Nepochopil sice řadu souvislostí, kauzalit a determinismů v dalším vysvětlení, ale oficiální historie byla adeptům vyložena takto:

- v roce 9011 vznikla rovnováha lidstva – tzv. Ultima Paradise
- aby úmyslné nebo neúmyslné změny minulosti neměly negativní vliv na vytvoření tohoto zářného cíle a stavu lidstva, je s okamžitou platností zakázáno cestovat do minulosti (až na výjimky uvedené dále)
- vědci sestavili dějiny lidstva a tyto dějiny se nesmí změnit, neboť by to mohlo mít za následek to, že Ultima Paradise nevznikne
- to, že je možné cestovat časem, plyne z obecné teorie relativity propojené s kvantovou teorií, teorií neurčitosti a teorií tachyonů (částice rychlejší než světlo)
- malá změna v historii může, ale nemusí mít za následek změnu různé intenzity s různým dopadem v jiném čase
- dějiny jsou to, co lidé z jiného času vědí o čase předchozím
- mimo prostor Země ve velmi těžko energeticky vzdálené části vesmíru vznikla časová kapka, která má speciální energetický tunel do Ultima Paradise, v časové kapce je výcvikové středisko Strážců času, analyticko-historické oddělení a zásahová jednotka vycvičených strážců času
- důvodem je, že při změně dějin se sice může stát, že se významně změní známé dějiny a dokonce i zmizí Ultima Paradise, ale časová kapka touto změnou není dotčena a analyticko-historické oddělení navrhne takové změny, úpravy, které vedou k tomu, že se objeví opět Ultima Paradise a dalšími změnami dokončí to, že se dějiny dostanou do souladu s popsaným a známým stavem
- dějiny se někdy mění zcela nečekaně a bez zásahu zvenčí a to na základě vnitřních energetických fluktuací, které plynou z teorie neurčitosti, z hlediska pozorovatele v daném časoprostoru se nějaká událost prostě stane, ale podle dějin se stát neměla (nebo opačně)

- jako příklad bylo Petrovi uvedeno toto: „Podívejte se, třeba ve vaší specializaci. Nějaký luštitel má před sebou zašifrovanou zprávu. Pokud ji vyluští, má to za následek např. vítězství v bitvě a tím třeba v celé válce. Jenže právě díky časové fluktuaci se může stát, že se mu zprávu nepodaří vyluštit. To může mít za následek, že se změní významným způsobem následné dějiny. Třeba díky tomu ale zmizí i Ultima Paradise. V tom okamžiku zasáhne naše jednotka strážců času."
- Petr se naivně zeptal, jak to jednotka udělá? Vtrhne tam s novodobou technikou a pomůže bitvu vyhrát nebo tak nějak? Přednášející jen zdvihl obočí. Jistěže ne. To by mělo za následek, že zmínky o pomoci by se objevily v dalších dějinách. Protože ale o nich nevíme, znamená to, že nastat v tomto rozsahu nesmí. Nesmíme změnit známé dějiny. Můžeme však dotyčnému v tomto případě pomoci zprávu vyluštit. Pokud to uděláme vhodným způsobem, který nebude dále v dějinách zachycen, tak se nám naše dílo podařilo a důsledkem bude, že se vše v čase vrátí do původního stavu a tedy včetně vzniku Ultima Paradise.
- Aha, rozumím. Jsem tedy zde pro případ, že bude potřeba vyluštit nějakou klasickou šifru a napovědět luštitelům v daném čase a prostoru nebo ji místo nic vyluštit a předat. To chápu, ale proč já? To nemáte někoho z dalších století a tisíciletích lepšího? Velitel výcviku se usmál a řekl: „Petře, nepodceňujte se! Již sto let po datu Vašeho narození se používaly pouze binární šifry a dvěstě let po Vašem narození kvantové šifry. Prostě zkušenosti s luštěním klasických šifer již vaši následovníci nemají. Navíc znáte dějiny od roku cca 0 n.letopočtu do roku 2011 a tedy právě dějiny období, kdy se tyto šifry používaly. Máte představu, jak lidé v dané době žili, jak se oblékali, víte co jedli a máte základní jazykovou vybavenost.. Prostě pro toto období a pro tuto činnost jste vhodným strážcem. Čili při výběru kandidátů pro nějakou činnost dáváme vždy přednost pro kandidáty z vrcholu daného období. Máme zde všechny možné specializace, které se hodí pro speciální úkoly, které naše jednotky strážců času plní.
- Znovu opakuji, v dějinách je mnoho a mnoho událostí, které nejsou nikde zaznamenány a tedy se o nich neví a jejich dopad tedy může, ale nemusí mít vliv na dějiny. Zde tedy máme velké možnosti a můžeme nasadit prakticky libovolnou techniku a prostředky; když se o tom neobjeví záznam a naše dějiny se nezmění, pak se zásah povedl.
- Analyticko-historické oddělení provedlo vždy před zásahem podrobný rozbor a navrhlo vhodný způsob nápravy. Zásah po provedení pečlivě vyhodnotilo a pokud se o něm neobjevil někde v budoucnosti záznam, byl úspěšný.
- Mezi strážci se vyprávěly neuvěřitelné příběhy. Jeden ze strážců neustále například dokola popisoval svůj nejzajímavější úkol. Skutečná matka Leonarda da Vinciho – Caterina - byla otrokyně pocházející z Východu. Otci Leonarda ji věnoval jeden florentský šlechtic. S ní měl mít Piero da Vinci syna Leonarda. Jenže v té době Piero - Leonardův otec - žil v manželství s jinou ženou. Ta velmi hlídala jeho večerní návštěvy u Cateriny. Prakticky k ní přicházel na lože velmi málo. To mělo za následek jednu z fluktuací v čase. Caterina neotěhotněla a právoplatná manželka Piera da Vinci u manžela prosadila, že Caterinu prodal svému příteli. Tím se ovšem stalo, že se Leonardo da Vinci nenarodil. To však byla tak významná historická událost, že to změnilo celé dějiny světa. Nezbylo než zasáhnout. Řešení bylo více, ale nakonec se našlo to nejjednodušší. Jeden ze strážců dostal za úkol navštívit rodinu da Vinci jako mladý kupec a zde přespat. Podařilo se mu navázat kontakt s Caterinou a dokonce ji v noci navštívit. Strážce tu noc s ní zplodil syna. Ta se samozřejmě nikdy nepřiznala. Piero da Vinci si myslel, že je otec chlapce on a měl z otěhotnění Cateriny radost. Nátlakům své právoplatné manželky odolal a Caterinu u sebe ponechal a o chlapce, který se narodil, se řádně postaral a do smrti věřil, že je to jeho syn. V tomto platném čase se na svět dostal geniální Leonardo da Vinci díky zásahu

z daleké budoucnosti.. Strážce se při vyprávění tohoto příběhu rozhlédl a řekl: „Jak by nebyl Leonardo geniální, vždyť byl po mně!“

Po úvodním kurzu absolvoval Petr jednoroční kurz sebeovládání, psychologie, historie a jazykovědy. To jej poměrně bavilo a bez velkých problémů kurz absolvoval.
Následoval 6-ti měsíční kurz, ve kterém se seznámil s různými technologiemi, kterými strážci disponují a mohou je na základě rozhodnutí analyticko-historického oddělení použít.
Pak absolvoval 5 jednodenních návštěv v různých časových obdobích. Naučil se tak prakticky ovládat technologii cestování časem a získal potřebný stupeň profesního sebevědomí a umění se pohybovat mezi lidmi jiného věku.

Celá jeho příprava byla uzavřena jednoměsíční dovolenou na začátku třetihor. Koupal se v teplém šelfovém moři, chodil na vycházky a obdivoval panenskou třetihorní přírodu, lovil, rybařil.

Po návratu z dovolené byl pozván na vedení analyticko-historického oddělení a zde mu byl předán diplom o absolvování a odznak strážce – zlatou hvězdu se zeleným smaragdem a s vyrytým jménem a jednoznačným identifikačním kódem, který byl vytvořen jako otisk jeho DNA. Peterovi byla přečtena rozsáhlá přísaha a on vyslovil nahlas: „Tak přísahám“.
Tak se stal Dr. Peter Hayek jedním ze strážců času se speciální profesí luštitel klasických šifer.

Peter trávil svůj volný čas v knihovně a hltal zde dějiny lidstva. Dějiny, které pro něj byly budoucností, jej nesmírně zajímaly. Divil se, že lidstvo dělalo stále stejné chyby, ale současně obdivoval, že vždy v těch těžkých chvílích se našel nějaký vůdce – vizionář a řada poctivých lidí, kteří tyto vize dokázali realizovat.

A pak nastal ten den, na který byl připravován a na který čekal. Byl nasazen do své prvé akce. Na historicko-analytickém odboru mu podrobně vysvětlili, co se stalo a jak se očekává, že by náprava mohla proběhnout. Byl seznámen s tím, co vše se o daném časovém okamžiku a osobách ví a tedy co by během řešení svého úkolu neměl porušit. Pak Dr. Peter Hayek dostal naprogramovanou kartu s nahranou stáží, popřáli mu mnoho štěstí a pak nastoupil do časoprostorového výtahu na svoji prvou akci.

Úloha č.1
Vstupní test

Šifrový text
Kdo netresta zlo, prikazuje, aby se dalo.

Systém: Uhodnout autora citátu.

Upřesnění: Citát pochází od Leonarda da Vinci, nápovědou je to, že je v úvodním textu vzpomenut. Citát lze snadno vyhledat.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: neuvdena

Správná odpověď: LEONARDO
Body: 2

Otevřený text:
Kdo netrestá zlo, přikazuje, aby se dálo.

Zveřejněná nápověda k úloze č.1 - Vstupní test
Nápověda k zadání správného řešení (Autor).

Dodatečně zveřejněná nápověda k úloze č.1 - Vstupní test

úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení sys-tému
1	********	2	neuvedeno	vstupní test	"IQ" (citát)

Pokračování v příběhu
Mise 1 - Shiloh

Dr. Peter Hayek dostal naprogramovanou kartu s nahranou stáží, popřáli mu mnoho štěstí a pak nastoupil do časoprostorového výtahu na svoji prvou akci…

Ve výtahu si opakoval, co se na analyticko-historickém oddělení dozvěděl. Došlo k významné změně v dějinách. Jižanům se podařilo zvítězit v krvavé bitvě u Shilohu. Potom, povzbuzeni vítězstvím, napadli přibližující se jednotky generála Granta a opět dosáhli vítězství. To významným způsobem změnilo válku Severu proti Jihu a trvalo o dva roky déle než Seveřané konečně zvítězili. Dopad na dějiny byl však zcela zásadní a bylo potřeba zasáhnout a zajistit v bitvě u Shilohu vítězství Seveřanů.

