Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 12, číslo 9/2010 **17.září 2010**

9/2010

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1370 registrovaných odběratelů)

Obsah: str.

A. Z dějin československé kryptografie, část IX.
Vzpomínky Jiřího Václava na výrobu dálnopisů a částí šifrátorů ve Zbrojovce Brno
Jiří Václav (e-mail – předá redakce e-zinu Crypto-World)

Toto velmi zajímavé sdělení upřesňuje informace o konstruktéru Weberovi a výrobě dps 302-Dalibor ve Zbrojovce Brno, které byly uvedené ve starších číslech e-zinu Crypto-World, zejména:
Crypto-World 10/2007: Z dějin československé kryptografie, část III., Paměti armádního šifranta (J.Knížek)
Crypto-World 78/2008: Šklíba,K: Z dějin československé kryptografie, část VIII., Trofejní šifrovací stroje používané v Československu v letech 1945 - 1955. Šifrátory ENIGMA, ANNA a STANDARD.
Text mi byl poskytnut pamětníkem těchto událostí a zde uvedená fakta lze považovat za důvěryhodná a opravují informace, které byly uvedeny v dřívějších článcích.
Text je otištěn s laskavým souhlasem autora, kterému tímto děkuji.

Předmět: Wdf: Dálnopisy ve Zbrojovce Brno
Od: Jiřího Václava
Datum: 8 Srpen 2010, 10:15

Vážený pane Vondruško,

se zájmem jsem si přečetl na INTERNETU Crypto-World 10/2007 o výrobě dálnopisů ve "Z" Brno, tehdy ještě Závody Jana Švermy. Jako absolvent VTA jsem začátkem r. 1957 nastoupil na umístěnku do Z Brno do Výzkumně vývojové konstrukce sdělovací techniky. V té době byl z VÚ 8871 Hradce Králové předán vzorek dálnopisu 302-Dalibor. VÚ tehdy řídil E. Řehola, ministr a pozdější ředitel Z Brno. Nebudu rozebírat kvalitu dokumentace, která nám byla předána, ale nelze pomlčet o konstrukčním řešení. Jen na okraj, absolutně nevyhovovalo požadavkům sériové výroby. Většina součástí nebyla dle ČSN (byla speciální), tj. vč. spojovacích dílů, nepoužívala se lícovací soustava (i když je Vámi zdůrazňována mechanická náročnost na přesnost - jednalo řádově o mikrony). Taktéž kooperační díly (relé, jejichž kontaktní pérové svazky nebyly pro daný způsob využití vhodné, řešení pérových kontaktních svazků pomocí šroubových pružin, (což bylo hlavním předmětem patentů p. Webera), dělaly stroj zcela nepoužitelný a nespolehlivý, dále to byly spínače atd.). Vše bylo buď upravované, nebo specielně vyrobené jako miniatury, které nedodržovaly předepsané vzdálenosti atd. Znamená to, že bylo nutné vše znovu konstrukčně znovu řešit.

Předností tohoto dps stroje byly zejména ***malé rozměry, výměnnost jednotlivých částí a tím i snadná opravitelnost, malá hlučnost a pro voj. účely otřesuvzdornost.***
To všechno bylo v podstatě pravda, ale jen částečně. Bylo zřejmé, že stroj řešili pracovníci, kteří neměli prakticky žádné výrobní zkušenosti, bez znalostí techn.norem, takže stroj byl pro sériovou výrobu prakticky nevhodný.

Uvádíte, že: „Duševním otcem tohoto zařízení byl Ing. Weber. Jeho nástup do "Z" Brno je obestřen tajemstvím“. Tak tedy pan Weber neměl žádného bratra, ale byl to bývalý zaměstnanec firmy Lorenz A.G. Řešení dps na ektromechanickém principu bylo zahájeno v Berlíně firmou Lorenz AG. Ještě v době 2. světové války. Nálety na Berlín vyvolaly nutnost přemístit tehdejší vývojové středisko Lorenz do klidnější oblasti a to do bývalé továrny v Opočínku v Čechách. Členem tohoto vývojového útvaru byl i p. Karl Weber. Po konci války se toto středisko stalo válečnou kořistí sovětské armády a ještě nějaký čas po válce pracovalo. Pokud je známo většina německých pracovníků tohoto střediska odmítla pracovat v ČSR a jedině p. Weber přešel do VÚ HK, kde byla vytvořena vývojová skupina tohoto dps, řešení elektrické části vedl Ing. Váňa a mechanickou část p. Švec. P. Weber jako jediný znal historii řešení u firmy Lorenz AG. i když se sám na něm plně nepodílel. Měl ale schopnost mlžení a prodeje znalostí ze skupiny Lorenz a tím si získal mýtus nepřekonatelného odborníka. Nebyl tedy hloupý, ale naopak rychle pochopil možnost získání peněz, čímž se nikdy netajil. Každý konstrukční detail si nechával patentovat ve VÚ a později tím získal na tehdejší dobu nevídané částky peněz. Podle toho jak se účastnil prací v „Z“ Brno, a faktu, že za jeho působení v Brně již do řešení nic nového nepřinesl, je možné říci, že u firmy Lorenz nebyl jediným původcem základního řešení stroje. To nicméně nevadilo tehdejším pracovníkům vojenské správy ve velmi rafinované propagandě o převratném světovém řešení, že získali svolení vzorek stroje vystavovat na MSV Brno, získat příslušné orgány k tomu, aby uložili tehdejšímu Ministerstvu všeobecného strojírenství, aby zabezpečilo jeho sériovou výrobu. Protože šlo o zařízení pro vojenské účely, bylo nasnadě, že výrobcem byla určena Zbrojovka Brno, jakožto výrobce psacích strojů a vojenské techniky. Začalo to v r. 1957.

Přesto, že řešení stroje bylo ve vojenském útvaru, nebyly vypracovány žádné zadávací podklady zejména, co se týká klimatické a mechanické odolnosti, spolehlivosti a dalších parametrů důležitých pro využití v armádě. Tomu pak odpovídalo i konstrukční řešení. Tehdejší řešitelé byli rádi, že vůbec jakž takž fungoval v laboratorních podmínkách. V okamžiku, kdy byl program předán do Zbrojovky Brno, se příslušné vojenské orgány probudily a začaly vymýšlet ZTP (základní technické požadavky). Jak to bývá, aby měli původní tvůrci krytá záda, vymysleli ZTP takové, že byly prakticky nesplnitelné a vzorky vyrobené v HK se jim ani vzdáleně nepodobaly. Jen tak pro ilustraci: požadovala se možnost psaní na stroji při – 20st.C. Nikomu přitom nevadilo, že při takovém chladu se bez rukavic psát nedalo a s rukavicemi pak pochopitelně také ne, protože jednotlivá tlačítka byla blízko sebe. To už nemluvím o klimatické odolnosti nakupovaných součástek, např. relé, Ge diody atd. Přitom byl stanoven náběh výroby za rok. Ve Z. Brno byl sice poměrně v krátkém čase stroj částečně konstrukčně přepracován, ale základní neduhy, dané principem řešení, odstraněny nebyly a ani nemohly být, a tak kontrolní vojskové zkoušky, povedené dle dodatečně vypracovaných ZTP, dopadly podle toho. Byl z toho náramný poprask, vyhrožovalo se Stb, byl odvolán ředitel podniku a nahradil jej bývalý velitel voj. útvaru, pod který spadala vývojová skupina Dalibora ve VÚ HK.

Není nutné pokračovat v nářku nad tím, co bylo. Konstrukční skupina se ve Zbrojovce rozrostla, získala i těžce zaplacené zkušenosti a po stránce technické, tak i organizační a po dnes i neuvěřitelných peripetiích se podařilo do r. 1959 dps 302 do sériové výrony. P Weber se

těchto prací již prakticky neúčastnil a,jak jsem již uvedl, při dosažení důchodového věku odešel do penze.

Jako tlumočník a konstruktér jsem byl přítomen setkání s býv. plk. Dyutkinem, který p. Webera v r. 1945 zatýkal. P. Dyutkin byl již v té době ředitelem ruského výrobního závodu produkujícího ruský dálnopis. Bylo to téměř 13 let potom, co se pan W dostal do rukou Rusů. V prvním momentu se p.W lekl, že si pro něho znova přišli Rusi. Dyutkin ho okamžitě poznal a s úsměvem ho pozdravil. Rusi asi rychle zjistili, že to není žádný "lumen" a proto ho "uvolnili“ v náš prospěch. Jen pro objasnění p. W byl průmyslovák, tedy ne Dipl Ing. Byl to typický nácek, který se nikdy nepokusil mluvit česky, a my jsme pro něho byli podřadná rasa. Když jsem s ním jednou mluvil o jeho vztahu k nám a našemu jazyku, řekl mi, že my jsme národ jazyků a že to svědčí o naší nízké kulturní úrovni. V Německu mají vše německy a nemusí se jako my učit cizím jazykům. Nepochopil, že pro tvůrčí práci musí znát cizí jazyky ke studiu literatury, komunikaci s techniky, studium patentových spisů atd.

