Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 11, číslo 10/2009 **15. říjen 2009**

10/2009

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1328 registrovaných odběratelů)

Obsah :

Příloha: ---

A. Podzimní *Soutěž v luštění 2009* začíná

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

Úvodní informace k soutěži

Letošní soutěž je doprovázena fiktivním příběhem z padesátých let minulého století. V příběhu a tedy i v soutěži hraje důležitou úlohu šifrátor z té doby ŠD-2. Softwarový simulátor na základě jím provedené rekonstrukce naprogramoval můj student Vojtěch Brtník v rámci letošní bakalářské práce na MFF UK. Více informací o tomto šifrovacím stroji najdete v e-zinu Crypto-World 78/2009 v jeho článku Rekonstrukce šifrovacího stroje ŠD-2 . Zde najdete také odkaz na simulátor.

B. Pravidla Soutěže 2009

Soutěž začíná 18.10.2009 rozesláním e-mailu s výzvou k soutěži všem odběratelům e-zinu Crypto-World a končíkoncem listopadu 2009 (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://soutez2009.crypto-world.info).

Při registraci na webovské stránce soutěže musí řešitel zadat *Kód soutěže 2009*, který mu byl zaslán společně s kódy pro stažení e-zinu Crypto-World 10/2009 (*Kód soutěže 2009* 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)!

Zadává se "klíčové" slovo z vyluštěného textu, pomoc s výběrem klíčového slova bude uvedena v nápovědi, 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 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.

C. Soutěž 2009 - ceny

1. cena

a) Pro vítěze celé soutěže je připravena tradiční hlavní cena - bezplatná účast na mezinárodním kryptologickém workshopu Mikulášská kryptobesídka (http://mkb.buslab.org/), který se letos koná v Praze 3.-4.prosince.
Pořadatel 9.ročníku TNS (Trusted Network Solutions , http://www.kernun.cz/) a BUSLab (http://www.buslab.org/) hradí za vítěze registrační poplatek a zve jej srdečně na tuto akci.

b) kniha - Matyáš,V., Krhovják, J. a kol.: Autorizace elektronických transakcí a autentizace dat i uživatelů, Masarykova univerzita, 2008
věnuje kolektiv autorů http://www.fi.muni.cz/research/laboratories/labak/ , http://www.buslab.org/

c) kniha - Scott McNulty: WordPress - efektivní publikování na webu, Zoner Press 2009,
http://www.zonerpress.cz/kniha/pro-programatory/wordpress-efektivni-publikovani-na-webu
věnuje nakladatelství Zoner Press http://www.zonerpress.cz/

2. cena

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

c) kniha - Scott Kelby: Digitální fotografie 2, Zoner Press 2008
http://www.zonerpress.cz/kniha/pro-grafiky-a-fotografy/digitalni-fotografie-2
věnuje nakladatelství Zoner Press http://www.zonerpress.cz/

3. cena

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

b) kniha - Scott McNulty: WordPress - efektivní publikování na webu, Zoner Press 2009,
http://www.zonerpress.cz/kniha/pro-programatory/wordpress-efektivni-publikovani-na-webu
věnuje nakladatelství Zoner Press http://www.zonerpress.cz/

Ceny pro 3 náhodně vylosované úspěšné řešitele (losuje ze všech řešitelů, kteří splní limit)

2x Scott Kelby: Digitální fotografie 2, Zoner Press 2008
http://www.zonerpress.cz/kniha/pro-grafiky-a-fotografy/digitalni-fotografie-2

1x Scott McNulty: WordPress - efektivní publikování na webu, Zoner Press 2009, http://www.zonerpress.cz/kniha/pro-programatory/wordpress-efektivni-publikovani-na-webu

věnuje nakladatelství Zoner Press http://www.zonerpress.cz/

D. Doprovodný příběh k Soutěži v luštění 2009

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

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

1. JAK SE STAL VÁCLAV PROKOPEC VĚZNĚM

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

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

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

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

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

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

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

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

2. JAK SE STAL VÁCLAV PROKOPEC KRYPTOLOGEM

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

Václav vzpomínal:

Bylo mi již 21 let, když jsem ostříhaný dohola 1. října 1952 narukoval k ženistům do starých Fučíkových kasáren v Táboře. Měl jsem absolvovanou měšťanku v Nečtinách a pokračovací školu v Manětíně a vyučen jsem byl jako strojní zámečník. Zde jsem absolvoval tzv. přijímač, složil vojenskou přísahu a začal poddůstojnickou školu. Jako syn partyzána jsem byl považován za spolehlivého a tak když byli hledáni vhodní adepti pro šifranty, byl jsem pozván na PVS, kde jsme dostali k vyplnění speciální testy. Vypadalo to, že zjišťují naši inteligenci. Vůbec jsme netušili, proč nám dávají k řešení tyto rébusy a ptají se nás, zda rádi luštíme křížovky, zda umíme šachy apod.
Pplk. ing. Ondřej Sýkora, který nám na PVS tyto testy rozdal a vedl s námi pohovor, pak vybral mne a ještě jednoho mého kolegu a oznámil nám, že budeme vycvičeni jako pracovníci vojenské šifrové služby. Proč ne? Zdálo se mi to zajímavé a navíc nám sliboval i velmi slušné zacházení a po vojně i práci a zajímavé finanční ohodnocení.

A tak jsem byl v březnu 1953 vyslán do Administrativního kurzu C v Tloskově u Neveklova, což byl krycí název čtyřměsíčního kurzu šifrantů - důstojníků v záloze. Tehdejším náčelníkem šifrové služby GŠ byl právě ing. pplk. Ondřej Sýkora, kterého jsem již znal z testů. Jeho oddělení čítalo asi 20 osob, bylo to důstojníci - učitelé. Já jsem byl zařazen do první čety, kde nám velel npor. ing. Prachař.
V kurzu nás bylo na 300 absolventů ŠDZ (!) ode všech druhů vojsk. Seznámili nás s historií a rozvojem kryptologie (kryptografie), seznámili nás s jednouchými šifrovacími systémy a jejich luštěním, naučili nás šifrovat ručními prostředky za použití převodových tabulek a písmenkových heslových materiálů, ale také lehce zapamatovatelných klíčů, tvořit signální či hovorové tabulky, naučili nás používat německý diskový šifrovací stroj Enigma, který se stále v naší armádě používal a nakonec jako zvláštní tajemství nám ukázali i diskový šifrovací stroj ANNA, etablovaný na dálnopisných stanicích svazků. Museli jsme se naučit užívat i polní spojovací prostředky včetně sovětské přenosné radiostanice A7b a německého dálnopisu Hell, který byl získaný ve velkém množství jako válečná kořist. Během kurzu byly pořádány tři jednodenní soutěže v luštění jednoduchých úloh (jednoduchá záměna, transpozice apod.). Soutěže se pořádaly vždy v pátek. Tři nejlepší měli za odměnu slíben opušťák na následující sobotu a neděli. Jaké bylo překvapení velitele mé čety a velitele kurzu, když všechny tři soutěže jsem vyhrál já! Kolegové mne dokonce podezírali, že znám výsledky, tak rychle jsem některé úlohy vyřešil…