Důvodem, proč k fluktuaci ve vývoji dějin došlo, bylo podle analytiků to, že Konfederace jižních států uplatňovala zásadu širokých práv jednotlivých států i v oblasti kryptografie a připustila, aby každý velitel ozbrojených sil si sám vybral svůj šifrový systém. Před bitvou u Shilohu dne 6.dubna 1862 se jižanský generál Albert S.Johnston dohodl se svým zástupcem Pierrem Beaurgardem na používání XXXX šifry pro vojenské účely.

5.dubna generál S.Johnston zaslal zašifrovanou zprávu tímto systém s pokyny k útoku. Zpráva pak byla předána velícím důstojníkům na celé frontě u Shilohu. Jeden z opisů byl zachycen unionisty a doručen do štábu k dešifraci. Zde jej dostal k rozluštění jakýsi nižší důstojník namyšlený mládenec John Wallace. V dějinách zaznamenaných před fluktuací se stalo to, že severský důstojník Wallace při luštění uspěl. Zprávu v noci předal svému veliteli a ten na jejím základě poslal žádost o pomoc generálu Grantovi, který se svým vojskem byl necelý den přesunu od Shilohu. Grant výzvu uposlechl a vydal se neprodleně na cestu a dorazil na bojiště právě včas. Díky tomu se v encyklopedii oficiálních dějin objevilo toto:

6. dubna se znovu střetla vojska Severu a Jihu v bitvě u Shilohu. Jižanské Johnstonovi jednotky překvapily předsunuté Seveřany ve stanech nedaleko tohoto města. Albert S. Johnston měl početní převahu a tak se celkem hladce dařilo tlačit severské jednotky před sebou. Na pomoc však přišel nečekaně unionistický generál Grant s posilami. Jižanský velitel Johnston byl v další části bitvy raněn tříštivým nábojem a vykrvácel. Jeho nástupce Beauregard se proto stáhl. Unionisté pak již celkem snadno obsadili Corinth.

„Všichni jsme věděli, že vítězství je naše," řekl po bitvě Seveřan Wallace, který se o ni zasloužil nejen svojí odvahou na bojišti, ale především tím, že včas vyluštil obsah zachycené depeše. Bitva u Shilohu se stala nejkrvavější bitvou jakou Spojené státy do té doby zažily.

Úkol Petra byl jednoduchý, měl zjistit, co se stalo s depeší a proč ji Wallace včas nerozluštil a případně mu s vyluštěním pomoci. To musel navíc udělat tak, aby se o něm neobjevila v dějinách žádná zmínka. Psycholog analytického oddělení mu poradil. Wallace byl namyšlený chlapík. Stačí mu nějak poradit jak při luštění uspět nebo dokonce předat část vyluštěného textu nebo popis systému a on si určitě nechá pro sebe, že to vyluštil díky této pomoci. Nikomu se o tom nikdy nezmíní. Celý živost se bude chlubit tím, jak to byl ON, kdo rychle vyřešil zprávu a zachránil tak severské jednotky u Shilohu před porážkou.

A tak se také stalo. Peter vstoupil do stanu seržanta Wallace. Ten zde však nebyl, protože si odskočil na panáka Whisky, aby se mu lépe luštilo. Dokonce nechal na stole zachycenou zprávu, svůj blok a knihu o šifrách. Petr si zprávu prohlédl a užasl nad naivitou použitého systému. Neudělal proto nic jiného než, že nalistoval v knize o šifrách ten správný systém a list se šifrovou zprávou k němu přiložil a pak ze stanu odešel a čekal, zda tato nápověda pomůže.

DWWDFNVWDUWWRPRUURZPRUQLQJDWHLJKWDPRQWKHZKROHIURQWDOE
HUWVMRKQVWRQ

Wallace si naštěstí pro Unii opravdu dal jen jednu sklenku a když přišel do stanu, tak se sice nejprve divil, kdo že to manipuloval s jeho pomůckami ležícími na stole, ale pak se pozorně zadíval na šifru a šifrový systém v knížce. Zkusil jej použít k dešifraci a ejhle bylo tomu tak. Wallace rychle zprávu dešifroval a běžel ji předat velícímu důstojníkovi. Ten pak poslal žádost o pomoc generálu Grantovi a zbytek již znáte z dějin…

6. dubna se znovu střetla vojska Severu a Jihu v bitvě u Shilohu. Jižanské Johnstonovi jednotky překvapily předsunuté Seveřany ve stanech nedaleko tohoto města. Albert S. Johnston měl početní převahu a tak se celkem hladce dařilo tlačit severské jednotky před sebou. Na pomoc však přišel nečekaně brzy unionistický generál Grant s posilami a útok zastavil.

Petr se vrátil ze své prvé úspěšné mise. Jeho zásah byl sice jednoduchý, ale účinný a přesně takový, jak bylo potřeba. Oficiální dějiny se obnovili a neobjevila se nikde žádná nová linie, která by byla vyvolána jeho zásahem.

Úloha č.2
Mise 1 (Sever proti Jihu, Shiloh)

Šifrový text
DWWDFNVWDUWWRPRUURZPRUQLQJDWHLJKWDPRQWKHZKROHIURQWDOE
HUWVMRKQVWRQ

Systém: Caesarova šifra
Upřesnění: klasický systém, text v angličtině bez dělby na slova

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (3)
Správná odpověď': ZITRA
Body: 2

Otevřený text :
Attack start tomorrow morning at eight am on the whole front. Albert S. Johnston

Otevřený text přepis do češtiny :
Útok zahájit zítra ráno v 8.00 hodin na celé frontě. Albert S.Johnston

Přepis do mezinárodní abecedy
ATTACKSTARTTOMORROWMORNINGATEIGHTAMONTHEWHOLEFRONTALBERTSJOHNSTON

Nápověda k úloze č.2 - Mise 1 (Sever proti Jihu, Shiloh)
Nápověda k zadání správného řešení(3).

Dodatečně zveřejněná nápověda:
Tento šifrový systém patří mezi nejjednodušší. Je jistě zajímavé, že před bitvou u Shilohu skutečně došlo mezi zde uvedenými veliteli k jeho používání.. EN/CZ.

úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení sys-tému
2	*****	2	(3)	Mise 1 (Sever proti Jihu, Shiloh)	jednoduchá záměna

Pokračování v příběhu
Mise 2 – Petr Vok

Dr. Peter Hayek opět dostal naprogramovanou kartu s nahranou stáží. Popřáli mu mnoho štěstí a on nastoupil do časoprostorového výtahu na svoji další cestu do minulosti.

Tentokrát byla mise velmi zvláštní. Český šlechtic nechal hrdlem ztrestat svého sluhu za to, že uvařil jakýsi lektvar, který pak dal jedné z jeho konkubín. Té tváře nejprve zčervenaly, ale pak se včetně očí zanítily a měla velké bolesti a stala se ohyzdnou. U sluhy byl nalezen papír s čarovným zaříkadlem. Sluha se sice bránil, že je to návod na elixír krásy, který sám slovutný český alchymista Tadeáš sepsal a to na základě návodu významného italského vědce. Nic mu to platné nebylo. Petr Vok se na papír podíval a když viděl, že neobsahuje žádný návod, ale slova nedávající smysl a tedy určitě zaklínadlo, jak ostatně všichni kolem tvrdili, nechal sluhu ihned popravit. Jenže tím nastal problém. Petr Vok na to neměl právo a byl pozván, aby svůj čin obhajoval před císařem na zemském sněmu.

Dějiny však měly jít jinou cestou. Bez fluktuace děj vypadal takto. Sluha návod, který byl zašifrován, dešifroval a správně přečetl a neudělal při přípravě lektvaru chybu. Děva zvaná Matylda z Hradce však byla alergická na látku, která byla v masti obsažena, a tak po masti onemocněla. Sám Petr Vok sluhu vyslýchal, aby zjistil příčinu té nemoci. Sluha však měl právo se před Petrem hájit, ukázal mu, jak lze z „kouzelného zaříkadla“ získat návod na mast pro krásu. Tedy ukázal a vysvětlil, jak je text jednoduše zašifrován. Petr rychle pochopil, sluhu jen pokáral, aby příště dával pozor a raději mast nejprve ozkoušel na selských dívkách. Děva Matylda se rychle vyléčila a možná díky masti byla dokonce ještě krásnější. Brzy na to

otěhotněla. Není zcela jasné, kdo byl otcem. Při křtu držel chlapce sluha, ale zlé jazyky říkaly, že otcem byl Petr Vok. Ostatně, proč jinak by mu na srdci tak moc leželo zdraví toho děvčete?

Úkol byl jasný. Ohlídat, aby Petr z Rožmberka pochopil, že tajemný text není kouzelné zlé zaříkadlo, ale aby pochopil, že jde o zašifrovaný text a skutečný návod lektvaru krásy od významného českého vědce, dokonce osobního lékaře císařů Maxmiliána II. a Rudolfa II.