Ve Vašem článku se uvádí, že tento pán navrhoval typ D 305, tj. šifrák ŠD-3. O řešení tohoto typu kryptografického stroje v dané době neměl potuchy. Dps 302 Dalibor doplněný o děrnopáskový vysílač 322 a děrovač 323 se k tomu přímo nabízel. Toho se již p.Weber nezúčastnil, protože byl v důchodu a toto řešení bylo předmětem utajení. Mohu Vás ujistit, že se k tomu se nedostal, protože jak sám v dalším článku uvádíte, řešili ho pracovníci MV. Na jeho vývoji jsem se podílel a to co probíhalo u nás, bylo v konspiračních podmínkách, tzn., že jsme jako spolupracovníci měli každý svoji kancelář na klíč a mohli jsme spolu setkávat pouze mimo své kanceláře.

Já jsem se s tímto kompletním zařízením setkal pouze jednou na velvyslanectví v Moskvě, když šifrér měl problémy s T100. Požádal mne jako představitele výrobního podniku, který v SSSR řídil budování servisu, v noci při službě na velvyslanectví, abych mu pomohl opravit T100. Když jsem uviděl špatně zakrytou D 305, zeptal jsem se ho jak s ní je spokojený. Velice ho to zarazilo, protože tam kromě velvyslance a jeho samotného na šifru neměl nikdo přístup. Vysvětlil jsem mu, že pro to dodáváme hlavní díly. Potom se přiznal, že mu to také dělá problémy. Seřídil jsem přijímač a on mne prosil, abych se o tom nikomu nezmiňoval.

Pokud jde o Dalibora, zúčastnil jsem se za podnik všech vývojově výrobních zkoušek, ověřování dílčích skupin v mezních klimatických podmínkách (při -50st.C, otřesech a dlouhodobých zkoušek pro stanovení životnosti vč. vojskových a pro poštovní komunikaci, rušení atd. ve VÚS (spojovacím).

Tolik jsem považoval za nutné doplnit Váš článek. Navíc uvádím, že v době, když jsem nastupoval do Z Brno, to byl typický strojírenský podnik, a co se nedalo změřit "šuplerou", to prostě vzbuzovalo nedůvěru. Já jsem absolvoval elektrotechnickou (spojovací) fakultu na VTA a díky ing. Vašicovi, který je též elektrotechnik, vedl výzkumně vývojové středisko, nejen po stránce elektrotechnické, ale i mechanické. Měl jsem u něho podporu a díky jemu jsem se poměrně rychle zorientoval hlavně v problematice strojírenské sériové výroby. V Z Brno byla tradice, jako první na světě zavedla lícovací soustavu do výroby zbraní a tím došlo k jejich radikálnímu snížení ceny. Totéž se pozitivně projevilo i při výrobě dps. Tento podnik mi dal solidní základy pro další práci.

B. Podzimní *Soutěž v luštění 2010* začíná

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

Úvodní informace k soutěži

Vážení čtenáři, **18. 9. 2010** bude zahájena tradiční **podzimní soutěž v luštění jednoduchých šifrových textů o ceny – *Soutěž v luštění 2010***. Pro nově registrované čtenáře uvádím, že obdobné soutěže pořádal náš e-zin již od roku 2000 a doporučuji se s minulými příklady a jejich řešením seznámit (http://crypto-world.info/souteze.php).

Letošní doprovodný příběh k soutěži je inspirován životními osudy známého dobrodruha a svůdníka Giacoma Casanovy (1725-1798).
Postava Giacoma Casanovy se velmi hodí pro náš příběh. Nebyl totiž jen známý svůdce, ale byl také členem lóže Svobodných zednářů, špión a diplomat. S šiframi se ve svém životě tedy skutečně běžně setkával a zabýval.

Pravidla Soutěže 2010

Soutěž začíná 17. 9. 2010 rozesláním e-mailu s výzvou k soutěži všem odběratelům e-zinu Crypto-World a končí vyluštěním všech zveřejněných úloh případně vypršením termínu na vyluštění všech úloh (přesný den bude uveden dodatečně).

Zúčastnit soutěže se může pouze odběratel e-zinu Crypto-World. Vstup na stránku soutěže je přes domovskou stránku Crypto-Worldu - ikona **Soutěže** nebo přímým voláním soutěžní stránky (http://soutez2010.crypto-world.info/).

Při registraci na stránce soutěže musí řešitel zadat do formuláře *Kód soutěže 2010*, který mu byl zaslán společně s kódy pro stažení e-zinu Crypto-World 10/2010 (*Kód soutěže 2010* bude zaslán i všem nově registrovaným odběratelům e-zinu Crypto-World, kteří se během soutěže k jeho odběru přihlásí).

Soutěžící při registraci zadá své uživatelské jméno (login) a autentizační heslo pro opětovné přihlášení a dále e-mail, na který mu je zasílán e-zin Crypto-World. Tento e-mail se dále na stránce nezobrazuje a je pro ostatní návštěvníky soutěže nedostupný. Slouží k odesílání pokynů a informací soutěžícím a k ověření, že uživatel je registrovaným odběratelem e-zinu.

Soutěžní úlohy budou letos zpřístupněny po nepravidelných etapách. K některým úlohám budou zveřejněny dodatečné nápovědy, které umožní jejich vyluštění resp. jejich dešifraci. Nápovědy budou zveřejňovány v sekci Crypto-NEWS. Za vyřešení úlohy se připisují soutěžícímu body. Registrovaný řešitel zadává své odpovědi přes www rozhraní (vždy velkými písmeny)!

Informace o zveřejnění dalších úloh bude vždy dostupná minimálně jeden den předem na stránce soutěže v sekci *aktuality*.

Řešitel zadává "klíčové" slovo z vyluštěného textu, pomoc s výběrem klíčového slova bude uvedena v nápovědě, která bude zveřejněna v Crypto-NEWS. Odpověď bude automaticky vyhodnocena a řešitel se ihned dozví, zda odpověděl správně nebo ne.

Příklad vyhledání a zadání klíčového slova z úlohy:
Řešitel vyluští zadanou úlohu a získá např. tento otevřený text:
KDE ZACNOU PALIT KNIHY TAM NAKONEC BUDOU LIDI UPALOVAT XX
(Kde začnou pálit knihy, tam nakonec budou lidi upalovat.)

Klíčovým slovem, kterým řešitel prokáže, že úlohu vyřešil, je vždy jedno ze slov otevřeného textu. Aby luštitel nemusel zkoušet všechna slova, slouží k jeho určení vždy nějaká jednoduchá nápověda (zveřejněná v NEWS).
Pokud bude v nápovědě např. uvedeno *CO ?* je klíčové slovo odpověď na tuto otázku dle kontextu úlohy. V tomto případě slovo KNIHY.
Pokud bude uvedeno *(4),* je klíčové slovo KNIHY, neboť je čtvrtým slovem získaného textu.
Pokud bude v nápovědě uvedeno *K2*, je klíčové slovo druhým slovem textu, které začíná na písmeno K. Klíčovým slovem je tedy opět slovo KNIHY atd.

Na stránce soutěže bude zveřejňován aktuální průběh soutěže. U každého řešitele bude v celkovém žebříčku uveden počet dosažených bodů a lze se podívat i na pořadí úloh, ve kterém je soutěžící vyřešil. O pořadí soutěžících rozhoduje celkový počet dosažených bodů, v případě rovnosti bodů je rozhodující, kdo dosáhl tohoto počtu bodů dříve! V případě, že soutěžící ještě nezískali žádné body, jsou uvedeni podle pořadí registrace.

Pro určení celkového pořadí je rozhodující stav **v době oficiálního ukončení soutěže**. První tři řešitelé získají cenu automaticky. Další tři ceny se vylosují mezi řešitele, kteří dosáhnou alespoň patnáct bodů.