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

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

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

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

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

3. JAK SE STAL VÁCLAV PROKOPEC ZRÁDCEM

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

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

Byl teplý květnový večer roku 1957. Václav se procházel po Kampě a pak zašel do vinárny u Dvou grošů. Objednal si dvě deci bílého vína a rozhlížel se znuděně po místnosti. V tom uviděl u protějšího stolu svého spolužáka z měšťanky v Nečtinách Karla Webera. Bylo mu to trochu divné, myslel si, že byl odsunut tak, jako ostatní Němci z vesnice Stvolny, kde Karlův otec měl velký statek. Byl však rád, že vidí někoho známého, a protože tam Karel seděl sám, vstal a přisedl k němu. Strávili spolu zajímavý večer, povídali si a vzpomínali na školu a své spolužáky a spolužačky. Řeč přišla i na spolužačku Evu, která se Václavovi tolik líbila. Václav nechtěl kazit ten hezký večer, ale pak si našel odvahu a zeptal se, jak je to možné, že zde Karel je. Byl přece odsunut. Karel se zasmál a řekl: „Neboj, jsem zde legálně. Ale nechce se mi o tom mluvit.“ Jenže vypili další sklenku, tedy přesněji další džbánek a Václav zase stočil řeč na jeho návrat.
„Ty ses vrátil, Karle?“ Karel se na něj podíval a pak po chvilce řekl: „No a proč ne?“ „Myslel jsem, že to nejde“, pokračoval Václav. „Ale jde“ řekl na to Karel a pak mu

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

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

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

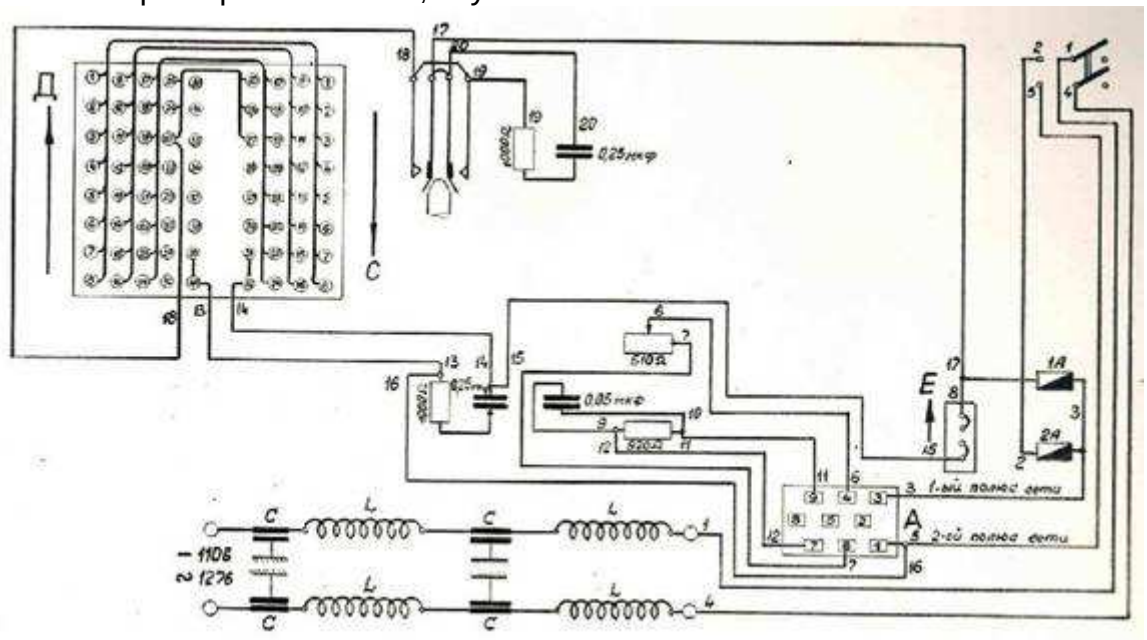
Na jednom z flámů dokonce Karel hostil Václava i s jeho nadřízeným ing. Ondřejem Sýkorou. Ten flám se o pár měsíců později stal inženýru Sýkorovi osudným. Jeho nadřízení mu vyčítali, že se více nezajímal, s kým vlastně jeho podřízený tráví večery a navíc na něm ulpělo i vážné podezření, že snad věděl,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

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

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

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

Václav velmi brzy pochopil obrovský význam, jaký mají plány tohoto šifrátoru, který byl v Sovětském svazu používán. Kontaktoval Karla a o šifrátoru mu řekl. Slíbil, že plány překreslí a vše, co mu bude o zařízení známo, předá. Současně si však vymínil, že to bude ta poslední věc, co pro něj udělá. Žádá za to pak ihned zařízení přechodu do Německa a slušnou sumičku peněz. Karel vše do centrály ohlásil, počkal na pokyny a za týden se s Václavem opět sešel. Oznámil mu, že je vše zařízeno. „Přines plány a budeme se bavit, kdy a kde přejdeš.“ Václav Karla nečekaně překvapil. Plány již měl obkresleny a dokonce je přinesl na schůzku s sebou. Beze slova je teď vyndal a zabalené v Rudém Právu je dal Karlovi. Po chvilce mlčení překvapenému Karlovi pak řekl: „Jsme tedy domluveni, zajisti mi odchod a příští pátek mi řekni, kdy a kde!“ S tím se také ten večer rozloučili.



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

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

Zatčen byl druhý den i jeho nadřízený, protože dle vyšetřovatelů nebylo možné, aby netušil, že se děje něco nepatřičného. Navíc bylo zjištěno, že se sám jedné ze schůzek dokonce zúčastnil a přitom nic podezřelého nenahlásil. Nezodpovědně dokonce zařadil Václava Prokopce na jeden z nejdůležitějších úkolů odboru. Mělo se však všeobecně za to, že Václav Prokopec byl zatčen dříve, než se pořádně seznámil s plány šifrátoru a že nebylo možné, aby je stačil obkreslit a předat cestou Karla Webera cizí rozvědce. Ing. Ondřej Sýkora sice tušil, že to mohl stihnout, neboť mu umožnil, aby se s plány seznámil ještě dříve, než celý projekt oficiálně startoval, ale ve vlastním zájmu mlčel a ani u soudu se o tom on nebo Karel Weber nezmínil.