I tentokrát se podařilo Peterovi vnuknout správným způsobem myšlenku, **jak návod snadno dešifrovat** a dějiny se vrátily do svých správných kolejí…

Úloha č.3
Mise 2 (Petr Vok)

Šifrový text

```
WCACL VTHAX MLIAZ AIAEZ LFDXC TETMJ
RCXJI AMTCJ HTPLW TDHUM LEWCA CLVTH
AHTGC TPXFT RARZL KXGAG XDGLJ IAHAF
CLVCT VMTZL JHUFZ AMLJH UHXDJ FUGTV
DLCTH AWLFT ELKTX GLDGT CTVFZ LKTXC
LHXHT PGKXC FKXGT YLNXH XETNE LFDZT
HHTDL ZPUHX ZTNHX GLDLV AYLMZ TDXXV
KFTID LWCAD CUNTE TNELZ XVHTM XCATX
KUWXZ VGLYL KLEJG LJKLE LJMTN FLPTG
KXCXP JETFW TDHXH TGCTP XGTMX ZLKXG
AAGTM GUGLD LZXID UMXZT GXDTG KXCWT
DHLJI AHAKT VMAMA VDUMT ZLJHL KTGTV
AVFTM THWCA IAHDG LMJML JDUFD CDXKA
IHTYL YCXIY JJFJF HXFZJ HIAXH XETZT
NDLZX IDJKD EUVWX DIYIT FNAIY JVAKX
GAKTV MAKLE UVDLC THTGT PUZAH UDGTC
XVFZL KTZAI AEZLC LVWJF GKHAN TETHX
HTPEK XDLZX IDUXG LJKLE LJFLP TGKXC
JMUKT NMXFA GLFGM TZLJH LKXWC AZLVT
HAMLG LDLIA LENAM XHXIT ZLWCA ZLVTH
XGLDD LIAMN ELJIA LEKCX ITNTD LCTHM
TZLJH LKUKM TELKA HTWAG UVGAV AIGKC
GITEX KTHAK VPJVJ NTMTZ LJHUW ZLEAK
GTZTV ZTKZY DLFGA XDELV NAIYM HLYLN
AHTVX NAZAN AHUME LPCUM WLDCM TMEXK
THAWC AKLEA
```

Systém: Jednoduchá substituce

Upřesnění (převodová tabulka):

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

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

Otevřený text:
PŘIROZENÍ A MOCI
Líčidlo škaredému fraucimeru (nebo pěkným od přirození netřeba se fiflovati) takto učiníš: Rozřež melouny s limouny na kusy, též koření posedové a to, kteréž slove aron aneb tvář svatého Jana, dej do sklenné kolby, nalej na to kozího mléka, až všecko přikryje, dej do lázně Marie a vypal z toho vodu. Tou vodou mej sobě tvář a budeš pěkná, netřeba tě malovati. Item tyto koláčky malé také tvář pěknou činí: Vezmi mízky melounové, též i z semen, přičiň k tomu mouky škrkavičného hráchu, usuš na slunci a nadělej koláčkův. Když pak chceš jich užívati, vezmi vody z kořene té byliny, kteráž slove ličidlo, rozpust v ní jeden aneb dva koláčky a tou vodou sobě tvář umývej. Masitost melounová přiložením otok očí odjímá. Na čelo přiložená tok k očím jdoucí odvraceje. Kořen melounový v medovině pitý ztiží čtvrtce dávení vzbuzuje. Melouny plodí v těle zlé vlhkosti, a kdož jich mnoho jí, nezají-li jiným dobrým pokrmem, dávení přivodí.

Přepis do mezinárodní abecedy
PRIROZENI A MOCI LICIDLO SKAREDEMU FRAUCIMERU (NEBO PEKNYM OD PRIROZENI NETREBA SE FIFLOVATI) TAKTO UCINIS: ROZREZ MELOUNY S LIMOUNY NA KUSY TEZ KORENI POSEDOVE A TO KTEREZ SLOVE ARON ANEB TVAR SVATEHO JANA DEJ DO SKLENNE KOLBY NALEJ NA TO KOZIHO MLEKA AZ VSECKO PRI-KRYJE DEJ DO LAZNE MARIE A VYPAL Z TOHO VODU TOU VODOU MEJ SOBE TVAR A BUDES PEKNA NETREBA TE MALOVATI ITEM TYTO KOLACKY MALE TAKE TVAR PEKNOU CINI: VEZMI MIZKY MELOU-NOVE TEZ I Z SEMEN PRICIN K TOMU MOUKY SKRKAVICNEHO HRACHU USUS NA SLUNCI A NADE-LEJ KOLACKUV KDYZ PAK CHCES JICH UZIVATI VEZMI VODY Z KORENE TE BYLINY KTERAZ SLOVE LICIDLO ROZPUST V NI JEDEN ANEB DVA KOLACKY A TOU VODOU SOBE TVAR UMYVEJ MASITOST MELOUNOVA PRILOZENIM OTOK OCI ODJIMA NA CELO PRILOZENA TOK K OCIM JDOUCI ODVRACE-JE KOREN MELOUNOVY V MEDOVINE PITY ZTIZI CTVRTCE DAVENI VZBUZUJE MELOUNY PLODI V TELE ZLE VLHKOSTI A KDOZ JICH MNOHO JI NEZAJI-LI JINYM DOBRYM POKRMEM DAVENI PRIVODI

Nápověda k úloze č.3 - Mise 2 (Petr Vok)
Nápověda k zadání správného řešení (KOMU).

Dodatečná nápověda k úloze č.3:
Opět základní šifrový systém. Problém (zvláště při automatickém luštění) může být pouze s použitým jazykem - staročeštinou. Možná může pomoci to, že se jedná o originální text z Herbáře Pietra Andrea Matthioliho v překladu Tadeáše Hájka z Hájku (což je v doprovodném příběhu naznačeno).

úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení sys-tému
3	**********	3	(KOMU)	Mise 2 (Petr Vok)	jednoduchá záměna

Pokračování v příběhu
Mise 3 – Emanuel Voska

Dr. Peter Hayek opět dostal naprogramovanou kartu s nahranou stáží. Popřáli mu mnoho štěstí a on nastoupil do časoprostorového výtahu na svoji další cestu do minulosti.

Zpráva z historicko-analytického oddělení:

První světová válka dala vzniknout typu českého špionážního hrdiny – neohroženého vlastence, jehož typickým představitelem se stal Čecho-američan Emanuel Voska (1875–1960).

Ve studiích zachycujících dobu první světové války či dějiny zpravodajských služeb je pokládán za dvorního špiona T. G. Masaryka, představitele jeho rozsáhlé zpravodajské agentury, špionážní eso, zakladatele československé špionáže či rozeného špióna se zálibou v tajných operacích, ale i naivu, fantastu či ne zcela důvěryhodného muže. Voska mimo jiné organizoval kurýrní službu. Poslové, které Voska využíval, byli za války financováni především ze sbírek krajanů a nějaké cestovní náklady hradila i britská tajná služba. Podle Vosky pracovali Češi zpočátku bezplatně a až od roku 1916 byli financováni Brity. Je však pravděpodobné, že pravidelnou finanční podporu Voska pro svoji síť dostával již v roce 1915.

Těžko hodnotit Voskův přístup – na jednu stranu neustále tvrdil, že žádné peníze nechce, aby byli Spojenci zavázáni, na straně druhé připomínal v komunikaci s nimi své finanční těžkosti s nadějí, že mu bude pomoženo. Samozřejmě že sám nebyl tak bohatý, aby vše mohl financovat. Masaryk urgoval, kde mohl, ale vyřízení o permanentní hrazení všech nákladů se táhlo až do pozdního jara 1916.

Hlášení z rakousko-uherského konzulátu nabízejí i jiné vysvětlení – podle nich byl Voska hochštapler. Nejenže bral peníze z vlastního podniku, ale používal i peníze z krajanských sbírek a začal se bát, že bude obviněn ze zpronevěry.

Tentokrát byl Peterův úkol tento:

Fluktuace v dějinách vypadala následovně. Hlášení z rakousko-uherského konzulátu vedlo k policejnímu vyšetřování a následnému zatčení a odsouzení Emanuela Vosky. Nejprve za podvody a zcizení většího množství peněz, ale pak se během vyšetřování zjistila jeho špionážní činnost, a tak byl na začátku roku 1917 popraven.

Celý problém podle analytiků vznikl tím, že původní zpráva byla vlivem fluktuace změněna a zatímco v oficiální historii nevedla k zatčení, byla po fluktuační změně důvodem k zatčení E.Vosky. Ví se, že původní zpráva byla zašifrována, ale nedochovala se. Kdyby se dochovala, pak by ji pravděpodobně stačilo vyměnit za původní, ale takto to není možné a je nutné ji vyměnit za jinou, podobnou, ale také zašifrovanou. Příjemce ji musí být schopen dešifrovat, a proto měl Peter za úkol zašifrovanou zprávu z rakousko-uherského konzulátu rozluštit, pochopit jaký konkrétní systém a klíč byl použit a pak s ním zašifrovat zprávu, kterou mu analytické oddělení připravilo. Ta již E.Vosku přímo neobviňovala. Pokud ji policejní ředitelství dešifruje, pak na základě získaného obsahu této zprávy Emanuela Vosku již neobviní a tím bude fluktuace překonána a dějiny se vydají svojí správnou cestou.

Vše tedy závisí pouze na tom, aby Peter původní zprávu dešifroval a našel klíč, který bude použit k zašifrování připravené zprávy.
I tentokráte Dr. Peter Hayek poměrně rychle uspěl při vyluštění zprávy, větší problém měl s nalezením použitého klíče. Pak již podvržený text lehce zašifroval a vyměnil. Tato mise tím byla úspěšně splněna a ukončena.

Úloha č.4
Mise 3 –Emanuel Voska

Šifrový text

```
NMJCE TDLCK UPTIC STJCW FQTPK FLLMV
CVFZT LYNFL TLFZF HJFIT NPTIE BMZCH
MPTQN MLITL ETFVY ZVYHN PMQTS PTLCN
MITZP TJYEB MREBM ILCEB FHSCV CSNFL
FTKFL UTJFV MQHYQ ITJUD CZTRT ZNTEL
MQSLC MIITJ TLCLF QTBMH MLZUJ FSUVT
ENPMV TPCJM FZDCQ SCJMZ TNFLT KFLUT
JVMQH FQHUS TELTV YHFZF JLTHS TPTNJ
FSRYV TJKCL TQSFL IFPIL TKUDL FIPCZ
TLYIM NMPUE UDTPT QCSCL STPLT NMHFP
FLCKF QLCZT LCKNJ FSUNP TQSMV QFHIF
VFQMU BJFQH IFJQC KUQTS PTLCH STPTR
YNPCN FILTM IBFJC JMZIF QTLTD TILFM
QHMIU VTSQC BMPMZ QFBUL TZDQK TVJFQ
SLCKN MQSUN TKMIB FJCJC PUIMJ ATCEB
KFLL
```

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

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (klíč systému)
Správná odpověď: FREITAG
Body: 2

Otevřený text:
Policejnímu řediteli Wasermannovi. Vážený pane, na základě předchozí korespondence a výzvy k prošetření podezřelých obchodních aktivit pana Emanuela Vosky sděluji, že bezpečnostní oddělení našeho konzulátu věc prověřilo a zjistilo, že pan Emanuel Voska skutečně vykázal některé platby velmi nestandardně. Můj nadřízený doporučuje řešit interně pokáráním a snížením platu. Přesto však dává souhlas k dalšímu šetření, které by případně odhalilo, zda se nejedná o škodu většího rozsahu než jsme vlastním postupem odhalili. Rudolf Eichmann.