Ceny

1. cena

a) Pro vítěze celé soutěže je připravena tradiční **hlavní cena** - bezplatná účast na mezinárodním kryptologickém workshopu Mikulášská kryptobesídka (MKB, http://mkb.buslab.org/), který se koná 2.- 3. prosince v Praze. Cenu věnují pořadatelelé MKB - Trusted Network Solutions (http://www.kernun.cz/) a BUSLab (http://www.buslab.org/).

b) kniha - Justin Seitz: Python - Pro hackery a reverzní inženýrství, Zoner Press 2009 http://www.zonerpress.cz/kniha/pro-programatory/python-pro-hackery-a-reverzni-inzenyrstvi věnuje nakladatelství Zoner Press http://www.zonerpress.cz/

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

2. cena

a) kniha - Gus Hansen: Hra za hrou - Strategie pokerového turnaje profesionála, Zoner Press 2010 http://www.zonerpress.cz/kniha/ostatni/hra-za-hrou-strategie-pokeroveho-turnaje-profesionala věnuje nakladatelství Zoner Press http://www.zonerpress.cz/

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

3. cena

a) kniha - Justin Seitz: Python - Pro hackery a reverzní inženýrství, Zoner Press 2009 http://www.zonerpress.cz/kniha/pro-programatory/python-pro-hackery-a-reverzni-inzenyrstvi věnuje nakladatelství Zoner Press http://www.zonerpress.cz/

b) P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, nakladatelství Albatros, 2006, http://crypto-world.info/oko/index.php
věnuje autor

Ceny pro 3 další náhodně vylosované úspěšné řešitele

Tyto tři ceny se losují ze všech řešitelů, kteří splní limit.
Ceny věnuje nakladatelství Zoner Press http://www.zonerpress.cz/:

2x Gus Hansen: Hra za hrou - Strategie pokerového turnaje profesionála, Zoner Press 2010 http://www.zonerpress.cz/kniha/ostatni/hra-za-hrou-strategie-pokeroveho-turnaje-profesionala

1x Justin Seitz: Python - Pro hackery a reverzní inženýrství, Zoner Press 2009 http://www.zonerpress.cz/kniha/pro-programatory/python-pro-hackery-a-reverzni-inzenyrstvi

C. Doprovodný příběh k Soutěži v luštění 2010

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

Následující doprovodné texty jsou sestaveny pro účel této soutěže. Vycházejí z historických událostí a vystupují v něm (většinou) reálné osoby, ale konkrétní skutečnost byla přizpůsobena našemu soutěžnímu vyprávění. Vstupní text je však až na tvrzení, že se Giacomo Casanova znal a dokonce byl přítel svérázného českého léčitele Eleazara Kittela, v souladu s dochovanými dokumenty z jeho života. Také není pravdou, že by chystal ještě jeden životopis, ve kterém chtěl uvést některé ze svých životních příběhů, které ve svých Pamětech vynechal (Příběh mého života - *Histoire de ma vie).*

Giacomo Casanova - Tajnosti mého života (Secrets de ma vie)

Giacomo Casanova opustil Benátky v lednu 1783 a odjel do Vídně. Na nějakou dobu dělal sekretáře benátského velvyslance Foscariniho a potom, po jeho smrti, přijal post knihovníka na zámku Duchcov hraběte Valdštejna v Čechách. Těšil se, že zde bude blízko svého dlouholetého přítele Eleazara Kittela a že si najde čas na jeho návštěvu, ale osud tomu chtěl, že se s ním již nesešel, neboť český lékař a léčitel dr.Kittel právě v tomto roce umírá.
Zde v Čechách strávil Giacomo poslední smutné roky svého života. Zvyklý na ruch velkoměst a dobrodužný život se cítil velmi osaměle a navíc byl nespokojen se svým společenským postavením pouhého služebníka. Také cítil, že jej již opouštějí životní síly a byl si vědom, že jej okolí nechápe a netuší, jaký bohatý život prožil.

Není tedy divu, že Casanova sám Duchcov ani tamní lidi moc nemiloval, nerozuměli mu a on jim, zlobil se na služebné. Po chodbách honil kuchaře, který zkazil makarony. Jiný sluha jej zase zesměšňoval nevhodnými nápisy na toaletě apod.

O svém pobytu v Duchcově prohlásil: „Hrabě učinil hloupost, že mě v Duchcově zdržel, ale tu kterou jsem učinil já, když jsem byl ochoten zůstat, byla ještě větší."

Nakonec se mu podařilo najít přátelské a chápající duše v nedalekých Teplicích a to členy rodiny Clary-Aldringen. Pravidelně do jejich společnosti dojížděl a zde také navázal přátelství s princem Charlesem de Ligne, který se později stal jeho prvním životopiscem.
Giacomo nedokázal žít v klidu a tak si našel práci, která jej naplňovala a dávala jeho životu nový smysl. Rozhodl se psát. Zvolil si téma, ve kterém se rozhodl prozradit něco málo z tajností, se kterými se během svého bohatého života setkal. Využil informace, které získal po svém zasvěcení v lóži Svobodných zednářů. Informace o možných budoucích vynálezech zkombinoval se starou antickou bájí o Hyperborejcích a zde uvedeným výkladem severských bílých nocí. Věřil, že píše dílo, díky němuž se stane nesmrtelný.

Výsledkem byl mnohasvazkový velmi pozoruhodný román Icosameron (Historie Eduarda a Alžběty, kteří strávili jednaosmdesát let u Megamikrů, původních obyvatel Protokosmu v nitru naší zeměkoule). Hlavním tématem románu je cesta do hlubin země, kde svítí věčné slunce, které nikdy nezapadá. K cestě do hlubin země využil Casanova legendární vodní vír Malström u břehů Norska. Do hlubin země cestovali jeho hrdinové v olověné bedně. Za zajímavost stojí, že jako zásoby tekutin si hrdinové s sebou vzali šest lahví vody a šest lahví pálenky. Casanova fantazií předběhl notně svoji dobu - popisuje zde např. stroj na výrobu elektřiny třením a dále zařízení, které bychom dnes nazvali telegraf, automobil, televize nebo letadlo. Jako příznivec alchymie nezapomněl ani na otravný plyn…

Kniha se stala jedním z prvních utopických (chcete-li - sci-fi) románů, které vůbec kdy byly napsány. Vydal ji vlastním nákladem v létě 1787.
Jeho očekávání, že mu přinese slávu, se nenaplnilo. Román zůstal nepochopen a stal se literárním propadákem. Objednalo si ho jen 136 předplatitelů a část nákladu zůstala v zámecké knihovně, kde je dosud uložena. Ocitl se proto v dluzích, ale pomohl mu hrabě Valdštejn, který je za něj vyrovnal

Zahořkl a již se nechtěl psaní dále věnovat. Teplická společnost, kam stále pravidelně zajížděl, jej však přesvědčila, že jeho rozhodnutí není správné. Vždyť přece tak nádherně a poutavě vypráví své vzpomínky. Ty by měl sepsat!
Giacomo uposlechl. Nejprve sepsal zprávu o útěku z olověných komor benátských. Ta byla bezesporu literárním úspěchem a byla velmi dobře přijata. To jej povzbudilo a vrhl se ze všech sil do sepisování svých Pamětí *(Příběh mého života / Histoire de ma vie)*. Autobiografie pohltila všechny jeho zbývající síly, neboť ji psal ve vytrvalém zanícení, téměř jako by chtěl předejít smrt, kterou už cítil přicházet. Rozhodl se ji sepsat ve francouzštině, aby byla dostupná pro větší počet čtenářů.

Když ji psal, znovu prožíval svůj život, tak naprosto jedinečný, že se stal skutečným mýtem. Svůj život pak zobrazil jako umělecké dílo. Jistě si při jejím vypravování uvědomoval, kolik toho v životě zažil. Psal velmi otevřeně. Je vidět, že jeho dílo je rekapitulace života a jeho rozloučení se s ním. Nic netají a nezamlčuje. Píše i o svých selháních. Snad jen tu a tam, aby neuškodil ještě žijícím přátelům nebo dámám, se kterými měl více než přátelský vztah, vynechává jméno, či příběh drobně upraví. Celkově se však má za to, že kniha pravdivě, podrobně a místy velmi krásným uměleckým a kultivovaným jazykem popisuje jeho osudy a příběhy. Je pravda, že se zaměřil spíše na příběhy lehce skandálního charakteru, ale i to možná byl jeho úmysl, neboť chtěl knihou čtenáře zaujmout.

Splnilo se mu jeho přání. Kniha mu přinesla skutečnou nesmrtelnost a díky ní zůstává jeho jméno a jeho příběhy součástí kolektivního vědomí evropské vzdělanosti.
Ale opravdu nic mimo jmen některých urozených milenek nezatajil a nevynechal? Giacomo při psaní přece jen své vzpomínky cenzuroval, a tak některé detaily z jeho bohatého a pestrého života se zde jen naznačují a nejsou, i přes jistě velkou zajímavost, rozvíjeny nebo popsány jen stručně bez souvislostí. Giacomo se vyhýbá především tématu špionáže a vše co s tím souvisí. Přitom je Giacomo uváděn mezi deseti nejznámějšími špióny. (http://listverse.com/2007/08/24/top-10-famous-spies/). Uchovává také tajemství Zednářské lóže. Nezmiňuje se, jak a kde se naučil luštit tehdy oblíbenou periodickou šifru, znalost v luštění systému prokázal, když jeden z takto zašifrovaných textů pro markýzu d´Ufré vyluštil. O této příhodě se sice zmiňuje, ale to podstatné, jak to provedl, vynechává. V knize se také neobjevilo jméno jeho přítele, českého léčitele Josefa Antonína Eleazara Kittela. Během svého života se s ním několikrát setkal, ale ani o jednom setkání z různých důvodů nevypráví.