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

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

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

E. Luštitelské etudy I. Rusko 1918

Mgr. Karel Šklíba (karel.skliba@cryptoworld.info)

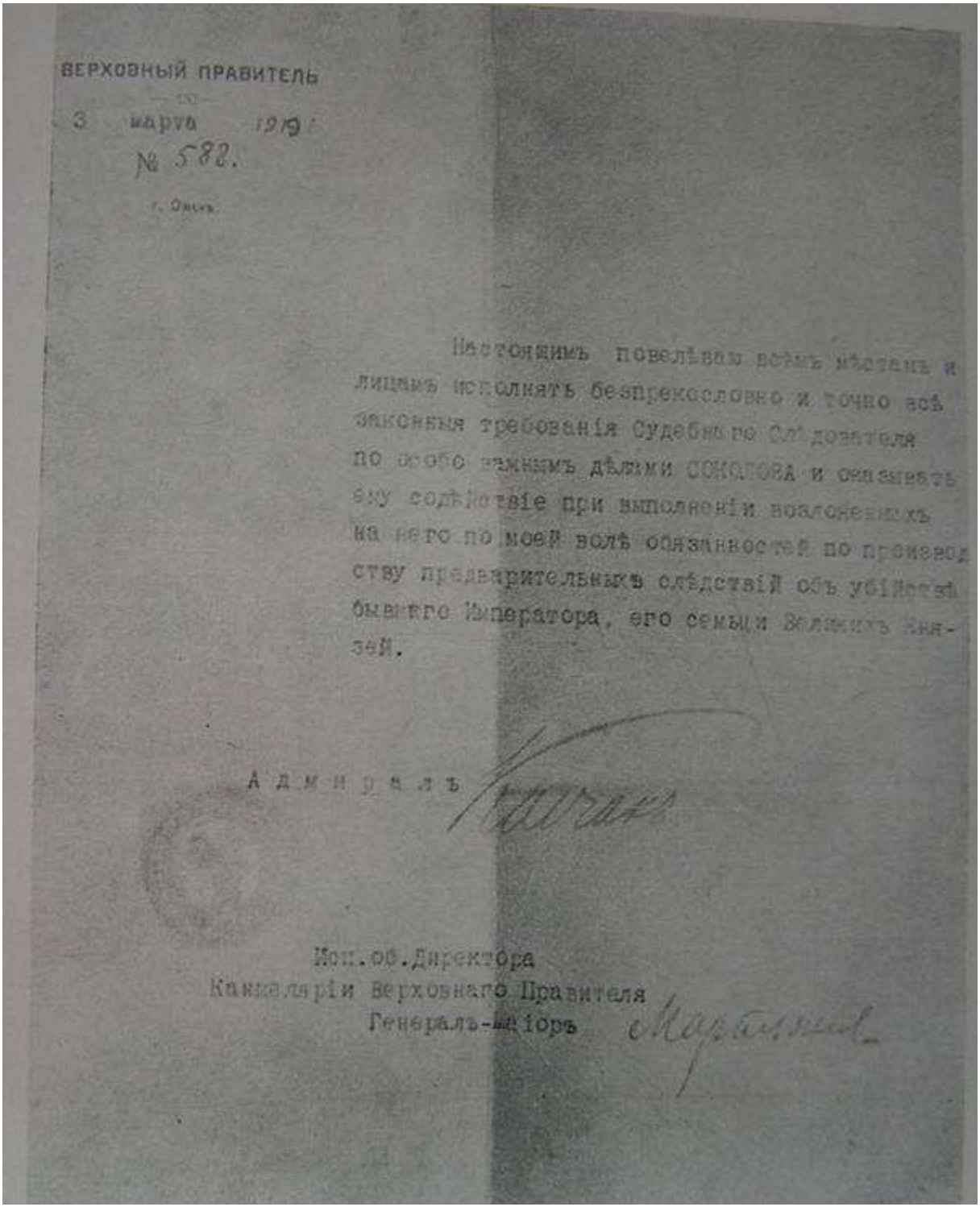
Jednou z nejvýznamnějších událostí ruské a sovětské revoluce v letech 1917 a 1918 bylo určitě zavraždění cara Mikuláše II. a jeho rodiny v Ipatievově domě v Jekaterinburgu v noci ze 16. na 17. července 1918 a následná likvidace těl v železnorudném povrchovém dole „Čtyř Bratří“ u vesnice Kopťaky ve dnech 17. a 18. července 1918. Tato událost byla aktéry z řad bolševických sil pečlivě připravována a důkladně provedena, a přestože její vyšetřování započalo téměř bezprostředně a bylo soustředěno mnoho nezvratných důkazů, zůstalo mnoho nejasností a otázek, které později nový vítězný režim tutlal a samozřejmě nijak neřešil. Zejména legenda o tom, že byl zabit pouze car a ostatním členům rodiny se podařilo konspirativně uniknout do zahraničí, přetrvala desítky let. Jedním z hlavních důkazů k objasnění této události bylo vyluštění šifrového telegramu, který odeslali vykonavatelé exekuce po události Jakubu Sverdlovovi do Moskvy.

Jekaterinburg byl dobyt 3. plukem a částí 2. pluku československých legií a dvěma setninami kozáku 25. července 1918 a již 30. července byl pověřen krajský vyšetřující soudce Nametkin soudním vyšetřováním události. Z důvodu jeho byrokratického a laxního přístupu (nejspíše však měl oprávněně strach z návratu bolševiků) byl 7. srpna 1918 na gremiální poradě Jekaterinburského krajského soudu z případu odvolán a vyšetřováním byl pověřen vyšetřující soudce pro důležitější případy Sergějev, protože vyšetřující soudce pro zvláště důležité případy, kterému by podle zákona vyšetřování tohoto případu náleželo, nebyl v této oblasti Sibiře k dispozici. V prvních měsících práce soudce Sergějeva neměli bolševici na celém území Ruska od Volhy až na Dálný východ prakticky žádný vliv a celé území představovalo konglomerát mnoha samostatných lokálních vlád. K jejich sloučení došlo v Ufě 23. září 1918, kde se pro celé toto území ustanovila jediná vláda ve formě pětičlenného direktoria. Za měsíc 18. října 1918 soustředil nejvyšší moc ve svých rukou Vrchní vládce admirál Kolčak. Ten dne 17. ledna 1919 vydal rozkaz bývalému vrchnímu veliteli fronty generálu Diterichsovi, aby mu byly předloženy všechny nalezené věci carské rodiny i všechny vyšetřovací spisy. Na základě tohoto rozkazu, který nahrazoval za tehdejších okolností speciální zákon, vydal nařízením z 25. ledna 1919 soudce Sergějev generálu Diterichsovi prvopisy vyšetřovacího řízení a všechny věci doličné v přísně právním pořádku v přítomnosti soudního prokurátora V.F.Jordanského. Admirál Kolčak se zcela jistě obával o osud těchto historických dokumentů a chtěl, aby zůstaly zachovány. Začátkem února 1919 předložil generál Diterichs v Omsku všechny materiály Vrchnímu vládci admirálu Kolčakovi. Tak závažný případ měl být podle zákona přidělen jen zvláštnímu sboru vyšetřujících soudců. Před admirálem Kolčakem však evidentně stála otázka, kde je vzít.