Přepis do mezinárodní abecedy
POLICEJNIMU REDITELI WASERMANNOVI VAZENY PANE NA ZAKLADE PREDCHOZI KORESPONDENCE A VYZVY K PROSETRENI PODEZRELYCH OBCHODNICH AKTIVIT PANA EMANUELA VOSKY SDELUJI ZE BEZPECNOSTNI ODDELENI NASEHO KONZULATU VEC PROVERILO A ZJISTILO ZE PAN

EMANUEL VOSKA SKUTECNE VYKAZAL NEKTERE PLATBY VELMI NESTANDARDNE MUJ NADRIZENY DOPORUCUJE RESIT INTERNE POKARANIM A SNIZENIM PLATU PRESTO VSAK DAVA SOUHLAS K DALSIMU SETRENI KTERE BY PRIPADNE ODHALILO ZDA SE NEJEDNA O SKODU VETSIHO ROZSAHU NEZ JSME VLASTNIM POSTUPEM ODHALILI RUDOLF EICHMANN

Nápověda k úloze č.4 - Mise 3 (Emanuel Voska)
Nápověda k zadání správného řešení (klíč použité šifry).

Dodatečně zveřejněná nápověda:
Základní šifrový systém. Dostatečná délka textu k vyluštění. Klíč se v tomto případě dá vyčíst z převodové tabulky. Jeho délka je 7.

úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení sys-tému
4	*******	2	(klíč použité šifry)	Mise 3 (Emanuel Voska)	nalezení klíče k JZ

Úloha č.5
Mise 3 – dokončení (Emanuel Voska)

Šifrový text

```
NMJCE TDLCK UPTIC STJCW FQTPK FLLMV
CVFZT LYNFL TLFZF HJFIT NPTIE BMZCH
MPTQN MLITL ETFVY ZVYHN PMQTS PTLCN
MITZP TJYEB MREBM ILCEB FHSCV CSNFL
FTKFL UTJFV MQHYQ ITJUD CZTRT ZNTEL
MQSLC MIITJ TLCLF QTBMH MLZUJ FSUVT
ENPMV TPCJM FZDCQ SCJMZ TNFLT KFLUT
JVMQH FQHUS TELTV YHFZF JLTHS TPTNJ
FSRYV TJKCL TQSFL IFPIL TKUDL FIPCZ
TLYIM NMPUE UDTPT QCSNM UZTCL STPLT
NMHFP FLCKF QLCZT LCKNJ FSUDT ILFJM
QTNMU ZTMIP MRLTE BYRYV UETSL CESVC
FNPMS MQTIM KLCVF ZTIFJ QCQTS PTLCL
TLCLU SLTPU IMJAT CEBKF LL
```

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

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (klíč systému)
Správná odpověď: FREITAG
Body: 1

Otevřený text:
Policejnímu řediteli Wasermannovi Vážený pane na základě předchozí korespondence a výzvy k prošetření podezřelých obchodních aktivit pana Emanuela Vosky sděluji že

bezpečnostní oddělení našeho konzulátu věc prověřilo a zjistilo že pan Emanuel Voska skutečně vykázal některé platby velmi nestandardně Můj nadřízený doporučuje řešit pouze interně pokáráním a snížením platu Jednalo se pouze o drobné chyby v účetnictví a proto se domnívá že další šetření není nutné Rudolf Eichmann

Přepis do mezinárodní abecedy
POLICEJNIMU REDITELI WASERMANNOVI VAZENY PANE NA ZAKLADE PREDCHOZI KORESPONDENCE A VYZVY K PROSETRENI PODEZRELYCH OBCHODNICH AKTIVIT PANA EMANUELA VOSKY SDELUJI ZE BEZPECNOSTNI ODDELENI NASEHO KONZULATU VEC PROVERILO A ZJISTILO ZE PAN EMANUEL VOSKA SKUTECNE VYKAZAL NEKTERE PLATBY VELMI NESTANDARDNE MUJ NADRIZENY DOPORUCUJE RESIT POUZE INTERNE POKARANIM A SNIZENIM PLATU JEDNALO SE POUZE O DROBNE CHYBY V UCETNICTVI A PROTO SE DOMNIVA ZE DALSI SETRENI NENI NUTNE RUDOLF EICHMANN

Nápověda k úloze č.5 - Mise 3 - dokončení (Emanuel Voska)
Nápověda k zadání správného řešení (-12).

Dodatečně zveřejněná nápověda:
Pokud vyřešíte správně předchozí úlohu, pak je to jen otázka chvíle, jak vyřešit i tuto.

úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení sys-tému
5	**********	1	(-12)	Mise 3 (Emanuel Voska)	jednoduchá záměna

Pokračování v příběhu
Mise 4 – test pro Bletchley Park

Po prvních úspěšných misích následovaly další a další. Pomalu se tato zajímavá práce stávala pro Dr. Petera Hayeka rutinou.

Rád uvítal kratší dovolenou, kterou, jak bylo mezi pracovníky Ultima Paradise zvykem, trávil na pobřeží třetihorního moře. Zpravidla volili ke svému odpočinku návštěvu doby v eocénu. Vyhovovaly jim zde vládnoucí velmi vysoké teploty. Líbilo se jim, že většinu planety pokrývaly lesy (dokonce i na jižním pólu). Tropické deštné lesy zasahovaly až k 45° zeměpisné šířky. Oni měli svůj kamp na břehu moře v oblasti dnešního Španělska. Den trávili výlety na různá místa tehdejšího světa a prohlídkou krajiny. Někteří se zabývali lovem ryb a ptáků. Večer pak zasedli ve společenské místnosti a střídali se ve vyprávěních, která se skládala jednak z příběhů, které zažili dříve než se stali Strážci, a jednak z příběhů, které Strážci na svých misích prožili. Tím, že byli z různých časů, tak byly příběhy vždy pro všechny velmi zajímavé.

Přímo z dovolené odjížděl Peter na další misi. Tentokrát to bylo do Londýna těsně před druhou světovou válkou. Do doby, kdy se vybírali vhodní kandidáti do Bletchley Parku, který sehrál během druhé světové války tak důležitou úlohu v luštění a zpracování informací, že se pro další desetiletí a jak od kolegů věděl i pro další staletí stal synonymem pro velký úspěch kryptologů a to zejména v prolomení německého šifrového stroje Enigma.

Ze zprávy kryptoanalyticko-historického oddělení:

Winston Churchill si byl plně vědom důležitosti práce v Bletchley a 6. září 1941 kryptoanalytiky navštívil. Při setkání byl překvapen podivnou směsicí lidí, kteří mu poskytovali tak hodnotné informace; vedle matematiků a lingvistů tam byl také specialista na porcelán, kurátor pražského muzea, mistr Británie v šachu a četní experti na bridž. Churchill řekl siru Stewartu Menziesovi, šéfovi Secret Intelligence Service: „Řekl jsem vám, abyste obrátili každý kámen, ale nečekal jsem, že to vezmete tak doslova.“ I přes tento komentář měl velkou slabost pro nesourodý tým.

Vlivem neočekávané energetické fluktuace se stalo, že specialista na porcelán John Gordon do Government Code and Cypher School při Blatchley Parku nebyl vybrán, protože nezaslal formulář s kódem, kterým by prokázal, že vyluštil předložené šifrové úkoly. Dokonce nebyl vybrán nikdo, kdo by se zabýval porcelánem. To bylo potřeba dát do pořádku, neboť by jinak všeobecně známá zpráva z návštěvy Winstona Churchilla nebyla pravdivá a pro soulad s oficiálními dějinami je proto nutné, aby Peter vyhledal Johna Gordona a pomohl mu vyluštit úlohy, které by mu zajistily pozvánku do kurzu a následné přijetí do Bletchley.

Peter úkol splnil velmi snadno. John všechny úkoly totiž poměrně snadno vyřešil, ale nebyl schopen do formuláře zapsat správný výsledek. Johnovi totiž stále nedocházelo, co tam má napsat. Tady mu Peter velmi nenápadně napověděl a John pak již snadno správně vyplnil zbývající údaj do formuláře a následně byl proto pozván na pohovor a do Bletchley Parku byl přijat.

Úloha č.6
Test pro Bletchley I.

Šifrový text

```
REKCU RDFRE TEPDI ASGNI EBTNS ITAHW
RAEHO TSINO ITACI NUMMO CNIGN IHTTN
ATROP MITSO MEHTE ERHTY TNEWT DNAEN
OKSAT
```

Systém: psáno pozpátku
Upřesnění: anglický text

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

Otevřený text:
Task one and twenty-three. The most important thing in communication is to hear what isn't being said. *Peter F. Drucker*

Otevřený text přepis do češtiny :
Úloha jedna a dvacettři. Nejdůležitější věc v komunikaci je slyšet to, co nebylo řečeno nahlas.

Přepis do mezinárodní abecedy
TASK ONE AND TWENTY THREE THE MOST IMPORTANT THING IN COMMUNICATION IS TO HEAR WHAT ISNT BEING SAID PETER F DRUCKER

Dodatečně zveřejněná nápověda:

úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení sys-tému
6	***	1	(2)	Test pro Bletchley I.	transpozice

Úloha č.7
Test pro Bletchley II.

Šifrový text

```
AXTYI TTTXA EIYJZ XSIET ZJXKH OXOBX TZLEX VXWLX OYBZN YXAEX NGXDF QILNX
FWXIY XFEXK ORXTT UVAAX ELSTB NXEEN JOIXN KUWMW XTNXH YMPGZ XEDXM HXOMX
SPXTL VSNLX IQXMC XPQXO QXRFB QKSXT WXATU KSOXN HXTFX TPUTW CXHHX IQWFV
HXNEX GRXIT XNURM IBXCP XOIAD ICXMD XMOGS QGXUJ XNMXI ZJHFU XCJXA HXTCG
BAWXI FXOJT SJUXN HXIPR FPRXS QEIQJ XTLXO CXHAR NBIXE TXAEX RMSUY TXWHQ
MORXH EXKDH XAAXT BXIHD DOBXS ZRECN XNTUM CQXTP XBGXE BLMHF XINRC JNXND
XGMXS QXAQX INXDS EZQVX PZFJK MXEVA NPEXT KXEHX RYFND FXFKX DEPWM RXRWE
GSMXU EXCRX KDXET YMUEX RXXXX
```

Systém: Doplněno náhodnými písmeny - klamači
Upřesnění: Text se získá vypsáním písmen za písmenem X

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

Otevřený text:
Task two and fifteen The most important thing in communication is to hear what isn't being said. Peter F. Drucker

Otevřený text přepis do češtiny :
Úloha dva a patnáct. Nejdůležitější věc v komunikaci je slyšet to, co nebylo řečeno nahlas.