Jak knihu psal, uvědomoval si, že třeba již nebude mít jinou příležitost tyto své vynechané příhody zveřejnit. Také se stávalo, že příběh nejprve do svých pamětí vložil a pak se rozhodl, že to přece jen v této knize není vhodné zveřejnit a již napsané listy z rukopisu vyjmul. Takto vyjmuté listy ukládal do jednoho z dřevěných šuplíků slonovinou vykládané komody, která stála těsně vedle jeho oblíbeného křesla, které se dodnes dochovalo a lze si je v Duchcově prohlédnout. Do tohoto šuplíku časem přidal i různé související dochované dopisy a listiny, které si během života na památku schovával. Časem, když již v šuplíku byla docela slušná hromádka textů, začal zvažovat, zda je přece jen neuspořádá do souhrnného dílka, které by doplňovalo jeho Paměti a které by popisovalo jeho utajovanou stránku života. Dokonce si již

pro tuto knihu vymyslel jméno *Tajnosti mého života (Secrets de ma vie).* Tedy název, který na jeho Paměti (*Příběh mého života / Histoire de ma vie)* jasně odkazuje a současně naznačuje o jaká témata tuto knihu rozšiřuje.

Další útěchou v jeho smutném životě na zámku v Duchcově byla také velmi rozsáhlá korespondence s benátskými přáteli, kteří ho zpravovali o dění v jeho rodném městě. A také korespondence s francouzskými přáteli a dalšími zednáři, ve které napomáhal Francouzské revoluci a k pádu Benátské republiky.

Mimo korespondence s touto elitou udržoval čilý písemný styk s Francescou Buschiniovou. Francesca byla prostá dívka, která mu po jeho druhém vyhoštění z Benátek celá léta psala dopisy s dojemnou upřímností a něhou. Toto byl poslední významný vztah G. Casanovy, tedy až na jeho drobnou, ač mediálně mnohem známější, aféru s dcerou zámeckého duchcovského klíčníka. Giacomo k Francesce velmi přilnul a udržoval s ní hustou korespondenci a stále na ni vzpomínal a to navzdory tomu, že od sebe byli nepřekonatelně daleko a on již byl hluboce smuten z temnoty svého života a blížícího se konce.

Giacomo Casanova zemřel ve svém milovaném křesle 4. června roku 1798.

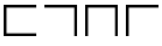
Úkoly z šuplíku – Kittlův dopis

Když se Giacomo Casanova rozhodoval, zda knihu *Tajnosti mého života* napsat nebo ne, tak zpravidla otevřel šuplík s uloženými podklady a materiály a probíral se v něm. To oživovalo jeho bohaté vzpomínky a on často pak strávil s vyjmutým dokumentem ve svém křesle celé hodiny a vzpomínal a vzpomínal. Často se rozhodoval, zda přece jen ještě nemá zařadit do svých oficiálních pamětí resp. co všechno má k této události do svých pamětí zařadit, a co ponechat do této knihy.

Tento večer vyndal dopis od svého přítele Eleazara Kittela. S tímto svérázným mužem, kterého místní pověrčivý lid nazýval *černokněžníkem ze Šumburku,* se seznámil, když se vracel koncem května roku 1766 zraněn přes Čechy z Polska po souboji s hrabětem Františkem Xawerem Branickim. Tento nesmírně nadaný ranhojič nejen, že jej velmi rychle vyléčil, ale navíc našli oba dva v sobě zalíbení. Giacomo během dlouhých večerů, které spolu trávili, mu vyprávěl o svém bouřlivém životě a o některých tajnostech Zednářského řádu. Kittel mu zase ukázal starodávnou čarodějnou knihu, kterou vlastnil a která obsahovala různá zaříkávání a byl zde i návod jak létat na plášti. Oba dva se zajímali o alchymii, a tak trávili večery i diskuzemi na téma elixíru mládí a výroby zlata. Kittel se také velmi zajímal o šifrování. Na toto téma se dostali, když mu Giacomo popisoval, jak probíhalo jeho zasvěcení v Zednářském řádu.
Oba dva si opravdu vzácně rozuměli, a když Giacomo z Šumburku odjížděl, bylo mu jasné, že našel opravdového a vzácného přítele. Ještě se spolu několikráte setkali. Rád například vzpomínal na setkání v roce 1777, kdy pořádal Kittel v Šumburku velikou oslavu své zlaté svatby. O svatbě, které se zúčastnilo mnoho význačných hostů a to včetně šlechty, se ještě dlouho mluvilo. Takový lesk měla svatba i díky Giacomovi, který sem nejen sám z Benátek přijel, ale pozval na ni se svolením Kittela i několik svých přátel z šlechtických kruhů. Kittel byl takovým zájmem velmi potěšen a společně s manželkou na tuto skvělou oslavu dlouho a s vděčností vzpomínali.
Dopis, který Giacomo držel v ruce, mu poslal Kittel dva roky po této události. Dopis se vztahoval k jiné pro Kittela velmi významné události a napsal jej v noci 15.9.1979. Pokusil se jej napsat zašifrovaně, ale protože neměl s Giacomem domluven žádný nomenklátor nebo jiný

vhodný šifrový systém, použil velmi jednoduchou šifru. Věděl, že dopis bez problémů Giacomo vyluští i to bez toho, že by mu poslal klíč nebo nějakou jinou nápovědu.
Giacomo se díval na tento zvláštní dopis a zavzpomínal si, jak jej luštil. Byl obsahem tehdy velmi potěšen a to hned dvakrát. Poprvé proto, že pro přítele mohl něco zařídit a jednak, že jeho přítel to ocenil a hned mu napsal a zaslal tento dopis. To, že k tomu použil takovou jednoduchou a naivní šifru, také ocenil. Bylo mu jasné, že jeho přítel mu tím chtěl udělat radost a takto mu svérázně poděkovat.

Úkoly z šuplíku – Lóže Svobodných zednářů

Díky vlivným známým mé přítelkyně Adelaide de Gueidan a na její opakovanou přímluvu se mi splnilo mé přání a byl jsem přijat roku 1750 do Lóže Svobodných zednářů v Lyonu. O vstup jsem měl velký zájem nejen proto, že mne k tomu lákala má romantická povaha, ale také jsem doufal, že kontakty, které zde získám, budou pro moji kariéru a další život velmi důležité a potřebné.
Krátce po mém přijetí mne začal zasvěcovat do tajů této Lóže její bratranec hrabě Henri Gaspard de Gueidan, který byl jejím významným členem. Když mi začal předávat tajemství utajování psaných textů Lóže, byl jsem překvapen, jaké jednoduché prostředky se zde k tomu používaly. Byl to především neviditelný inkoust a jakási podivná grafická abeceda (). Od svého chráněnce Matteo Bragadiniho, který se v Benátkách svého času zabýval uspořádáním archívu Benátské republiky a díky tomu se dostával do styku s šifrovými texty, jsem věděl, že jednoduchá záměna je velmi lehce luštitelná a nic na tom nemění, když se použije nějaká neznámá, exotická nebo zcela vymyšlená grafická abeceda. Od něj jsem také věděl, že za nejbezpečnější se považuje periodická šifra deVigenére.
Když jsem to Henrimu sdělil, usmál se a řekl: „Giacomo, zapomínáš, že je to jen první stupeň zasvěcení. Je to jen jakýsi úvod do používaných šifrových systémů. Používáme i jiné, složitější systémy, ale o nich se nesmí dozvědět nejen lidé mimo naše společenství, ale ani lidé s nižším zasvěcením."
Byl jsem velmi zvědavý a k tomuto tématu jsem se stále vracel. Henri mne stále odbýval s tím, abych počkal, až postoupím v zasvěcení do dalšího stupně, ale nakonec jsem jej za použití dvou láhví vynikajícího koňaku přemluvil a on prozradil více, než asi původně chtěl.
Tak jsem se dozvěděl, že periodickou šifru nepoužívají z důvodu, že jedno z tajemství Lóže je, že se dá luštit. Dokonce mi tento postup ukázal. Byl jsem překvapen, jak je tento postup v případě, že se použijí srovnané abecedy a nepříliš dlouhé heslo, jednoduchý. Teprve na dalším setkání a po dalších dvou lahvích koňaku, který Henri tolik miloval, jsem se dozvěděl, jakou šifru Lóže používá. Vychází ze všeobecně zednáři používaného grafického písma, které je jako jednoduchá záměna samozřejmě slabým systémem. Jenže oni jeho použití vylepšili. Nejprve text přepíši do této grafické úpravy a pak podle dohodnutého klíče provedou otočení jednotlivých grafických znaků o úhly, které jsou dány tímto klíčem. Otáčení se provádí vždy o násobky 90 stupňů. Nezasvěcenec pak při luštění textu jako jednoduché záměny neuspěje a to hned z několika důvodů. Jednak se může stát, že vlivem otáčení je pak znaků šifrové abecedy ve výstupním textu více než má skutečně použitá grafická šifrová abeceda k dispozici a navíc se může stát, že vlivem otáčení se znak otevřeného textu zobrazí po otočení jako jiný znak otevřeného textu, který však otočen nebyl.
Příklad: A=  M=  O= R=  , Klíč: 1 0 0 2 (tj. otočit znaky o 90^o, 0^o, 0^o, 180^o)
Výsledek:  . Sám jsem se přesvědčil o pár měsíců později, že luštit text takto zašifrovaný není nijak jendoduché. Ovšem se znalostí luštění periodické šifry jsem to nakonec také dokázal.