Dne 5. února 1919 povolal admirál Kolčak do Omsku soudce Nikolaje Alexejeviče Sokolova, který se narodil 1882 v Mokšaně, vystudoval gymnázium v Penze a práva na Charkovské univerzitě a působil jako vyšetřující soudce v Penzenské gubernii. Po dvou poradách u admirála Kolčaka dne 6. února 1919 obdržel soudce Sokolov 7. února nařízení ministra spravedlnosti o převzetí vyšetřovacího řízení a ještě téhož dne převzal od generála Diterichse všechny vyšetřovací spisy a věci doličné. Admirál Kolčak měl na věci vyšetření smrti carské rodiny eminentní zájem a vydal proto v Omsku 3. března 1919 pod číslem 588 následující rozkaz:

„Nařizuji tímto všem úřadům a osobám plniti bezpodmínečně a přesně všechny zákonné požadavky vyšetřujícího soudce pro zvlášť důležité případy SOKOLOVA a

pomáhati mu při plnění rozkazů, jež mu byly z mé vůle dány pro vyšetřovací řízení o zavraždění bývalého cara, jeho rodiny a velkoknížat. Admirál Kolčak.
Přednosta kanceláře Vrchního vládce V zastoupení generálmajor Martyjanov“ (viz ilustrace)



ВЕРХОВНЫЙ ПРАВИТЕЛЬ

3 марта 1919 г.

№ 582.

г. Омскъ.

Настоящимъ повелѣваю всѣмъ мѣстнымъ и лицамъ исполнять безпрекословно и точно всѣ законныя требованія Судебнаго Слѣдователя по особо важнымъ дѣламъ СОКОЛОВА и оказывать ему содѣйствіе при выполненіи возложенныхъ на него по моей волѣ обязанностей по производству предварительныхъ слѣдствій объ убійствѣ бывшаго Императора, его семьи и Великихъ Князей.

Адмиралъ

Исп. об. Директора
Канцеляріи Верховнаго Правителя
Генералъ-маіоръ

Je všeobecně známo, že během roku 1919 se politické a zejména vojenské postavení Kolčakovy vlády postupně zcela zhroutilo a admirál Kolčak sám zahynul 7. února 1920. Soudce Sokolov pracoval neúnavně a nekompromisně na vyšetřování, prováděl výslechy v Jekaterinburgu a pracoval na vykopávkách v obvodu dolu „Čtyř bratří“, což byl název zbytků čtyř samostatně stojících borovic nedaleko šachty, kam byly vhozeny zbytky mrtvol

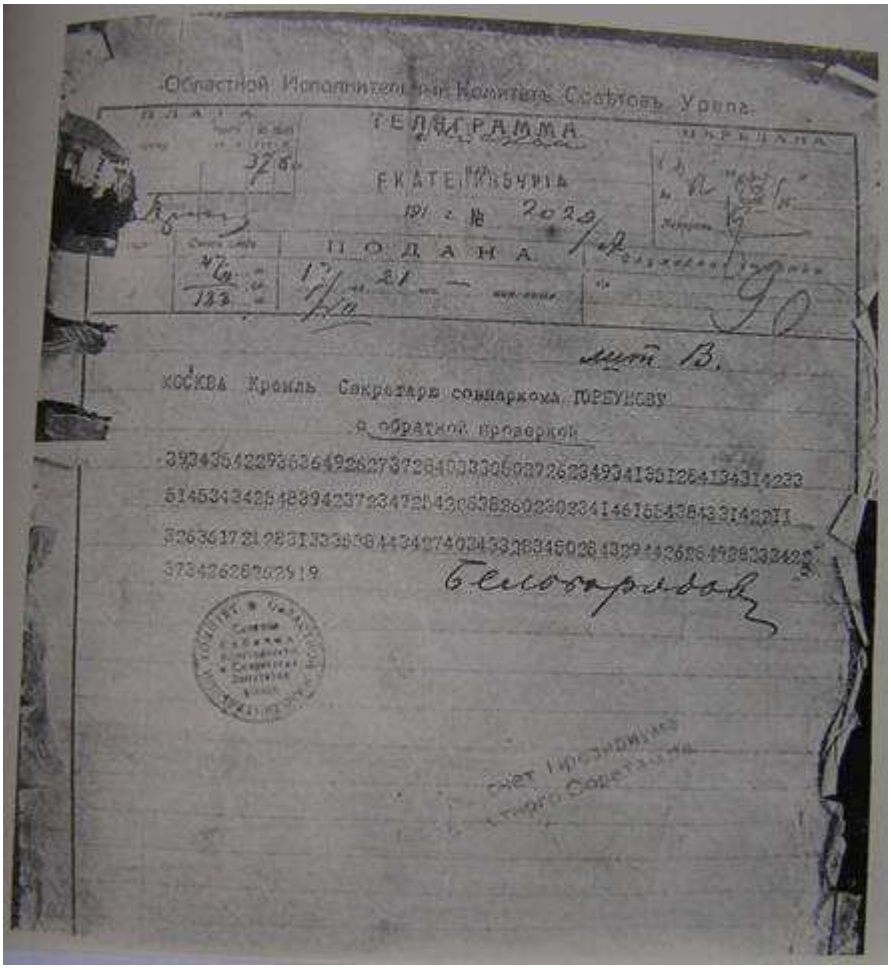
cara a členů jeho rodiny 18.7.1918. Mrtvá těla byla předtím vedle šachty polita benzínem a zapálena a ohořelé zbytky byly před vhozením do šachty polity celkem 177,6 kg japonské kyseliny sírové. Sokolov na vykopávkách pracoval v roce 1919 až do okamžiku, kdy důl kontaktovaly hlídky rozvědky bolševiků. Potom začal se všemi důkazy, vyšetřovacími spisy a doličnými předměty po železnici přesun na Dálný východ s představou odjezdu do evropské emigrace. Kolčakova smrt ho zastihla v mandžuském Charbinu, odkud se snažil odcestovat do Evropy. První pokus učinil u anglického velvyslance v Pekingu Lampsona, kterého prosil, aby mu umožnil vyvézt do Evropy soudní akta a věci doličné s poukazem na to, že mezi nimi je pozůstalost carské rodiny. 23. února 1920 přijel do Charbinu velvyslancův tajemník Keef, který oznámil, že věc je v řízení v Londýně, a pravděpodobně nepochyboval o kladné odpovědi, protože Sokolovův vagón byl připojen ke Keefovu vlaku a hlídán. Studená sprcha přišla 19. března, kdy anglický konzul v Charbinu Sley doručil lakonickou odpověď britské vlády – „Nemůžeme“. Soudce Sokolov se společně s generálem Diterichsem obrátili na francouzského generála Janina, který odpověděl, že se nebude nikoho ptát a pomoc v takové situaci považuje za čestnou povinnost. Finance na cestu poskytli dva Rusové žijící v Chabrinu a soudce Sokolov se se všemi materiály dostal do Paříže, kde pokračoval ve vyšetřování až do roku 1922. Zemřel 23. listopadu 1924 v Salbrie, kde je také pochován. V letech 1921 až 1924 stihl zpracovat a poté publikovat precisní a maximálně podrobnou zprávu (300 stran) o zavraždění carské rodiny, která vyšla v roce 1926 v českém překladu. Rovněž generál M. K. Diterichs vydal v Paříži v roce 1924 knihu „Zavraždění carské rodiny a členů rodu Romanova na Urale“ (Société Anonyme de Presse, de Publicité et d'Editions), která však nebyla při psaní tohoto textu k dispozici.