Přepis do mezinárodní abecedy
TASK TWO AND FIFTEEN THE MOST IMPORTANT THING IN COMMUNICATION IS TO HEAR WHAT ISNT BEING SAID PETER F DRUCKER

Dodatečně zveřejněná nápověda:

úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení sys-tému
7	*******	2	(3)	Test pro Bletchley II.	steganografie

Úloha č.8
Test pro Bletchley III.

Šifrový text

```
UOARA RAAET RAETE DLZTJ IEVOU IAIEL
STOOE YOEEO ALSAH NNCRL BNCTE YSJCK
NMKCV SEIEU JNSSI YCLDI TITHL
```

Systém: Transpozice
Upřesnění: Vypisování textu střídavě odpředu a odzadu

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

Otevřený text:

```
Úloha tři a tři a dále čtyři a šest. Nejdůležitější věc v komunikaci je
slyšet to, co nebylo řečeno nahlas.
```

ULOHA TRI A TRI A DALE CTYRI A SEST NEJDULEZITEJSI VEC V KOMUNIKACI JE SLYSET TO CO NEBYLO RECENO NAHLAS

Dodatečně zveřejněná nápověda:

úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení sys-tému
8	******	1	(-1)	Test pro Bletchley III.	transpozice

Úloha č.9
Formulář pro Bletchley

Šifrový text

```
NYNIZ BYVAV YBRAT KODOV ESLOV
OAZAP SATJE JDOFO RMULA RETIM
PROKA ZETEZ EJSTE VSEVY RESIL
AJSTE PRONA SZAJI MAVYX XXXXX
```

Systém: výběr slova z tabulky
Upřesnění: výběr písmen z tabulky se uskuteční na základě výsledků předchozích tří úloh.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: neuvdena
Správná odpověď: LOOP
Body: 3

Otevřený text:
Nyní zbývá vybrat kódové slovo a zapsat jej do formuláře. Tím prokážete, že jste vše vyřešil a jste pro nás zajímavý.

Přepis do mezinárodní abecedy
NYNI ZBYVA VYBRAT KODOVE SLOVO A ZAPSAT JEJ DO FORMULARE TIM PROKAZETE ZE JSTE VSE VYRESIL A JSTE PRO NAS ZAJIMAVY

Přepis do tabulky

```
          1           2
12345 67890 12345 67890 12345
NYNIZ BYVAV YBRAT KODOV ESLOV
OAZAP SATJE JDOFO RMULA RETIM
PROKA ZETEZ EJSTE VSEVY RESIL
AJSTE PRONA SZAJI MAVYX XXXXX
```

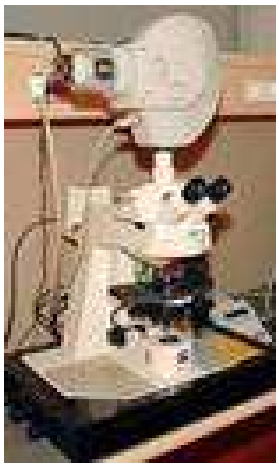
Dodatečně zveřejněná nápověda:

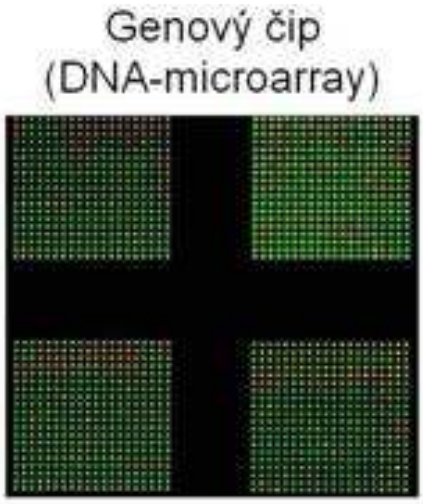
úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení sys-tému
9	****	3	neuvedeno	Formulář pro Bletchley	"IQ" ("Jordanova mřížka")

Pokračování v příběhu
Mise 5

Po úspěšných misích následovaly další a další. Dr. Peter Hayek byl vždy úspěšný a mezi Strážci byl považován za úspěšného a spolehlivého kolegu.
Peter rád využíval volný čas ke studiu a rozhovoru s kolegy. Nikdy se přitom nenudil, každý z jeho kolegů byl jiný a to v tom nejpravějším slova smyslu. Každý byl odborníkem na jiný obor a pocházeli z různých staletí. Rád vyhledával společnost genetika Johna Miltona z historicko-analytického oddělení, který mu vysvětloval co se v jednotlivých stoletích událo zásadního a jak jeho oddělení vlastně kontroluje, že nedošlo k úmyslné nebo neúmyslné energeticko-časové fluktuaci. Petera nejvíce zajímalo období, kdy bylo objeveno cestování v čase a celé skupiny nezodpovědných jedinců se snažily proniknout do minulosti a změnit ji ve svůj prospěch nebo prospěch idejí, který věřili. John mu popisoval, jak se podařilo jejich aktivity zastavit a nakonec zcela eliminovat. Kdyby se to nepovedlo, nepodařilo by se vybudovat stabilní svět Ultima Paradise v němž nyní lidstvo žije. Přesto zde prý pořád existovalo jisté nebezpečí, že by se podobné období zmatků mohlo opakovat. Proto také bylo vybudováno jejich středisko, které je odděleno od prostoru a času, který „normálně“ probíhá. Ne všemu Peter opět rozuměl, a tak se vyptával a vyptával.
Petera nejvíce zajímalo, jak se pozná, které dějiny jsou ty pravé. John mu vysvětloval a vysvětloval.
Tak se také Peter dozvěděl, že velmi důležitou úlohu v kontrole časové následnosti hraje analýza genetických kódů, speciálně DNA. Peter se dozvěděl, že někteří Strážci také provádí kontrolu DNA u podezřelých osob při své návštěvě v minulosti. Dokáží tak odhalit ty, kteří se tam dostali z budoucnosti nebo jsou potomky osob z budoucnosti. Ty pak musí eliminovat. Historicko-analytické oddělení nejprve zjistí, kdy se tam asi dostali – tedy přesně, kdy došlo k nějaké změně proti historickému standardu. Navrhnou operaci, která dá vše do původního stavu a tyto lidé prostě zmizí neboť vše co souvisí s jejich existencí v minulosti prostě nenastane.

Petera to zajímalo, a tak uvítal, když jej jednou John pozval k sobě do laboratoře a řekl: „Něco Ti ukáži, ale to jen Tobě, protože Tě to tak zajímá!“.





Pak John řekl: „Vidíš ten přístroj, je to nejmodernější a nejrychlejší analyzátor DNA, který tu máme. V praxi, ovšem používáme i jiné přenosné a mnohem menší. Stačí pár molekul vhodného genetického materiálu a hned se dozvíme na desítky let přesně, které je období do kterého dotyčný patří. Mimochodem půjč mi svůj odznak Strážce.“

Peter, mu podal svůj smaragd se zlatou hvězdou a vyrytým identifikačním kódem a strukturou jeho DNA. „Nyní si odeberu ještě trochu Tvého genetického materiálu. Stačí když položíš na vteřinu svoji ruku na sem na podložku pod DNA-microarray.“ Peter to udělal. John pak položil jeho odznak na kruhovou desku pod zařízení. Stiskl tlačítko a řekl. Tak a máme zde výsledek. Zařízení promítlo získané údaje na stěnu a v závěru stálo:

1) Identifikační kód uložený v odznaku byl přidělen Dr.Peterovi Hayekovi
2) Otisk DNA vložený do smaragdu a vyrytý na jeho povrch se 100% shoduje s genetickým materiálem testované osoby
3) DNA odpovídá typu GlowThetaQ – Evropa, konec 20.století. Pravděpodobné datum narození s přesností na 20 let je 1975.

Peter se zeptal: „Stalo se, že jsi někdy odhalil neshodu?“. John se usmál a řekl: „To víš, že ano. Je to moje práce. A mimochodem, vždy, když se vracíte z mise, tak provedeme kontrolu, zda to jste opravdu vy ☺ .

Peter se zamyslel a pak řekl: „Co když se, čistě hypoteticky, stane to, že se vrátíme z mise a mezitím dojde k takové změně času, že zde sice bude vybudovaná naše stanice, ale svět a dějiny budou zcela jiné a vše zde bude sloužit k zafixování jiné časové linie. Tedy, že nás již buď bude testovat někdo jiný nebo nás nebudete testovat vůbec?“

John se smál: „To se přece nestane. Kvůli tomu zde jsme my Strážci času a naše stanice mimo prostor a čas…“.

Peter, ale na rozhovor musel stále myslet a přemýšlel, jak by si vytvořil vlastní mechanismus kontroly, aby i on po svém návratu měl jistotu, že se vrací zpět do času a stavu, který opustil. Tedy to, že čas od data jeho narození po vznik jejich stanice nebyl změněn. Pak jej napadlo, co by mohl udělat. Napsal zašifrovaně text, který označil jako závěť a tu uložil do trezoru, který měl hned vedle postele ve svém pokoji.

Od té doby se vždy po svém návratu z mise, vždy raději ve svém pokoji přesvědčil, že je vše v pořádku a žádná neočekávaná změna po jeho narození již s vysokou pravděpodobností nenastala.

Dr. Peter Hayek zase na oplátku vyprávěl svému příteli o svých misích a o kryptologii dvacátého a jednadvacátého století, o šifrových systémech a o luštění. Pro Johna Miltona bylo zase toto úplně nové. Lidé dvacátého devátého století odkud pocházel neměli o této problematice již vůbec ponětí. Bylo to pro něj tak vzdálené a nové, jakoby např. někdo zasvěcoval Petera do magických rituálů Keltů.

Peter Johnovi vyložil vše o luštění základních šifrových systémů a pak mu předložil i s výkladem tři úlohy, které musel na svých posledních misích řešit.
Prvá byla z konce devatenáctého století a to konkrétně z doby francouzsko-rakouské války a byla to zpráva generála Mac Mahona zaslaná lotrinskému maršálovi Bazainovi těsně před zahájením války.
Druhý text pocházel z I.světové války. Jednalo se o zprávu z nižšího stupně velení německé armády o výcviku vojáků čekajících v zákopech na ofenzívu.
Třetí text byl milenecký dopis z roku 2008. Jeho vyluštění bylo důležité nejen pro mileneckou dvojici, ale i pro chod dějin. Kupodivu tento velmi lehký systém dal Johnovi nejvíce práce. Důvodem samozřejmě bylo, že o této době mnoho nevěděl, a tak nemohl tušit co mladí lidé k šifrování použili.