D. Giacomo Casanova - *Příběh mého života (Histoire de ma vie)*

(2. dubna 1725, Benátky – 4. června 1798, Duchcov)

- Jméno článku: Casanova
- Autor: Přispěvatelé Wikipedie
- Vydavatel: *Wikipedie: Otevřená encyklopedie*.
- Datum poslední úpravy: 15. 02. 2010, 02:46 UTC
- Datum převzetí: 12. 08. 2010, 04:03 UTC
- Trvalý odkaz: http://cs.wikipedia.org/w/index.php?title=Casanova&oldid=4962671
- Hlavní autoři: Statistika editací stránky
- Identifikace verze stránky: 4962671 ,
- Pro účely této citace odstraněny některé překlepy a pravopisné chyby, které jsou v uvedené verzi a provedeno zalomení do tohoto formátu (12.8.2010, Vondruška, P.)

Giacomo Casanova se narodil v Benátkách v ulici Calle della Commedia (dnes Calle Malipiero). Jeho otcem byl Gaetano Casanova a matkou Zanetta Farussi, některé zdroje ho ale považují za nemanželského syna matky se šlechticem Michele Grimanim. Rodiče byli herci. Malý Giacomo, vychovávaný babičkou Marziou Farussiovou, byl křehkého zdraví. Proto ho babička jednoho dne odvedla k čarodějnici a té se podařilo vyléčit jeho potíže. Po tomto dětském zážitku, ho zájem o magické praktiky provázel po celý zbytek života, ale on sám byl prvním, kdo se vysmíval důvěřivosti, s níž mnozí přijímali esoterismus. Studoval na padovské univerzitě, kde vystudoval právo v roce 1742. Následně cestoval na ostrov Korfu a do Istanbulu.

V roce 1743 se vrátil do Benátek. Od konce března do konce července byl uvězněn. Spíše než o výkon trestu, se jednalo o výstrahu s úmyslem snahy o nápravu bouřlivého charakteru. Když se dostal na svobodu, odcestoval díky matčiným dobrým vztahům jako doprovod biskupa, který měl převzít diecézi, do města Martirano v Kalábrii. V roce 1744 odcestoval do Říma, kde vstoupil do služeb kardinála Acquavivy, španělského velvyslance při Svatém stolci. Pro nevhodné chování musel brzy ze služby odejít.

Vrátil se tedy do Benátek a na jistou dobu se živil hrou na housle v divadle San Samuele. Roku 1746 zachránil Casanova život Benátčanu Matteo Bragadinimu. Ten jej pak považoval téměř za syna a poskytoval mu podporu na výživu, dokud byl naživu. Ovšem styky se šlechtou přitahovaly pozornost státních úřadů a Casanova na doporučení Bragadina opustil Benátky v očekávání lepších časů.

Roku 1749 potkal jistou Henriette, která se stala zřejmě největší láskou jeho života. Pseudonym skrýval identitu jedné vznešené dámy z Aix-en-Provence Adelaide de Gueidan (1725-1786).

V červnu roku 1750 v Lyonu Casanova vstoupil do lóže Svobodných zednářů. Vstup byl motivován pragmatickým přáním získat užitečné kontakty. To pak využil během svého

života. Získal tak kontakty a některé získané výhody při různých příležitostech se zdají být dílem přínosu pocházejícího z členství v organizaci dobře zakořeněné v téměř všech evropských zemích. V téže době se odebral do Paříže, kde se naučil plně Francouzky.

Když se vrátil se do Benátek po svém dlouhém pařížském pobytu a dalších cestách do Drážďan, Prahy a Vídně, byl v noci z 25. na 26. června 1755 zatčen a uvězněn v Piombi (vězení Dóžecího paláce). Jak bylo tehdy obvyklé, nebyl odsouzenému sdělen důvod obžaloby ani doba trvání zadržení. To, jak později napsal, se ukázalo jako škodlivé, neboť kdyby býval věděl, že trest měl trvání celkového možného součtu, byl by se vystříhal smrtelného nebezpečí při pokusu o útěk, ale především nebezpečí z možného následného omezení ze strany vyšetřovatelů, kteří nezřídka operovali daleko za hranicemi Republiky. Tito soudní úředníci byli nejzřetelnějším ztělesněním svévolné moci oligarchie, která vládla Benátkám. Byly zároveň zvláštní soudním aparátem a špionážní centrálou.

O skutečném důvodu zatčení se stále diskutuje. Jisté však je, že Casanovovo chování vedli v patrnosti agenti a ti zanechali *riferty* (raporty špiónů na účet policejního úřadu), které podrobně popisovaly jeho chování, především ty, které byly považovány za společensky nevhodné. V žalobě nakonec zněla: "zhýralost" spáchaná na vdaných ženách, zneuctění církve, oklamání několika urozených pánů a za obecně nebezpečné chování pro dobré jméno a stabilitu aristokratického režimu. Casanova nevedl o mnoho jiný život než mnoho mužů z „dobrých rodin“, jen se tím nijak netajil.

Také jeho přijetí do zednářského spolku, jež bylo úřadům známo, mu příliš neprospívalo, jako například skandální vztah s „sestrou M. M.“, zcela jistě patřící k urozeným, jeptiškou kláštera Sv. Marie od Andělů v Muranu a milenkou francouzského velvyslance opata De Bernis. Oligarchie u moci nemohla tolerovat nic jako zatčenou sociálně nebezpečnou osobu, která je na svobodě.

Nicméně pomoc, jíž mohl využívat ze strany svých aristokratických známých, mu značně pomáhala, ať už v podobě zmírnění trestu, či lepšího zacházení během pobytu v káznici, a dost možná mu i napomohli k útěku. Casanova byl vždy dvoustranná osobnost: svým předurčením a prostředky patřil mezi poddané, i když s těsnou vazbou na šlechtu, ale díky své protekci a frekvenci vztahů se mohlo zdát, že je nějak začleněn do vládnoucí třídy. Z tohoto pohledu se má za to, že jeho předpokládaný biologický otec, šlechtic Michele Grimani, patřil do jedné z nejvýznamnějších aristokratických rodin v Benátkách, z jejích řad vzešla tři dóžata, jakož i kardinálů. Casanova sám se k tomuto otcovství hlásil v pamfletu *Né amori né donne* (Ani láska, ani ženy) a zdá se, že i podobnost tváře i podoba tělesná obou dvou tuto domněnku nemálo podporovala.

Od útěku z Piombi po návrat do Benátek (1756 - 1774)

Sotva se vzpamatoval ze šoku z uvěznění, začal Casanova připravovat útěk. První pokus byl zmařen přemístěním do jiné cely, avšak v noci z 31. října na 1. listopad 1756, uskutečnil svůj plán: protáhl se skrz celu v podkroví, přes otvor ve zdi vytvořený spoluvězněm, fráterem jménem Marino Balbi, odtud vnikl na střechu a úspěšně se spustil vikýřem zpátky do interiéru paláce. Dostal se tak, v doprovodu komplice, přes několik místností, kde byl nakonec zpozorován chodcem, který se domníval, že jde o návštěvníka, který zůstal zamčený uvnitř. Chodec pak zavolal jednoho ze zaměstnanců paláce, jenž otevřel vrata a dal oběma vězňům souhlas k opuštění paláce a bleskovému odjezdu na gondole.

Rychle se nasměrovali k severu. Problém však byl, že útěk vrhal špatné světlo na benátské justiční orgány a bylo jasné, že se úřady budou všemožně snažit o znovudopadení uprchlíků. Po nedlouhých pobytech v Bolzanu, Mnichově, kde se Casanovovi konečně podařilo zbavit se nepohodlného doprovodu mnicha, dále v Augustě a Štrasburku, 5. ledna 1757 dorazil do Paříže, kde se mezitím jeho De Bernis stal ministrem a tudíž neměl potíže s ochranou a podporou.