Zpráva soudce Sokolova obsahuje obrovské množství nepřímých a řadu přímých důkazů k událostem zavraždění carské rodiny a následné likvidace těl v Jekaterinburgu ve dnech 16. až 18. července 1918. Ovšem korunní důkaz o tom, že vražda všech členů carské rodiny, tedy nejen poprava samotného cara Mikuláše II., byla domluvena a připravena předem v Moskvě, je šifrovaný telegram, který odeslal z Jekaterinburgu do Moskvy předseda Uralské krajské rady dělnických, selských a vojenských zástupců Běloborodov 17. července 1918. Předem domluvená legenda k této popravě, ale nikoliv vraždě, kterou potvrzuje tento telegram, zněla, že popraven byl revolučními silami pouze car, ovšem ostatní členové jeho rodiny zahynuli spíše náhodou při evakuaci. Šifrovanou verzi tohoto telegramu měl soudce Sokolov k dispozici již v materiálech předaných generálu Diterichsovi vyšetřovacím soudcem Sergějevem v lednu 1919, neboť na základě nařízení prokurátora Jekaterinburského krajského soudu ze dne 4.1.1919 předal ve dnech 20. a 26.1.1919 přednosta Jekaterinburského telegrafního úřadu soudci Sergějevovi prvopisy celkem 65 bolševických telegramů. Počet 65 telegramů představuje skvělé východisko pro luštitele. Takový člověk ovšem musí existovat, ale kde ho najít na Sibiři za občanské války v roce 1919. Soudce Sokolov předpokládal, že telegramy mohou být klíčem k mnohým informacím, obrátil se proto již 24. února 1919 na odborníka (není ve zprávě jmenován) u Nejvyššího velitelství Kolčakovy armády s negativním výsledkem, 28. února 1919 kontaktoval ve věci Ministerstvo zahraničních věcí Kolčakovy vlády a později předal požadavek na vyluštění telegramů Vrchnímu veliteli spojeneckých vojsk v Rusku francouzskému generálu Janinovi. Vše s výsledkem nula. Škoda, že se soudce Sokolov neobrátil se svým problémem i na velení Československých legií na Rusi, možná by se tam nalezl nějaký šikovný šifrér schopný vyluštit polyalfabetickou substituční šifru. Soudce Sokolov ve své zprávě uvádí, že teprve v roce 1920 se „mi v Evropě podařilo najíti toho ruského člověka, který byl vždy znám jako osobnost mimořádných schopností a zkušeností v tomto oboru“. Identita tohoto člověka není ve zprávě ani náznakem uvedena, což je pochopitelné, neboť zveřejnění jím vyluštěných telegramů pro něho tehdy představovalo smrtelné nebezpečí ze strany rozvědky ČEKY. Telegramy předal tomuto

„ruskému člověku“ soudce Sokolov 25.8.1920 a 15.září téhož roku dostal telegramy vyluštěné (není však známo, zda bylo vyluštěno všech 65 telegramů, ale je pravděpodobné, že ano).

Zásadní význam mělo vyluštění telegramu ze dne 17.7.1918, který v českém překladu zní: „Předejte Sverdlovovi, že celou rodinu stihl týž osud jako hlavu, oficiálně rodina zahyne při evakuaci“. Text telegramu přímo dokazuje, že byla povražděna celá carská rodina a ne pouze car, jak bylo bezprostředně poté bolševickou vládou v Moskvě oznámeno. Dále telegram potvrzuje roli předsedy Ústředního výkonného výboru sovětů (CIK) Jakuba Sverdlova jako pravděpodobného organizátora a zcela jistého schvalovatele celé akce.
(Jakub Moisejevič Sverdlov byl občanem města Polock, Vitebská gubernie, židovské národnosti. Narodil se 1885 v Nižním Novgorodě, kde navštěvoval gymnázium, které nedokončil a byl lékárnickým učněm. Od roku 1907 byl členem bolševického permského výboru, byl dvakrát vězněn, stal se členem vojensko-revolučního výboru, který řídil revoluci v Rusku 25.10.1917, následně se stal předsedou CIK, tedy premiérem.)

Šifrový systém používaný bolševiky v tomto případě je periodický substituční systém s délkou periody 12 s vzestupně uspořádanými substitučními číselnými posloupnostmi. Metody luštění takovýchto systémů jsou široce popsány v kryptoanalytické literatuře (viz např. luštitelské soutěže v prvních ročnících Cryptoworldu). Podmínkou úspěšného luštění je ovšem dostatečná délka šifrového textu delší než vzdálenost jednoznačnosti pro tento systém. V tomto případě však bylo k dispozici minimálně 65 šifrových textů, z nichž nejméně 3 (pravděpodobně však mnohem více) byly zašifrovány stejným způsobem, jako zkoumaný telegram. Statistickou analýzou těchto šifrových textů (tj. číselných dvojic) náš tajemný luštitel nejprve zjistil délku hesla a následně rekonstruoval převodovou substituční tabulku, kde mu velice pomohlo, že číselné posloupnosti byly vzestupné číselné řady.



Telegram z Jekaterinburgu do Moskvy 17.VII. 21 hodin (viz ilustrace)

MOSKVA Kreml Sekretarju sovnarkoma GORBUNOVU
s obratnoj proverkoj
39343542293536492627372840333050272623493413512841343142 33
51453434254839423723472542283826023023414615543843314221 1
32636172128313335384434274034332834502843294426284938333422
37342628262919 Beloborodov

Statistickou analýzou frekvence číselných dvojic (všechny telegramy měly pravděpodobně sudou délku) tohoto a dalších minimálně 64 šifrových telegramů byla odhadnuta v tomto případě délka periody 12. Šifrový text byl proto periodicky rozepsán po dvojicích s periodou 12 a byl do něho postupně vpisován otevřený text a zároveň byla rekonstruována substituční tabulka:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
39	34	35	42	29	35	36	49	26	27	37	28
P	E	R	E	D	A	I	T	E	S	V	E
40	33	30	50	27	26	23	49	34	13	51	28
R	D	L	O	V	U	Č	T	O	V	S	E
41	34	31	42	33	51	45	34	34	25	48	39
S	E	M	E	I	S	T	V	O	P	O	S
42	37	23	47	25	42	28	38	26	02	30	23
T	I	G	L	A	T	A	Ž	E	U	Č	A
41	46	15	54	38	43	31	42	21	13	26	36
S	T	Č	T	O	I	G	L	A	V	U	O
17	21	28	31	33	35	38	44	34	27	40	34
F	F	I	C	I	A	L	N	O	S	E	M
33	28	34	50	28	43	29	44	26	28	49	38
I	JA	P	O	G	I	B	N	E	T	P	R
33	34	22	37	34	26	28	26	29	19		
I	E	V	A	K	U	A	C	I	I		

Tedy otevřený text telegramu zní:

Peredaite Sverdlovu čto vse semeistvo postigla taže učast čto i glavu officialno semija pogibnet pri evakuacii