Úloha č.10
Francouzsko-rakouská válka

Šifrový text

```
XUNQH EUFCV VEEZZ DVLPR PEQXT PMCNK ZJEFV EYEQI GKTLP EQXTC ZTZMZ EEZGG
VUKWY PWLSX AQGEG MIIRA SBWOC OHMKR ZJKRC WPVZZ JNJDE PMILR HIYYN SAIQV
DKZEP RYKEA DICSF MVBFU EAUOP JZLIO YBYPG PVEHR ZTTGE GUIET DADCA FJNMY
GZVHZ MNJEC TMARV DPJJU AYUMN HEMYN TJTBU IOENI OTNJI PBEWO UVDKZ RJRFR
ZSOWY EARDR UEETD ADCRL ZHBIX SFMYO RFBEC RJNVA ZRTUN NHVLN XQZNJ EIACZ
LLFCY OGIEC TMARV DZNFR RZCHL MVAOA AKRVU XLSZL HDJJA GVMDI XUPZZ QTBJS
DEYMN AYKIF KGDLJ CUIAR LMKVD KPIZS YKIFK GGRDU ZVTAS XQDLU EIGOU FUMGN
PNJJM ASEEC QWEAQ MIIUF DRNXC INBVK RYRNP MNVMK CNNYO IGPPN DAZPT ULROC
NHUXM AALJZ GOZNX MHCJI VRPGP SVUXI XRRIG PTTZT GOYII AUOPA MUVDD DAEUE
WBVHV ISV
```

Systém: periodické heslo, polyalfabetická substituce
Systém Vigenere

Upřesnění: periodické heslo LAVIVAFRANCE

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

Správná odpověď: VELITEL
Body: 2

Otevřený text:
Musíme počítat, že válka proti Prusku se stane válkou proti celému Německu. Pod pruským velením jsou kromě pruské a severoněmecké armády i bavorské, württenberské a bádenské jednotky. Celkem je to 500 000 vojáků, v zázemí se připravuje dalších 160 000 záložníků a 190 000 mužů zemské domobrany.

Naše rodná Francie není na válku dobře připravena. Armáda má stav 370 000 mužů, z toho 60 000 slouží v Alžírsku a 6000 v Římě. Vojsko zaujalo pouze jen obranné postavení podél 300 km hranic. Vrchního velení se podle mých zpráv ujme koncem července sám císař. Velitel lotrinské armády maršál Bazaine.

Přepis do mezinárodní abecedy
MUSIME POCITAT ZE VALKA PROTI PRUSKU SE STANE VALKOU PROTI CELEMU NEMECKU POD PRUSKYM VELENIM JSOU KROME PRUSKE A SEVERONEMECKE ARMADY I BAVORSKE WURTTENBERSKE A BADENSKE JEDNOTKY CELKEM JE TO PET SET TISIC VOJAKU V ZAZEMI SE PRIPRAVUJE DALSICH JEDNO STO SEDESAT TISIC ZALOZNIKU A JEDNOSTO DEVADESAT TISIC MUZU ZEMSKE DOMOBRANY NASE RODNA FRANCIE NENI NA VALKU DOBRE PRIPRAVENA ARMADA MA STAV TRI STA SEDMDESAT TISIC MUZU Z TOHO SEDESAT TISIC SLOUZI V ALZIRSKU A ŠEST TISIC V RIME VOJSKO ZAUJALO POUZE JEN OBRANNE POSTAVENI PODEL TRISTA KM HRANIC VRCHNIHO VELENI SE PODLE MYCH ZPRAV UJME KONCEM CERVENCE SAM CISAR VELITEL LOTRINSKE ARMADY MARSAL BAZAINE

Dodatečně zveřejněná nápověda:

úloha číslo	klíčové slovo	body	určení klíčového slova	označení úlohy	zařazení systému
10	*******	2	(-5)	francouzsko-rakouská válka	periodiceké heslo

Úloha č.11
I. světová válka

Šifrový text
```
ZELTN VAOPO FUNOE ZKYOZ OTNHI TIZIE
LOSCS CEOAC AKBAP LSVSO ERISI ALTAO
LGZNO MNTEE JHDDU UDDKY APLKV UYVLT
AABKE JVOLR EMJPO ANALJ ANHDV OOJRV
AATTK DSICS KXAMV YRASO AMKKA ZAOPE
AORIB PYCEL TPUTE SIAAK IRAND EOOAM
MZOAD NHOOO KROOI NROIV UOPAT LIMSW
NEDMZ CIYIA NUCUI EPHYD TPKPA VYNOI
NNETV NKYIV IPVKO NOVEI AZOMR ONKAO
KRKAA GODOK EPTEE EPVAY ANIPU NPIBK
EUMLO TCAZB AESID YNOIO VPPPN ZSIKC
```

```
ARTCA IRSOM PPASM AEAEY YEPVY ZUAYB
ANESC CEAUE VOPLP UEAPV ISRDO TRPKS
LOAKM DONLM EOHAO HNBEV EVZAN SJTTX
EGEEA YSTRV EDIUL NUCVA SOUUV OVAPN
YMNIE ECPMI LOYSR OTATL SADIP VYORT
UAAIN AIYPT TUINJ SYOJB ZLNUO ACNUE
TTOOP IYVIE JNIRO VAROU NKCEA UVOEL
VSSNI AACII AADIA BHRIL NEASJ EZDIS
HRKCM YVICE STYSS RCYLE TANTA KNHRO
EAHTK LCPBN SLTHV TDBMO ZTKVO ATEAL
PEVMR IERRO ITBOE VOEVV CIMPJ RASTI
OPPPZ NZAOL EALVI PEAYK IJKSD AVOOA
ZTSRA NTAVU UEOTT KCTOE EUAYA SSOSS
OEYGA NIOPY ISVEX
```

Systém: transpozice
Upřesnění: sloupcová transpozice, tabulka 7x105
Heslo: victory (po vyčíslení se získá transpoziční heslo 6-2-1-5-3-4-7)
Doplnění pomocí X (v textu také X 1x použito, v šifrovém textu tedy celkem 3x)

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

Otevřený text:
Vážený pane generále. Dovolte mi můj názor na výcvik naší pěchoty před připravovanou ofenzívou. Důstojníci berou úkol velice vážně, avšak u prostých tento výcvik zadává dosti často příčinu k smíchu. Popíši Vám jak to v praxi vypadá. Za našimi postaveními byly na ohromné prašné a písčité ploše vyznačeny německé zákopy páskami. Vojáci vylézali ze zákopů a dobývali "pásky" - vše probíhalo naprosto nekrvavě a čistě symbolicky. Pěšáci vyrážející do akce si museli představovat plynový útok (postaralo se o to pár šluků z cigarety a zakašlání) a překonávat imaginární ostnatý drát ("Nepodvádět! Koukejte tu nohu přehodit pořádně!"). K tomu ještě musel každý pochodovat tak, jako kdyby měl na zádech plnou polní, na boku plynovou masku a nesl rýč, poštovního holuba, svitek ostnatého drátu nebo bomby. Mí kolegové považují tento výcvik považovali za potřebný, ale já si tím nejsem jist. Váš přítel Wood.

Přepis do mezinárodní abecedy

```
Vazeny pane generale Dovolte mi muj nazor na vycvik nasi pechoty pred
pripravovanou ofenzivou Dustojnici berou ukol velice vazne avsak u prostych
tento vycvik zadava dosti casto pricinu k smichu Popisi Vam jak to v praxi
vypada Za nasimi postavenimi byly na ohromne prasne a piscite plose
vyznaceny nemecke zakopy paskami Vojaci vylezali ze zakopu a dobyvali pasky
vse probihalo naprosto nekrvave a ciste symbolicky Pesaci vyrazejici do
akce si museli predstavovat plynovy utok postaralo se o to par sluku z
cigarety a zakaslani a prekonavat imaginarni ostnaty drat Nepodvadet
Koukejte tu nohu prehodit poradne K tomu jeste musel kazdy pochodovat tak
jako kdyby mel na zadech plnou polni na boku plynovou masku a nesl ryc
postovniho holuba svitek ostnateho dratu nebo bomby Mi kolegove povazuji
tento vycvik povazovali za potrebny ale ja si tim nejsem jist Vas pritel
Wood
```

Dodatečně zveřejněná nápověda:

úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení sys-tému
11	****	2	(W)	I. světová válka	transpozice

Úloha č.12
Milenecký dopis

Šifrový text

37 36 49 24 36 13 35 12 11 15 47 23 16 11 47 23 11 49 23 11 26
12 11 18 28 11 32 24 12 18 28 11 47 11 18 23 22 36 28 11 17 37
23 32 23 11 15 23 26 11 17 36 15 23 13 28 11 32 23 25 23 15 11
26 12 11 16 26 23 11 49 34 18 37 12 11 37 12 26 36 11 38 11 36
47 16 11 24 36 13 34 26 11 28 11 12 28 36 22 28 47 28 11 15 12
37 28 47 25 12

Systém: upravená mobilní šifra
Upřesnění: opakování číslice vyznačeno prvou cifrou, druhá číslice je významová
Takže 37 je v originální mobilní šifře 777 , tedy písmeno R (písmeno, které se získá na displeji mobilu trojím stisknutím číslice 7)

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (-1)
Správná odpověď: JARUSKA
Body: 4

Otevřený text:
Rozhodla jsem se, že na tu chatu s Tebou přece jen pojedu. Čekej na mne zítra ráno v osm hodin u autobusu. Jaruška

Přepis do mezinárodní abecedy
ROZHODLA JSEM SE ZE NA TU CHATU S TEBOU PRECE JEN POJEDU CEKEJ NA MNE ZITRA RANO V OSM HODIN U AUTOBUSU JARUSKA

Mobilní šifra
777 666 9999 44 666 3 555 2 1 5 7777 33 6 1 7777 33 1 9999 33 1 66 2 1 8 88 1 222 44 2 8
88 1 7777 1 8 33 22 666 88 1 7 777 33 222 33 1 5 33 66 1 7 666 5 33 3 88 1 222 33 55 33 5 1
66 2 1 6 66 33 1 9999 444 8 777 2 1 777 2 66 666 1 888 1 666 7777 6 1 44 666 3 444 66 1 88
1 2 88 8 666 22 88 7777 88 1 5 2 777 88 7777 55 2

Úprava do dvojic počet opakování/významová číslice
37 36 49 24 36 13 35 12 11 15 47 23 16 11 47 23 11 49 23 11 26
12 11 18 28 11 32 24 12 18
28 11 47 11 18 23 22 36 28 11 17 37 23 32 23 11 15 23 26 11 17
36 15 23 13 28 11 32 23 25 23 15 11
26 12 11 16 26 23 11 49 34 18 37 12 11 37 12 26 36 11 38 11 36
47 16 11 24 36 13 34 26 11 28
11 12 28 36 22 28 47 28 11 15 12 37 28 47 25 12

Dodatečně zveřejněná nápověda:

úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení sys-tému
12	*******	4	(-1)	Milenecký dopis	Mobilní šifra

Pokračování v příběhu
Poslední míse

Peter si na svůj nový život zvykl. Byl spokojen. Dobrodružství, která prožíval během plnění jednotlivých misí, jej naplňovala spokojeností. Měl však jedinou noční můru, pocházel z doby, kdy nedůvěra byla lidem vlastní a bál se, aby to vše kolem nezmizelo jako mávnutím čarovného proutku. Věděl, že kdyby se k moci dostala některá ze skupin, které se v dějinách čas od času objevovaly, že by se to mohlo stát, zvláště, kdyby se jejich členové dostali mezi samotné strážce. Věřil v poslání Strážců času, věřil v jejich sílu, moc a věrnost, ale stále si říkal, co když přece jen….