Povzbuzen, poté co získal pevnou půdu pod nohama, začal se věnovat své specialitě: zářit ve společnosti, při svých návštěvách pokud možno v kruzích, jaké jen mohlo město nabídnout. Seznámil se mimo jiné s markýzou Jeanne d'Urfé (1705-1775), velmi bohatou a extravagantní šlechtičnou, s níž udržoval dlouhý vztah, rozhazuje značné sumy peněz, které mu ochotně poskytovala, zcela okouzlena jeho půvabem a rozsáhlými znalostmi magických rituálů. S ohromnou vynalézavostí, jako vždy, se zhostil úkolu zakladatele národní loterie, za účelem posílit státní finance. Zjistil, že to je jediný způsob, jak přimět občany ochotně odvádět poplatky veřejných financí.

Jeho intuice byla natolik správná, že je tento systém dodnes s úspěchem praktikován. Jeho nápad byl úředně schválen a Casanova byl jmenován Výběrčím 27. ledna 1758. V září téhož roku, byl De Bernis jmenován kardinálem. O měsíc později byl Casanova pověřen francouzskou vládou **vykonáním tajné mise v Holandsku**. Při svém návratu byl zapleten do spletité záležitosti ohledně nechtěného těhotenství jedné benátské přítelkyně jménem Giustiniana Wynne.

Po matce Italka, po otci Angličanka, byla Giustiniana v centru pozornosti díky svému žhavému vztahu s benátským patricijem, Andreou Memmem. Ten se ji snažil všemi způsoby přesvědčit, aby si ho vzala, ale *Raison d'État* (byl členem jedné ze dvanácti – tzv. *apoštolských* rodin – nejvznešenější v Benátkách) mu v tom bránily, z důvodu jakýchsi obskurních poklesků její matky. V důsledku skandálu, který to následně vyvolalo, se Wynneovi odstěhovali z Benátek. Nešťastná dívka, jež se po příjezdu do Paříže nemohla vzpamatovat ze změny a v důsledku oné nepříjemnosti, se obrátila s prosbou o pomoc na Casanovu, jenž byl dobrým přítelem jejího vyvoleného. Znovu se našel dopis, v němž dívka naléhavě prosí o pomoc, a upřímnost, s níž se obrací na Casanovu je odzbrojující, a vkládá naprostou důvěru, vědoma si obrovského nebezpečí, kterému vystavovala sebe (i jeho) v případě, že by se zpráva dostala do špatných rukou.

Casanova se jí snažil pomoci, byl však vystaven udání za osvětu abortivních praktik, prováděnou porodní sestrou, Reine Demay, a v houfu přihlížejících stál krátkozraký člověk jménem Louis Castel-Bajac, jenž žádal výkupné výměnou za zrušení soudního přelíčení. Obvinění bylo závažné, nicméně Casanova se dokázal zprostit svou obvyklou duchapřítomností a byl propuštěn, zatímco žalující skončila ve vězení. Dívka opustila myšlenku na přerušení těhotenství a následně porodila v klášteře, kam se uchýlila. Poté co přenechal své zájmy v loterii jiným, pustil se Casanova do podnikatelské operace v konkurzu (textilním podniku), který zkrachoval také vinou silných omezení exportu vzešlých z válečného konfliktu. Dluhy, které vznikly, ho přivedly na krátko do vězení (srpen 1759). Jako vždy, včasná intervence vlivné přítelkyně, bohaté a mocné markýzy d'Urfé, ho dostala z ožehavé situace. Následující roky byly ve znamení častého cestování po Evropě. Procestoval Holandsko, pak Švýcarsko, kde se setkal s Voltairem. Posléze do Itálie, do Janova, Florencie e Říma.

Zde žil jeho bratr Giovanni, malíř, žák Raffaella Mengse. Během pobytu u bratra byl přijat papežem Klimentem XIII. Roku 1762 se vrátil do Paříže, kde se začal znovu věnovat esoterickým praktikám společně s markýzou d'Urfé, fino a che quest'ultima, která si

uvědomila, že si z ní celou dobu dělal blázny a ona věřila v znovuzrození jako mladá a krásné díky magii, náhle přerušila všechny kontakty se samozvaným čarodějem, tak že po krátkém čase, opustil Paříž, kde klima, které si kdysi vytvořil se mu stalo nesnesitelným, a odcestoval do Londýna, kde byl uveden na královském dvoře.

V anglické metropoli poznal osudnou Marianne de Charpillon, mladičkou francouzskou kurtizánu, s níž nemohl odolat navázat vztah. V této záležitosti i takový ostřílený svůdce jakým byl Casanova, podlehl a ukázal svou slabinu a tato vychytralá dívenka ho přivedla až na pokraj sebevraždy. Nebyla to velká láska, ale evidentně Casanova se nemohl smířit s tím, že ho nějaká holka naprosto bez zájmu přehlíží. A čím víc naléhal, tím víc ho ona vodila za nos. Ale nakonec se mu podařilo se z této absurdní situace osvobodit a odcestoval do Berlína.

Zde se setkal s císařem Bedřichem II. Pruským, jenž mu nabídl skromný post učitele na škole kadetů. Casanova nabídku znechuceně odmítl a zamířil na východ do Ruska. V Moskvě se v prosinci 1764 setkal s carevnou Kateřinou II. Velikou, která byla rovněž spojena s obrovskou sbírkou historických osobností, které potkala během svých nekonečných cest. S mimořádnou jednoduchostí Casanova dosáhl výše postavení na úrovni osobností prvního řádu – lidí, kteří jistě nebyli k mání pro kohokoli. Evidentně ho pravidelně předcházela pověst a, přinejmenším díky vyvolané zvědavosti, se mu dařilo pronikat do exkluzivních společností hlavních měst.

Tato záležitost se tak trochu živila sama, v tom smyslu, že na jakékoli místo, kam se Casanova chystal, dával si dost práce s tím, aby dostal dopisy s doporučením do svého příštího působiště. Evidentně si tam přidával své: uměl brilantně konverzovat, měl encyklopedické vzdělání, které se vymykalo normálu a pokud se týká zkušeností z cest, těch, v časech, kdy lidé zrovna moc necestovali, posbíral nekonečně. Zkrátka Casanova měl své veliké kouzlo a neužíval ho pouze u žen.

Roku 1766 v Polsku se stala příhoda, která Casanovu hluboce poznamenala: souboj s hrabětem Branickim. Ten ji během sporu o čest jedné benátské baleríny Anny Binettiové napadl označením *benátská matrace*. Hrabě byl významná osoba z okruhu krále Stanislava II. Poniatowského a pro soukromou osobu z ciziny bez jakékoli politické ochrany nebylo příliš radno mu odporovat. Takže, i když šlo ze strany hraběte o těžkou urážku, každý rozvážný člověk by se byl raději stáhl. Ne však Casanova, jenž evidentně nebyl jen pouhým milovníkem konverzace a schopný svůdník, ale také kurážný muž, hraběte vyzval na souboj s pistolemi. Podnik to byl velmi riskantní, protože jak v případě porážky, tak i vítězství, se dalo čekat, že se přátelé hraběte okamžitě pomstí.

Hrabě vyvázl s velmi těžkým zraněním, ale ne takovým, aby mu to zabránilo čestně požádat své přátele, aby nechali soupeře jít, neboť jednal podle pravidel souboje. S poměrně vážným zraněním na paži, se Casanovovi podařilo uprchnout z nevlídné země. Šťastná hvězda zdá se teď k němu obrátila zcela zády. Odjel do Vídně, odkud byl vypuzen.

Vrátil se tedy do Paříže, kde ho však zastihl (listopad 1767) královský dokument *lettre de cachet* od Ludvíka XV., v němž jej panovník vyzval k opuštění země. Toto nařízení si vyžádali příbuzní markýzy d'Urfé, kteří měli v úmyslu ochránit od dalších turbulencí ještě stále značný rodinný majetek.

Odjel tudíž do Španělska, již v zoufalé snaze najít nějaké zastání, ale ani zde se mu nedařilo lépe: byl uvržen do žaláře pod falešnou záminkou a celá věc se táhla déle než měsíc. Opustil Španělsko a skončil v Provence, kde těžce onemocněl (leden 1769).

Zde se mu dostalo pomoci od jeho někdejší milenky Henriette, jež se mezitím vdala a poté ovdověla, u které na sebe zanechal nejlepší vzpomínky. Rychle se vzpamatoval a znovu vycestoval, tentokrát do Říma, Neapole, Boloni, Terstu. V tomto období také zintenzívnil své styky s benátskými státními úředníky, aby my byla udělena kýžená milost, která konečně přišla 3. září 1774.