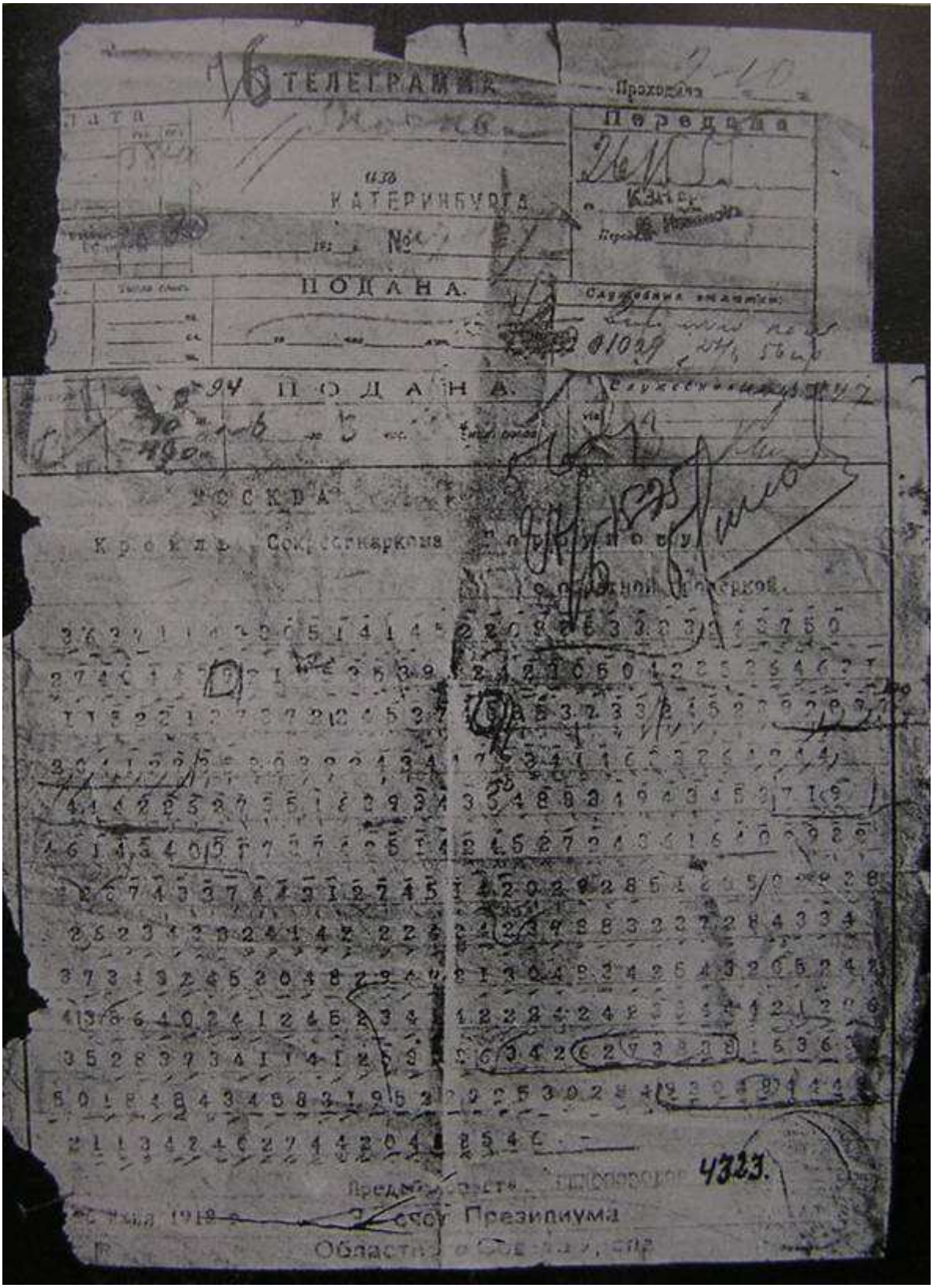
V šifrovém textu se vyskytovaly hodnoty číselných dvojic v intervalu <02,54>, přitom počet písmen azbuky je maximálně 32 a její největší posun může být maximálně dvojnásobný, tedy

64. Z praxe však je známo, že při používání ručních šifrových systémů se v té době nepoužívaly měkký a tvrdý znak, samohlásky tvrdé Y a tzv. obrácené E a dvojhláska JO. V našem případě není použita ani samohláska J a tím je počet používaných znaků zredukován na 27. Heslo pro vytvoření převodové substituční tabulky je v tomto případě téměř jistě slovo EKATERINBURG.

		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**		
		E	**K**	**A**	**T**	**E**	**R**	**I**	**N**	**B**	**U**	**R**	**G**		
U	**02**	16	20	11	28	16	26	19	23	12	02	26	14		
F	**03**	17	21	12	29	17	27	20	24	13	03	27	15		
CH	**04**	18	22	13	30	18	28	21	25	14	04	28	16		
C	**05**	19	23	14	31	19	29	22	26	15	05	29	17		
Č	**06**	20	24	15	32	20	30	23	27	16	06	30	18		
Š	**07**	21	25	16	33	21	31	24	28	17	07	31	19		
ŠČ	**08**	22	26	17	34	22	32	25	29	18	08	32	20		
JU	**09**	23	27	18	35	23	33	26	30	19	09	33	21		
JA	**10**	24	28	19	36	24	34	27	31	20	10	34	22		
A	**11**	25	29	20	37	25	35	28	32	21	11	35	23		
B	**12**	26	30	21	38	26	36	29	33	22	12	36	24		
V	**13**	27	31	22	39	27	37	30	34	23	13	37	25		
G	**14**	28	32	23	40	28	38	31	35	24	14	38	26		
D	**15**	29	33	24	41	29	39	32	36	25	15	39	27		
E	**16**	30	34	25	42	30	40	33	37	26	16	40	28		
Ž	**17**	31	35	26	43	31	41	34	38	27	17	41	29		
Z	**18**	32	36	27	44	32	42	35	39	28	18	42	30		
I	**19**	33	37	28	45	33	43	36	40	29	19	43	31		
K	**20**	34	38	29	46	34	44	37	41	30	20	44	32		
L	**21**	35	39	30	47	35	45	38	42	31	21	45	33		
M	**22**	36	40	31	48	36	46	39	43	32	22	46	34		
N	**23**	37	41	32	49	37	47	40	44	33	23	47	35		
O	**24**	38	42	33	50	38	48	41	45	34	24	48	36		
P	**25**	39	43	34	51	39	49	42	46	35	25	49	37		
R	**26**	40	44	35	52	40	50	43	47	36	26	50	38		
S	**27**	41	45	36	53	41	51	44	48	37	27	51	39		
T	**28**	42	46	37	54	42	52	45	49	38	28	52	40		

Touto substituční tabulkou byly zašifrovány ještě minimálně 2 telegramy odeslané z Jekaterinburgu do Moskvy 26.6.1918 a 8.7.1918, které se však osudů carské rodiny nijak netýkaly. Oba opět podepsal předseda uralského oblastního sovětu Běloborodov.