Po návratu na základnu z jedné z misí se začal odehrávat děj, kterého se tolik bál, ale na který ve svých snech a myšlenkách již byl připraven.

Hned po vystoupení z výtahu jej místo standardního textu „Vítejte na základně! Blahopřejeme ke splnění úkolu!“ Čekal ho text mnohem chmurnější, který zde byl uveden hned ve dvou jazycích, které pravděpodobně převládly na světě před jeho návratem z minulosti.

走到了身份检查。游侠，谁不控制，将被处以的职业损失，将不得不离开基地。

એ ક ઓળ ખ ચકાસવા માટે આવે છે. રેન્જર, જે નિયંત્રિત કરવા નિષ્ફળ જાય કારકિર્દી નુકસાન સજા થશે અને એ આધાર રજા રહેશે.

Pokynu se podrobil. Prošel detekční místností a pak byl odveden k veliteli základny.

Ten jej uvítal velmi chladně a hned potom pokračoval. „Pane doktore, nevím kdo jste, ale bylo mi oznámeno, že vaše identifikace byla negativní. V databázi Strážců nejste uveden. Musím vám oznámit, že ať jste kdo jste, budete muset ihned opustit základnu. Nebudu pátrat, proč jste se snažil na základnu vniknout. Nechám vás odejít. Za těmito dveřmi je časový výtah. Vyberte si konkrétní rok, měsíc a den a já vám vydám naprogramovanou kartu s nahraným cílem dle vašeho výběru a slibuji, že tím je celá věc vyřízena.“

Peter byl však na situaci připraven. Podíval se veliteli základny zpříma do očí a řekl:
„Věřím, že jste skutečný Strážce času a důvěřuji vám. Jenže já jsem jím také a mohu vám to dokázat! Nevím však, co se s naší základnou a Ultima Paradise stalo, ale bojím se, že buď vlivem nějaké rozsáhlé časové fluktuace nebo zásahem nějaké skupiny došlo ke změně, která se, ač se to nemělo stát, dotkla i naší základny.“

Velitel stroze odvětil: „Dokažte mi to a já podle toho rozhodnu“.

Peter pak začal vyprávět svůj příběh, zopakoval přísahu Strážců a vyprávěl vše, co věděl. Bylo vidět, že velitel naslouchal velmi pozorně. Nakonec velitel uzavřel jeho vyprávění slovy: „Rád bych uvěřil, ale vše, co jste vyprávěl, jste se mohl dozvědět někde mimo základnu od některého ze Strážců. Cítím však, že na základně opravdu není poslední dobou vše tak, jak bych očekával. Něco se mi samotnému nelíbí. Intuice mi říká, že vám mám věřit, ale nemohu, nesmím. Dokažte mi, že máte pravdu a pak začneme spolu pátrat, co se stalo…“
Peter jej ujistil, že doufá, že důkaz existuje. Pak pokračoval: „Sepsal jsem svůj příběh a je zašifrován tak, že mohu dokázat, že jsem jej zašifroval já. Lze také dokázat, že jej zašifrovala osoba, která se narodila kolem roku 1975 a navíc, že tou osobou je Strážce času.“

Velitel Petera vyslechl a pak se s ním vydal pro jeho důkaz. Peter jej vedl, a tím prokázal, že základnu zdá. Pravda, leccos se změnilo, ale zase ne tolik, aby se nedostal ke své skrýši. Základna byla mimo prostor a čas, a proto vnější časová změna nezměnila nic uvnitř. Změny byly výsledkem konání až konkrétních osob. Zašifrovaný text, důkaz, který Peter hledal, byl proto ve své skrýši v jeho bývalém pokoji. Peter jej radostně ukázal veliteli a řekl: „Zde je důkaz !“ a k textu přidal i svůj odznak.

Velitel odnesl text do analytického oddělení a vydal rozkaz šifrový text celý dešifrovat. Začátek textu vypadal následovně:

Po dešifraci textu velitel základny pochopil, že má Peter pravdu. Velitel proto svolal do hlavní auly základny všechny Strážce času. Zahájil mimořádnou schůzi. Nejprve Dr. Petera Hayeka představil, pak oznámil, že se podařilo zjistit, že na základnu pronikl někdo, kdo měl za úkol ochromit službu Strážců. Tomu někomu se to povedlo. Potom velitel všechny přítomné seznámil s jasným důkazem, že Peter je ten, za koho se vydává. Na závěr velitel oznámil, že schůze bude ukončena, až se zjistí, kdo je tím zrádcem. Ihned po jeho odhalení bude analyticko-historickému oddělení zadán úkol vypracovat postup, jak vrátit vše zpět, do stavu před zdařeným proniknutím zrádce na základnu.

Peter se zúčastnil hledání zrádce. Nejprve do jedné poloviny sálu nechal přesednout všechny, které znal. Následně se rozhodli hledat zrádce mezi těmi, které neznal ani podle vidění. Dalo se očekávat, že se zrádce dostal na základnu v době mezi jeho odchodem na misi a návratem z mise. Osob, které neznal, bylo relativně málo a to jen šest. Jejich národnosti byly ARAB, BASK, GRUZÍNEC, JAPONEC, GUDŽARÁT , TAMILEC.

Peter se zamyslel a pak ukázal na jednoho z nich. Při následném šetření se ukázalo, že měl pravdu. Peterovi byl dotyčný nápadný mimo jiné i tím, že jeho jméno délky 4 začínalo na písmeno, které v jazyce jeho údajného národa se nepoužívá.

Následovala perfektní analytická práce historicko-analytického oddělní. Do minulosti byla vyslána mise. Z hlediska základny uběhlo jen několik vteřin, když se otevřely dveře časového výtahu a mise se úspěšně vrátila. Že byla úspěšná, bylo vidět na prvý pohled, odhalený zrádce již mezi čekajícími Strážci nebyl, prostě zmizel. Také nadpis proti výtahu se jako mávnutím proutku změnil. Stálo zde: „Vítejte na základně! Blahopřejeme ke splnění úkolu!“

Peter tak splnil ten nejtěžší úkol, který pro něj osud připravil.
Když usínal a myslel na toho zrádce, uvědomil si, že jeho jméno jde napsat z prvých písmen, kterými si značil úkoly, které splnil.

Úloha č.13

Text úlohy

走到了身份检查。游侠，谁不控制，将被处以的职业损失，将不得不离开基地。

એ ક ઓળ ખ ચકાસવા માટે આવે છે. રેન્જર, જે નિયંત્રિત કરવા નિષ્ફળ જાય કારકિર્દી નુકસાન સજા થશે અને એ આધાર રજા રહેશે.

Systém: přepis textu do dvou různých méně obvyklých jazků
Upřesnění: překlad (oboustranný) pomocí Google překladače
Jazyk Čínština a Gudžárština (dále využito v úloze č.15)

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

Otevřený text:
Dostavte se na kontrolu totožnosti. Strážce, který se ke kontrole nedostaví, bude odsouzen ke ztrátě povolání a bude muset opustit základnu.

Překlad a přepis do jednoduché čínštiny:

走到了身份检查。游侠，谁不控制，将被处以的职业损失，将不得不离开基地。

Zpětný překlad pomocí Google-překladače:
Šel do kontroly totožnosti. Ranger, který nemá kontrolu, ztráty pracovních míst, bude potrestán, bude muset opustit základnu.

Překlad a přepis do Gudžárštiny:

એ ક ઓળ ખ ચકાસવા માટે આવે છે. રેન્જર, જે નિયંત્રિત કરવા નિષ્ફળ જાય કારકિર્દી નુકસાન સજા થશે અને એ આધાર રજા રહેશે.

Zpětný překlad pomocí Google-překladače:
Je ověření identity. Ranger, který nedokáže ovládat poškození jeho kariéra bude potrestán a opustí základnu.

Dodatečně zveřejněná nápověda:

úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení sys-tému
13	********	3	(-1)	Nadpis u výtahu času	?

Úloha č.14

Šifrový text

```
LOEGA PBYGP GVXXH CRGMM KNZUT KXTPL
GFYGR YTEAB TYKHT HBTRV USQCI YBXNO
DPGDU JUIXO PXBIG JSKHR IHTKM FAOHA
JQUIT HLZOF ULGLP XUDTZ CTSBO LIOJX
PVIMA GIXQD WMTFZ GCUGF BDUHE YEPYT
PBZQJ UMHTG QZWDA EYMXG FIGCA YA
```

Systém: „Absolutne bezpečný systém“,
ve skutečnosti Vigenere cipher s dlouhým periodickým heslem
Klíč (120 znaků):
CCATGGTGCACCTGACTCCTGAGGAGAAGTCTGCCGTTACTGCCCTGTGGGGCAAGGTGAACG
TGGATGAAGTTGGTGGTGAGGCCCTGGGCAGGTTGGTATCAAGGTTACAAGACAGGT
Klíč je řetězec, který lze nalézt na obrázku v doprovodném příběhu k Misi č.5. Text tohoto příběhu také obsahuje řadu indicií, že jedna z úloh bude na „absolutně bezepčný systém“ a lze předpokládat, že bude použit uvedený „genetický řetězec“. Stačí tedy řetězec vypsat a posunovat po šifrovém textu za současného sčítání modulo 26.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil: (5)
Správná odpověď: TENTO
Body: 20

Otevřený text:
Jmenuji se Peter Hayek. Tento text jsem sepsal a zašifroval pomocí svého DNA kódu pro případ, že bych někdy v budoucnosti musel prokázat svoji identitu a pro důkaz, že jsem v době sepsání tohoto textu byl Strážce času.