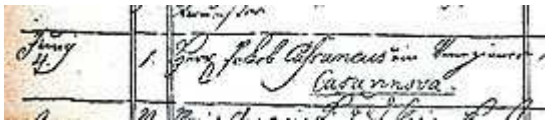
Od návratu do Benátek do smrti (1774 - 1798)

Když se Casanova po osmnácti letech vrátil do Benátek, znovu navázal stará přátelství, koneckonců nikdy nepřerušených díky velice intenzivní korespondenci. Aby mohl žít, nabídl své služby státním úřadům coby špión, vlastně kvůli těm, kteří byli nejprve rozhodnuti odsoudit do žaláře a potom ho donutit k dlouhému exilu. *Hlášení* od Casanovy nebyly nijak zvláště zajímavé a spolupráce se unaveně vlekla až k přerušení z důvodu "slabého přínosu". Pravděpodobně se mu příčilo být původcem pronásledování jiných, které sám dobře znal a zažil na vlastní kůži.

Když se ocitl bez finanční podpory zvenčí, začal se věnovat spisovatelským aktivitám, a při tom používal svou širokou síť známostí, aby zajistil publikaci svého díla. Tehdy se užívalo přepisování originálu knih ještě před předáním k tisku nebo přímo při dokončení díla, aby bylo zajištěno maximální snížení nákladů na tisk. Sazba se totiž prováděla ručně a náklad byl velmi nízký. V roce 1775 publikoval první svazek překladu Iliády. Výčet spolupracovníků, tedy těch, kteří se podíleli na financování díla, byl skutečně pozoruhodný a obsahoval přes dvě stě třicet jmen, mezi nimiž figurovala i ta z benátské horní vrstvy, včetně nejvyšších státních autorit, ať už úřadujících prokurátorů od Sv. Marka, dvou synů dóžete Moceniga, profesorů padovské univerzity a dalších. Zajisté, měl mnoho dobrých známých, díky své vězeňské minulosti a útěku a následnému omilostnění. Skutečnost, že byl někdo uveden na seznamu, nebyla utajovaná, ale na maloměstě, kde se všechny vlivné osobnosti znaly, bylo veřejným tajemstvím, a tudíž veškerá podpora naznačuje, že, navzdory osudu, Casanova zdaleka nebyl vyděděnec. Také zde je vhodné zamyslet se nad dvojakostí jeho osobnosti a jeho věčné oscilaci mezi táborem odpadlíků a vrstvou privilegovaných.

V tomto období Casanova navázal vztah s Francescou Buschiniovou, velmi prostou a nevzdělanou dívkou, která mu po jeho druhém vyhoštění z Benátek léta psala dopisy (nalezené v Duchcově) s dojemnou upřímností a něhou, užívajíc slovník silně ovlivněný benátským nářečím, s viditelnou snahou o co největší poitalštění textu. Toto byl poslední významný vztah G. Casanovy a on k této ženě velmi přilnul: i když od sebe byli nepřekonatelně daleko, a on hluboce smuten z temnoty svého života, udržoval hustou korespondenci s Francescou, a kromě toho jí celé roky nadále platil činži za dům v Barbaria delle Tole, v němž společně žili, a když mohl, posílal jí směnky na nevelké částky peněz.

V následujících letech publikoval další díla a snažil se protloukat, jak nejlépe mohl. Ale jeho bouřlivá povaha mu způsobila velkou nepříjemnost: teatrálně urazil v domě Grimaniho jistého Carlettiho, se kterým se přel ohledně peněz. Ale protože pán domu se přiklonil na stranu Carlettiho, Casanova se urazil. Rozhodl se sepsat jako pomstu pamflet, *Né amori né donne, ovvero la stalla ripulita (Ani láska ani ženy, aneb vyčištěný chlév*, v němž, byť pod chabou snadno odhalitelnou mytologickou zástěrkou, otevřeně tvrdí, že právě on je skutečným synem Michele Grimanijho, zatímco naopak Zuan Carlo Grimani je, „jak všichni vědí", plodem nevěry jeho matky (Pisana Giustinian Lolin) s jiným benátským aristokratem, Sebastiano Giustinianim.



Záznam o úmrtí Casanovy v duchcovských análech

Pravděpodobně to všechno byla pravda, také proto, že ve městě, kde se vzdálenosti mezi domy měřily na pídě, na procházky se jezdilo v gondolách, a kde houfy služebných přirozeně drbaly do úmoru, bylo naprosto nemyslitelné, že by se dalo udržet nějaké tajemství. Tak jako tak, i v tomto případě se místní aristokracie vzepřela a Casanova byl donucen k poslednímu a definitivnímu exilu. Nicméně tato záležitost nezůstala bez odezvy, jestliže se nechal kolovat anonymní pamflet, v němž se opakovala slova z Casanovova textu, nazvaný "*Contrapposto o sia il riffiutto mentito, e vendicato al libercolo intitolato Ne amori ne donne ovvero La stalla ripulita, di Giacomo Casanova*".

Giacomo opustil Benátky v lednu 1783 a odjel do Vídně. Na nějakou dobu dělal sekretáře benátského velvyslance Foscariniho a potom, po jeho smrti, přijal post knihovníka na zámku hraběte Valdštejna Duchcově, v Čechách. Tam strávil poslední a velmi smutné roky svého života, ponížen rolí služebníka a již nepochopen, a navíc považován za přežitek navždy zmizelé epochy.

Z Duchcova, Casanova údajně napomáhal Francouzské revoluci, k pádu Benátské republiky, k pádu jeho světa. Nebo přinejmenším toho světa, o němž snil, že se stane jeho pevnou součástí. Jeho poslední útěchou, kromě velkého množství dopisů od benátských přátel, již ho zpravovali o dění v jeho rodném městě, bylo sepisování díla *Histoire de ma vie*, autobiografie, jež pohltila všechny jeho zbývající síly, neboť ji psal ve vytrvalém zanícení, téměř jako by chtěl předejít smrt, kterou už cítil přicházet.

Když ji psal, Casanova znovu prožíval svůj život, tak naprosto jedinečný že se stal mýtem, v kolektivního vědomí. Život jako umělecké dílo. Jistě si při jejím vypravování uvědomoval, kolik toho v životě zažil a kolika nekonečných zkušeností byl interpretem. Zemřel 4. června roku 1798.

E. Jan Josef Antonín Eleazar Kittel

(3. února 1704, Šumburk – 16. listopadu 1783, Šumburk)

Detaily o článku Jan Josef Antonín Eleazar Kittel

- Jméno článku: Jan Josef Antonín Eleazar Kittel
- Autor: Přispěvatelé Wikipedie
- Vydavatel: *Wikipedie: Otevřená encyklopedie*.
- Datum poslední úpravy: 2. 07. 2010, 15:55 UTC
- Datum převzetí: 12. 08. 2010, 04:19 UTC
- Trvalý odkaz: http://cs.wikipedia.org/w/index.php?title=Jan_Josef_Anton%C3%ADn_Eleazar_Kittel&oldid=5532224
- Hlavní autoři: Statistika editací stránky
- Identifikace verze stránky: 5532224

Jan Josef Antonín Eleazar Kittel, německy **Johann Josef Antonius Eleazar Kittel** (3. února 1704, Šumburk (dnes Krásná, část obce Pěnčín) - 16. listopadu 1783 tamtéž) byl český lékař a léčitel. Jeho postava je opředena mýty a pověstmi. Byl nazýván také *Severočeský Faust*, *Faust Jizerských hor*, či *Černokněžník ze Šumburku*.

Život

Narodil se a zemřel v Šumburku, dnešní obec Krásná, část obce Pěnčín. Úspěchy doktora Kittela v léčení pacientů byly tak veliké, že již za jeho života o něm kolovaly legendy. Obviňovaly jej ze spolčení s ďáblem a vykreslovaly jeho nadpřirozené skutky.

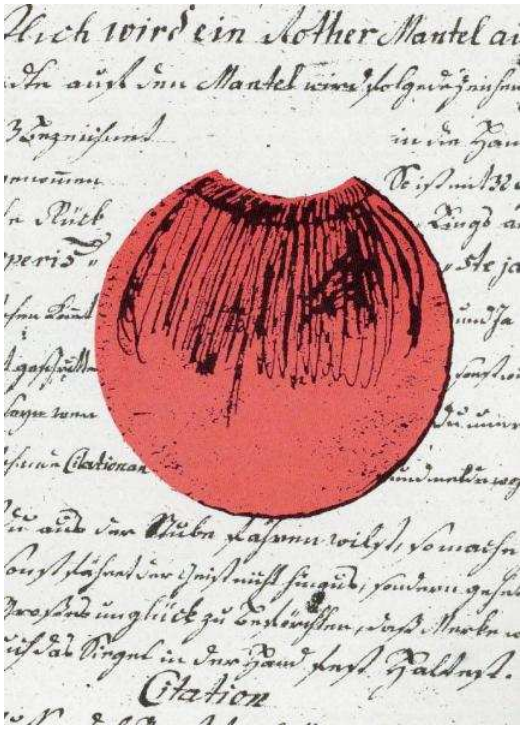
Do dnešních dnů po doktoru Kittelovi zůstalo mnoho památek - jeho dům zvaný Burk, kostel sv. Josefa, který nechal postavit, fara, studánka. Všechny je možné navštívit, stojí dodnes. Doktor Kittel byl i inspirací současníkům - byl o něm natočený amatérský celovečerní film Eleazar Kittel, kde postavu výborně ztvárnil Přemysl Ivan Hadrava, vyrábí se Kitl Šláftruňk nebo Bylinný likér doktora Kittela.¨

Kittelovo muzeum

V roce 2010 bylo na Krásné-Pěnčíně otevřeno Kittelovo muzeum. Vzniklo v domě č. p. 11, který leží mezi „Burkem“ a kostelem sv. Josefa. Interaktivní expozice muzea je zaměřena nejen na život a léčení pověstného doktora Kittela, ale i na historii Kittelovska, bohatství lidového léčitelství a sílu bylin. Mezi největší lákadla expozice patří například alchymistická Kittelova pracovna nebo replika tzv. „smržovského grimoáru“, čarodějné knihy připisované právě Kittelovi. Milovníci přírody si mohou prohlédnout obnovenou zahrádku léčivých bylin nebo se dozvědět zajímavosti, jak se u nás na horách dříve léčilo. Svým pojetím je muzeum vhodné také pro návštěvy rodin s dětmi.