Překlad telegramu z 26.6.1918 zní:
Již jsme vám oznámili, že veškerá zásoba zlata a platiny byla odtud vyvezena dva vagóny stojí na nádraží Permi prosím sdělit způsob ochrany v případě porážky sovětské vlády názor oblastního výboru strany a oblastního sovětu v případě nezdaru veškerý náklad zničit aby nepřipadl nepřátelům



Telegram č. 4323 z 26.6.1918 (viz ilustrace):
MOSKVA

Kreml Sekrsovnarkoma Gorbunovu
s obratnoj prověrkoj

(1	2	3	4	5	6	7	8	9	10	11	12)
36	37	11	43	30	51	41	45	22	08	35	33
M	I	U	Ž	E	S	O	O	B	ŠČ	A	L
33	24	37	50	27	40	44	39	21	25	35	39
I	Č	T	O	V	E	S	Z	A	P	A	S
32	42	30	50	42	35	36	46	31	11	52	31
Z	O	L	O	T	A	I	P	L	A	T	I
37	37	22	45	27	40	35	37	33	24	52	39
N	I	V	I	V	E	Z	E	N	O	T	S
23	33	20	41	27	35	30	32	24	24	47	23
JU	D	A	D	V	A	V	A	G	O	N	A
41	46	33	36	42	44	41	42	26	27	35	16
S	T	O	JA	T	K	O	L	E	S	A	CH
39	34	35	48	33	49	43	45	37	19	46	14
P	E	R	M	I	P	R	O	S	I	M	U
34	29	27	37	42	51	42	45	37	24	36	16
K	A	Z	A	T	S	P	O	S	O	B	CH
40	29	32	42	37	43	27	44	21	27	45	14
R	A	N	E	N	I	JA	N	A	S	L	U
20	29	28	51	38	50	28	38	26	23	43	22
Č	A	I	P	O	R	A	Ž	E	N	I	JA
41	42	22	42	42	37	38	32	37	28	43	34
S	O	V	E	T	V	L	A	S	T	I	M
37	34	32	45	30	48	29	42	21	20	48	34
N	E	N	I	E	O	B	L	A	K	O	M
25	43	20	52	42	43	36	40	34	12	45	23
A	P	A	R	T	I	I	I	O	B	L	A
41	42	22	42	42	35	44	42	12	06	35	28
S	O	V	E	T	A	S	L	U	Č	A	E
37	34	11	41	25	30	36	34	26	27	38	38
N	E	U	D	A	Č	I	V	E	S	G	R
16	36	34	50	18	48	43	45	33	19	52	27
U	Z	P	O	CH	O	R	O	N	I	T	D
25	30	28	49	30	48	44	49	21	13	43	40
A	B	I	N	E	O	S	T	A	V	I	T
27	44	20	40	25	46						
V	R	A	G	A	M						

Predoblasoveta Beloborodov

Otevřený text telegramu:
Mi uže soobščali čto ves zapas zolota i platini vivezen otsjuda dva vagona stojat kolesach Permi prosim ukazat sposob chranenija na slučai poraženija sovetvlasti mnenie oblakoma partii i oblasoveta slučae neudači ves gruz pochoronit dabi ne ostavit vragam

Telegram č. 4369 z 8.7.1918:

MOSKVA

Sekrsovnarkoma Gorbunovu
S obratnym otvetom

(1	2	3	4	5	6	7	8	9	10	11	12)
28	20	36	42	27	49	33	49	36	24	38	38
G	U	S	E	V	P	E	T	R	O	G	R
25	33	20	53	38	48	29	29	29	21	30	40
A	D	A	S	O	O	B	ŠČ	I	L	Č	T
38	28	35	50	41	45	28	34	31	16	37	36
O	JA	R	O	S	L	A	V	L	E	V	O
32	45	37	37	37	43	33	33	26	21	48	26
Z	S	T	A	N	I	E	B	E	L	O	G
27	29	35	41	30	43	22	37	33	25	48	28
V	A	R	D	E	I	C	E	V	P	O	E
32	33	32	37	36	43	30	45	28	13	50	23
Z	D	N	A	M	I	V	O	Z	V	R	A
22	34	32	50	26	50	28	49	33	24	27	37
ŠČ	E	N	O	B	R	A	T	N	O	F	P
30	44	31	36	25	44	42	45	37	28	26	37
E	R	M	K	A	K	P	O	S	T	U	P
25	46	24	37	35	40	33	45	22	27	26	27
A	T	D	A	L	E	E	O	B	S	U	D
33	46	25	40	38	45	41	29	26	20	43	35
I	T	E	G	O	L	O	ŠČ	E	K	I	N
33	40										
I	M										

Predoblasoveta Beloborodov

Otevřený text telegramu:
Gusev Petrograda soobščil čto Jaroslavle vozstanie belogvardeicev poezd nami vozvraščen obratno f Perm kak postupat dalee obsudite Gološčekinim

Český text telegramu:
Gusev z Petrohradu oznámil, že v Jaroslavi je povstání bělogvardějců vlak jsme vrátili do Permi jak jednat dále projednejte s Gološčekinem

Co bylo obsahem dalších telegramů, které měl soudce Sokolov v Paříži k dispozici v soudních spisech, které přivezl do Francie, není známo. S téměř jistou pravděpodobností jejich obsah nesouvisel s osudy cara ani jeho rodiny. Pro dokreslení situace je velice zajímavá skutečnost, že vyšetřující soudce Sokolov navštívil 14. června 1921 Berlín, kde byl přijat dr. Ritzlerem, který byl členem moskevské mise německé císařské delegace hraběte Mirbacha v roce 1918 a po jeho zavraždění se stal jeho nástupcem v čele mise. Dr. Ritzler seznámil soudce Sokolova s obsahem německé diplomatické korespondence z této mise a v září 1921 mu zaslal opisy části těchto dokumentů. Zajímavé jsou zejména následující 3 telegramy, které svědčí o tom, že sovětská moc utajovala provedenou vraždu členů carské rodiny a zveřejnila pouze zastřelení carovo s odůvodněním úspěšných operací Československých legií na Sibiři.