Přepis do mezinárodní abecedy
JMENUJI SE PETER HAYEK TENTO TEXT JSEM SEPSAL A ZASIFROVAL PO-
MOCI SVEHO DNA KODU PRO PRIPAD ZE BYCH NEKDY V BUDOUCNOSTI MU-
SEL PROKAZAT SVOJI IDENTITU A PRO DUKAZ ZE JSEM V DOBE SEPSANI
TOHOTO TEXTU BYL STRAZCE CASU

Dodatečně zveřejněná nápověda:

úloha číslo	klíčové slovo	body	určení klíčového slova	označení úlohy	zařazení systému
14	?	20	(5)	Důkaz	?

Úloha č.15

Úloha
Národnost a jméno zrádce. Napsat bez mezery.

Systém: jméno lze odhadnout podle jazyka ve kterém byl nápis, jméno lze poskládat z prvých písmen řešení úloh.

Nápověda pro výběr slova dokazujícího, že řešitel úlohu vyluštil:
Správná odpověď: GUDZARATWONT

Body: 2

Otevřený text:
Gudžarát Wont

Z nápovědy a předchozích indicií získaných zejména řešením úlohy č. 13 plyne, že zrádce je ze státu GUDŽARÁT. Vypsáním všech prvých písmen řešení úloh se získá množina písmen ze, kterých je potřeba složit hledané slovo délky 4. Úloha je sice pracnější, ale logicky poměrně nenáročná.

Další nápovědou bylo, že jméno zrádce začíná na písmeno, které gudžárštině není (W) a tedy se počet slov významně zmenšil.

Její zařazení mělo především zajistit to, že vítěz prokáže trpělivost a nestane se (jako v minulých ročnících), že rozdíl mezi prvním a druhým bude 1 vteřina ☺.

Všem úspěšným řešitelům BLAHOPŘEJI!

Souhrnná zveřejněná nápověda ke zveřejněným úlohám

úloha číslo	klíčové slo-vo	body	určení klíčového slova	označení úlohy	zařazení systému
1	********	2	neuvedeno	vstupní test	"IQ" (citát)
2	*****	2	(3)	Mise 1 (Sever proti Jihu, Shiloh)	jednoduchá záměna
3	**********	3	(KOMU)	Mise 2 (Petr Vok)	jednoduchá záměna
4	*******	2	(klíč použité šifry)	Mise 3 (Emanuel Voska)	nalezení klíče k JZ
5	**********	1	(-12)	Mise 3 (Emanuel Voska)	jednoduchá záměna
6	***	1	(2)	Test pro Bletchley I.	transpozice
7	*******	2	(3)	Test pro Bletchley II.	steganografie
8	******	1	(-1)	Test pro Bletchley III.	transpozice
9	****	3	neuvedeno	Formulář pro Bletchley	"IQ" ("Jordanova mříž-ka")
10	*******	2	(-5)	francouzsko-rakouská válka	periodiceké heslo
11	****	2	(W)	I. světová válka	transpozice
12	*******	4	(-1)	Milenecký dopis	Mobilní šifra
13	********	3	(-1)	Nadpis u výtahu času	přpis do jiného jazka / abeceda
14	?	20	**(5)**	Důkaz	Absolutne bezpečný systém“, Vigenere ci-pher s dlouhým heslem
15	**************	2	neuvedeno	Zrádce (Závěrečný test)	IQ
součet:		**50**		**konec**	

C. Soutěž 2011 - Statistika soutěže, úspěšnost, řešitelé

Přehled úspěšnosti řešení jednotlivých soutěžních úloh

Celkem publikovaných úloh: 15

1. úloha (2 body) (48 řešitelů)
2. úloha (2 body) (42 řešitelů)
3. úloha (3 body) (28 řešitelů)
4. úloha (2 body) (25 řešitelů)
5. úloha (1 bod) (25 řešitelů)
6. úloha (1 bod) (26 řešitelů)
7. úloha (2 body) (26 řešitelů)
8. úloha (1 bod) (25 řešitelů)
9. úloha (3 body) (18 řešitelů)
10. úloha (2 body) (22 řešitelů)
11. úloha (2 body) (21 řešitelů)
12. úloha (4 body) (22 řešitelů)
13. úloha (3 body) (20 řešitelů)
14. úloha (20 body) (7 řešitelů)
15. úloha (2 body) (9 řešitelů)

Maximální počet bodů za publikované úlohy: 50

Soutěžící

Soutežící, kteří vyřešili všechny úlohy:

1	**Klepetko**	50	27.11 (21:37)
2	**elpepe73**	50	28.11 (10:25)
3	**ony**	50	03.12 (19:51)
4	MD5Mir	50	03.12 (20:26)
5	Mirop	50	04.12 (12:24)
6	**mim3**	50	04.12 (21:22)
7	peddy	50	05.12 (19:33)

Pořadí do dvacátého místa:

pořadí	už.jméno	počet bodů	datum poslední akce
8	**Lokna**	30	29.11 (17:24)
9	paulie	30	04.12 (22:48)
10	andrej	28	27.11 (16:46)
11	misof	28	27.11 (17:25)
12	kasparov2	28	27.11 (17:44)
13	koc	28	27.11 (19:00)
14	Bob	28	27.11 (19:02)
15	luka	28	27.11 (19:22)
16	walros	28	27.11 (21:41)
17	**kesy**	28	28.11 (10:03)
18	Kulhavka	25	01.12 (15:30)
19	hodiny	25	05.12 (09:13)
20	jira_k	22	27.11 (18:47)

Celkem soutěžících:	**68**
Počet soutěžících, kteří vyřešili alespoň 1 úlohu:	48
Počet soutěžících zařazených do slosování:	24

D. Soutěž 2011 - Ceny a loga sponzorů

1.cena

Pro vítěze celé soutěže byla i letos připravena tradiční hlavní cena - bezplatná účast na mezinárodním **kryptologickém workshopu Mikulášská kryptobesídka** http://mkb.buslab.org/ , který se konal 1.- 2.prosince v Praze. Pořadatelé 11.ročníku Trusted Network Solutions (http://www.kernun.cz/) a BUSLab (http://www.buslab.org/) uhradili za vítěze registrační poplatek.

Mikulášská kryptobesídka 2011
Praha, 1.–2. prosinec 2011
tns TRUSTED NETWORK SOLUTIONS
BUSLab

Další odměnou pro vítěze pak byl dále zisk **rok web hostingu zdarma** (multihost/ftp/web), který věnovala firma HEXAGEEK http://www.hexageek.com/ .

Kernun

2.- 3. cena

Rok hostingu zdarma (multihost/ftp/web) a dále **registrace domény zdarma** (dle výběru CZ nebo SK). Věnovala firma HEXAGEEK http://www.hexageek.com/ .

HEXAGEEK

Dále byly předány 3 ceny pro náhodně vylosované úspěšné řešitele

(losovalo se 5.12.2011 ze všech řešitelů, kteří splnili limit pro zařazení do losování –zisk 15ti bodů)

1.vylosovaný: kniha P.Vondruška: Kryptologie, šifrování a tajná písma , edice OKO, nakladatelství Albatros, 2006, věnoval autor http://crypto-world.info/oko/index.php .

2. – 3. vylosovaný: registrace domény zdarma (dle výběru CZ nebo SK), věnovala firma HEXAGEEK http://www.hexageek.com/ .

HEXAGEEK

Informační server SOOM.cz si vás dovoluje pozvat na

SOOM Hacking & Security konferenci

s podtitulem hacking z různých perspektiv

Cílem konference je přiblížit účastníkům problematiku hackingu a ICT security tak, jak jí vnímají jednotlivé zainteresované strany. Vedle etických hackerů nebo předních odborníků na malware a kryptologii vystoupí na konferenci také zástupci z řad Policie ČR, práva a zástupce největšího českého portálu Seznam.cz.

Na návštěvníky konference čeká mnoho odborných přednášek. **Roman Kümmel** a **Martin Klubal** ze serveru SOOM.cz přiblíží nejčastější zranitelnosti současných webových aplikací, slabiny poskytovatelů webhostingu a registrátorů domén. **Igor Hák** s **Robertem Lipovským** z antivirové společnosti ESET poodhalí nejčastější útoky, které používají současní tvůrci malware. **Martin Dráb** ze serveru secit.sk naváže na problematiku škodlivého softwaru se svou přednáškou zaměřenou na implementaci systémů HIPS. Kryptologové **Vlastimil klíma**, **Tomáš Rosa** a **Pavel Vondruška** z Crypto-World.info seznámí návštěvníky s historií hledání absolutně bezpečné šifry a s možnostmi implementace bezpečnosti ve velmi malém prostoru, který představují RFID čipy. Opomenuty nezůstanou ani slabiny, které tato omezení mohou přinášet. **Mjr. Mgr. Václav Písecký** přiblíží práci Policie ČR při vyšetřování informační kriminality a vyvrátí některé mýty a pověry, které jsou s informační policií spojovány. **Vlastimil Pečínka** ze společnosti Seznam.cz se zmíní o prevenci a postupech při bezpečnostních incidentech na straně provozovatele webových aplikací. Chybět nebude ani zástupce z právnických řad, který návštěvníkům přiblíží paragrafy naší legislativy související s ICT a poukáže na tenkou hranici mezi etickým a ilegálním hackingem.

Konference se bude konat ve čtvrtek

2.února 2012

v příjemném prostředí konferenčních prostor

pražského hotelu Michael.

Účast na konferenci je podmíněna předchozí registrací a úhradou účastnického poplatku ve výši 300,-Kč.

Bližší informace včetně seznamu jednotlivých přednášek a možnost registrace jsou k dispozici na adrese:

http://www.soom.cz/konference

F. O čem jsme psali v lednu 2000 – 2011

G. Závěrečné informace

1. Sešit

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

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 Vlastimil Klíma Tomáš Rosa Dušan Drábik
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Jaroslav Pinkava
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.cz ,	http://crypto.hyperlink.cz/
Dušan Drábik	Dusan.Drabik@o2bs.com ,	
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