Externí odkazy

- stránky Kittelova muzea http://www.kittel.cz/
- stránky věnované doktoru Kittelovi http://www.kitl.cz/cz
- stránky obce Pěnčín http://www.pencin.cz/



Následující citace převzaty z externích odkazů

Kostel byl vysvěcen v roce 1760, o dva roky později byly do tzv. Svatých schodů uloženy ostatky svatých a po dalších jedenácti letech byla dostavěna také věž. Od roku 1772 byl šumburským kaplanem Filip Jakub, osmý z dětí Kittelových. Ten se pak v roce 1783 stal prvním šumburským farářem (podle pověstí další důkaz o snaze vyvázat se ze smlouvy s Ďáblem).

Na podzim 1777 se v Šumburku konala veliká oslava zlaté svatby manželů Kittelových, které se zúčastnilo mnoho význačných hostů včetně šlechty a o které se ještě dlouho mluvilo. Doktor Kittel byl již osobností známou po celých Čechách.

Kittelova žena Anna Marie zemřela 20. srpna 1782. Necelé tři měsíce před jeho osmdesátými narozeninami, dne 16. listopadu 1783, se Šumburk rozloučil i s věhlasným doktorem.

Kittel je v němčině označení pro dlouhý splývavý plášť. Doktor Kittel nosil za každého počasí, v každé roční době, volný hnědý plášť. Podle pověstí to byl plášť tmavě modrý s červenou podšívkou a na něm doktor Kittel létal. V čarodějné knize nalezené na Smržovce (tzv. Smržovský grimoár), jíž dle některých Kittel vlastnil, je podrobné zaříkávání a návod, jak na plášti létat.

Smržovský grimoár - dle pověstí čarodějná kniha doktora Kittela

Dne 15. 9. 1779 projížděl územím severních Čech císař Josef II. a v Šumburku (dnes Krásná) se s Kittelem osobně setkal. O jeho schopnostech si dokonce udělal záznam do svého cestovního deníku.

F. Call for Papers Mikulášská kryptobesídka

2. – 3. prosinec 2010, , Hotel Olympik Praha

http://mkb.buslab.org

Základní informace

Mikulášská kryptobesídka se koná letos již podesáté. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *2. prosince 2010* a (b) půldne prezentací příspěvků a diskusí v pátek *3. prosince 2010*. Pro workshop jsou domluveny zvané příspěvky:

- Danilo Gligoroski (NTNU, Norsko) na téma SHA-3 a BMW.
- Paul Leyland (Cepia Technologies, ČR) na téma GPU a kryptanalýzy.
- Tomáš Rosa (Raiffeisenbank a UK, ČR) na téma bezpečnosti RFID.
- Dan Cvrček (Apoideas, UK a VUT v Brně, ČR) na téma kryptografie v bankovnictví.
- Petr Hanáček (VUT v Brně, ČR) a Petr Švenda (MU, ČR) na téma kryptografie v bezdrátových senzorových sítích.

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: http://mkb.buslab.org.

Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. Návrhy se přijímají odděleně pro sekci KEYMAKER (studentská soutěž) a pro hlavní program workshopu. Oba druhy návrhů mají požadovaný rozsah 5-15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER, nebo STANDARD TRACK.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://mkb.buslab.org. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo PDF a to tak, aby na uvedenou adresu přišly nejpozději do *30. září 2010*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2010 – navrh prispevku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *26. října*. Příspěvek pro sborník workshopu pak musí být dodán do *18. listopadu*.

Důležité termíny

Návrhy příspěvků:	30. září 2010
Oznámení o přijetí/odmítnutí:	26. října 2010
Příspěvky pro sborník:	18. listopadu 2010
Konání MKB 2010:	2. – 3. prosince 2010

Mediální partneři

Programový výbor

Otokar Grošek, STU Bratislava, SR
Vlastimil Klíma, KNZ, ČR
Jan Krhovják, Cepia Technologies, ČR
Vašek Matyáš, FI MU, Brno, ČR – předseda
Luděk Smolík, Siegen, SRN
Martin Stanek, UK, Bratislava, SR
Pavel Vondruška, Telefónica O2 & UK, ČR

G. KEYMAKER – studentská soutěž

v rámci workshopu Mikulášská kryptobesídka

2. – 3. prosinec 2010, Hotel Olympik, Praha

http://mkb.buslab.org

BUSLab

Mikulášská kryptobesídka se koná letos již podesáté. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *2. prosince 2010* a (b) půldne prezentací příspěvků a diskusí v pátek *3. prosince 2010*. Pro workshop jsou domluveny zvané příspěvky:

- Danilo Gligoroski (NTNU, Norsko) na téma SHA-3 a BMW.
- Paul Leyland (Cepia Technologies, ČR) na téma GPU a kryptoanalýzy.
- Tomáš Rosa (Raiffeisenbank a UK, ČR) na téma bezpečnosti RFID.
- Dan Cvrček (Apoideas, UK a VUT v Brně, ČR) na téma kryptografie v bankovnictví.
- Petr Hanáček (VUT v Brně, ČR) a Petr Švenda (MU, ČR) na téma kryptografie v bezdrátových senzorových sítích.

KEYMAKER – Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie, počítačové a komunikační bezpečnosti a dalších souvisejících oblastí. Návrhy se přijímají odděleně pro sekci KEYMAKER (studentská soutěž) a pro hlavní program workshopu. Příspěvek pro KEYMAKER má požadovaný rozsah 5 -15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER. Přijímány jsou články, bakalářské či diplomové práce, nebo jiná kvalitní ucelená díla, kde v případě rozsahu nad 15 stran požadujeme výtah podstatného obsahu v max. rozsahu 8 stran, s vlastní prací jako přílohou.

Mezi autory nejlepších příspěvků PV rozdělí *finanční odměny v celkové výši 150 tisíc Kč*. Oceněno bude min. 3 a max. 7 příspěvků. Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *30. října*. Příspěvek pak musí být prezentován na workshopu.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://mkb.buslab.org. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu PDF, příp. RTF a to tak, aby na uvedenou adresu přišly nejpozději do *30. září 2010*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2010 – navrh prispevku KEYMAKER“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Důležité termíny

Návrhy příspěvků:	30. září 2010
Oznámení o přijetí/odmítnutí:	26. října 2010
Příspěvky pro sborník:	18. listopadu 2010
Konání MKB 2010:	2. – 3. prosince 2010

Mediální partneři

Programový výbor

Martin Drahanský, VUT v Brně, ČR
Otokar Grošek, STU Bratislava, SR
Petr Hanáček, VUT v Brně, ČR
Vlastimil Klíma, KNZ, Č
Jan Krhovják, Cepia Technologies, ČR
Vašek Matyáš, FI MU, Brno, ČR – předseda
Luděk Smolík, Siegen, SRN
Martin Stanek, UK, Bratislava, SR
Pavel Vondruška, Telefónica O2 & UK, ČR

H. O čem jsme psali v září 2000 – 2009

Crypto-World 9/1999

Crypto-World 9/2000

Příloha : gold_bug.rtf

Dnešní přílohou je klasická povídka The Gold Bug od Edgara Allana Poea (další informace k příloze viz závěr článku "Část I.- Začínáme steganografií" , str.10) .

Crypto-World 9/2001

Crypto-World 9/2002

Crypto-World 9/2003

Crypto-World 9/2004

Crypto-World 9/2005

Crypto-World 9/2006

Crypto-World 9/2007

Crypto-World 9/2008

Crypto-World 9/2009

I. 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
Stálí přispěvatelé:	Vlastimil Klíma
	Pavel Vondruška
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS (výběr příspěvků, komentáře a vkládání na web)	Jaroslav Pinkava Vlastimil Klíma Pavel Vondruška Tomáš Rosa
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info