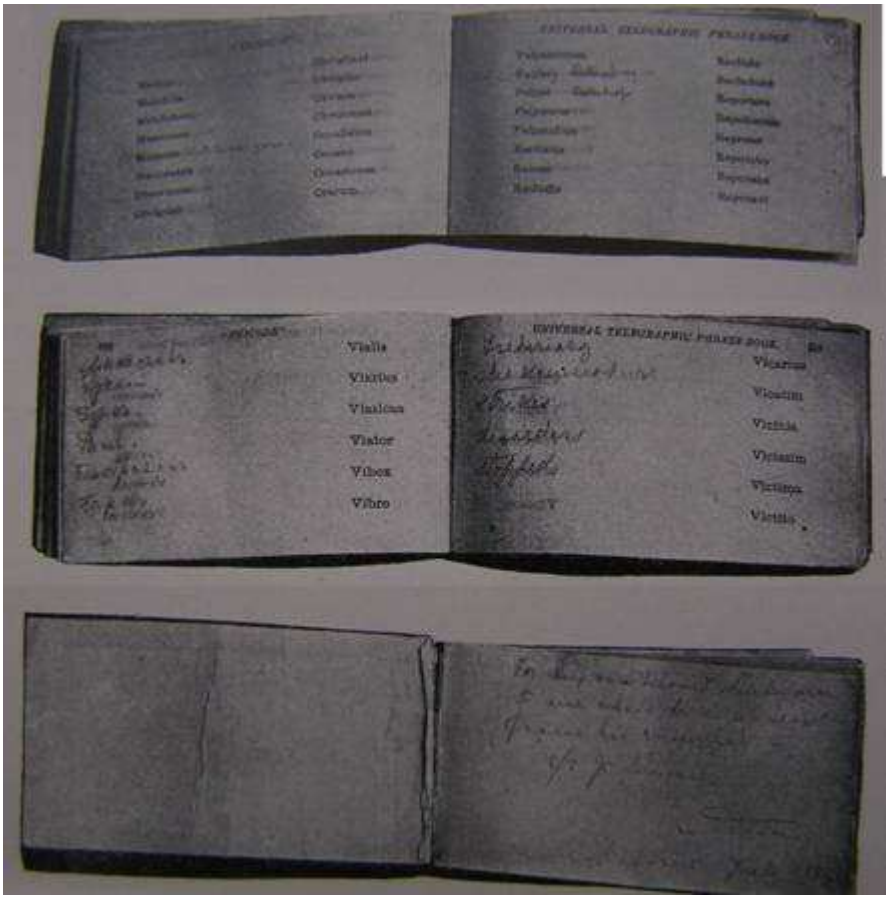
Mise v Moskvě Ministerstvu zahraničních záležitostí Berlín
20. července 1918

Včera jsem říkal Radeku a Vorovskému, že celý svět odsoudí nejpřísnějším způsobem zavraždění cara a že císařský vyslanec je rozhodně nucen varovati je před dalšími kroky na této cestě. Vorovskij odpověděl, že car byl zastřelen jen proto, poněvadž jinak by se ho byli zmocnili Čechoslováci. Radek se neoficielně vyjádřil, že projevíme-li zvláštní zájem o ženské členy carské rodiny z německé krve, pak by snad bylo možno dovoliti jim volný odjezd. Snad by se podařilo osvobodit carevnu a následníka (tohoto, jako neoddělitelného od matky) s odůvodněním humanity a vyrovnati tak otázku praporu. Ritzler

Ministerstvo zahraničních záležitostí Berlín Zplnomocněnci v Moskvě
20. července 1918
Se zakročením ve prospěch carské rodiny souhlasím. Busche

Mise v Moskvě Ministerstvu zahraničních záležitostí Berlín
23. července 1918
Zakročil jsem ve prospěch carevny a princezen německé krve s poukazem na vliv, který by zanechala vražda na veřejné mínění. Čičerin mlčky vyslechl moje slova. Ritzler

Ještě jedna záležitost se ve zprávě soudce Sokolova týkala šifer. Mezi mnoha položkami zabavenými již vyšetřovacím soudcem Nametkinem v Ipatievově domě 2.8.1918 byly i údajné carovy a carevniny šifry, které byly nalezeny v troubě kamen na záchodě pravděpodobně v prvním patře (viz ilustrace).



Byl to však blok označený UNICODE a UNIVERSAL TELEGRAPHIC PHRASEBOOK s ruskými a anglickými vpisky a ručně psanou datací 1894. Je možné, že tento blok používal

car nebo někdo z jeho okolí pro komunikaci, ale rozhodně se nejednalo o šifrový systém, který by používal car Mikuláš II jako ruský imperátor. Ve svém postavení vládce používal 3 šifrové systémy:

První byl z roku 1911 elegantní knížečka širokého formátu o rozměrech 14,5x21 cm ve smaragdově zelené moarové vazbě. Na přebalu byl zlatem vyražen erb Ruska (dvouhlavý orel) a nadpis zlatými písmeny „Ključ Boennogo ministerstva. Lit. M“. Tato knížečka byla chráněna speciálním futrálkem – koženým košíčkem. Jednalo se o dosti složitý substituční systém, jehož popis by přesahoval rámec tohoto traktátu.

Druhým systémem byl „Osobyj šifr No 1-j (čti pěrvoj) Gosudarja Imperatora“, což byl kód s přešifrováním. Přešifrování se provádělo dvoumístným heslem, které se periodicky měnilo po každých 19 znacích podle lineárního pravidla. Kód se skládal ze 13 tabulek, z nichž každá měla 99 položek. Šifrování i dešifrace bylo opět relativně složité, takže pan imperátor by musel být docela zběhlý šifrér, ale spíš na to měl lidi.

Ještě se zachoval jeden šifrový systém, který používal car Nikolaj II. Byl to kód o rozsahu 10000 slovníkových položek. Skládal se ze dvou knih první označené „Nabornyje tablici“ a druhé označené „Razbornyje tablici“. Obě měly rozměry 16,5x22 cm s višňově moarovou vazbou se zlatým tiskem. Použití kódu opět tradičně není nijak jednoduché. Carovi se však musely dokladovat všechny záležitosti, které se týkaly používání imperátorských šifer, což provádělo Ministerstvo vojenství.

Použitá literatura:

Sokolov Nikolaj Alexejevič: Zavraždění carské rodiny, Praha-Vršovice, Josef Šrámek, 1926
Soboljeva Tatjana: Istorija šifrovalnogo dela v Rossii, Moskva, OLMA-PRESS, 2002

F. O čem jsme psali v říjnu 2000 – 2008

Crypto-World 10/1999

Crypto-World 10/2000

Příloha : ZoEP.htm
Dnešní užitečnou přílohou je plné znění zákona č.227/2000 Sb.- "Zákon o elektronickém podpisu a o změně některých dalších zákonů (Zákon o elektronickém podpisu)", který nabyl účinnosti 1.10.2000.

Crypto-World 10/2001

Příloha : Vyhláška 366/2001 Sb. (366_2001.pdf)
(prováděcí vyhláška ÚOOÚ k Zákonu o elektronickém podpisu č.227/2000 ve tvaru předaném k vyhlášení ve Sbírce zákonů)

Crypto-World 10/2002

Crypto-World 10/2003

Crypto-World 10/2004

Příloha : J.Pinkava - Hashovací funkce v roce 2004 , hash_2004.pdf

Crypto-World 10/2005

Příloha : Další informace k článku V.Klímy - prilohy.zip (53 kB)
(Obsahuje: Žádost a podpisy odborníků, Návrh Šámal, Návrh Smejkal, Návrh VK_IURE, překlad části úmluvy, průvodní dopis vk_iure, link psp, stenozáznam jednání PSP, tisk zpráva ČTK)

Crypto-World 10/2006

Příloha: doprovodné materiály k Soutěži v luštění 2006 - vystava.pdf , epilog.pdf

Crypto-World 10/2007

Crypto-World 10/2008

Příloha: simulátor historického šifrátoru Lorenz SZ 40- lorenz.zip.enp

Crypto-World 11/2008

Crypto-World 11/1999

G. Závěrečné informace

1. Sešit

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

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

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

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/