Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 10, číslo 3/2008 **15. březen 2008**

3/2008

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1225 registrovaných odběratelů)

Obsah :

Příloha: ---

A. E-zin 3/2008 a Voynichův rukopis

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

Vážení čtenáři,
dnešní číslo je prakticky celé věnované historii šifrování. Pokračuje zde seriál o Československých šifrovacích zařízeních z období po druhé světové válce a to konkrétně technickým popisem šifrátoru ŠD-2.

Většinu prostoru zde však věnujeme Voynichovu rukopisu (VM). Důvodů, proč se zrovna tomuto záhadnému rukopisu věnujeme zde tak rozsáhle, je více.
Především jsem na podzimním (mezinárodním workshopu MKB (http://bsulab.mkb.org/) s údivem zjistil, že i mezi touto zasvěcenou odbornou komunitou ne každý příběh spojený s pokusy odhalit záhadu VM zná. Přitom v průběhu celého dvacátého století bylo mezi kryptology zvykem se mu věnovat a pokusit se jej dešifrovat (za všechny alespoň citujeme pokusy Friedmana nebo CIA). Je sice pravda, že v současnosti se objevilo několik článků, které popisují, jak by obdobný dokument šlo vytvořit na bázi statistických závislostí a tedy se z toho vyvozuje, že jde o podvrh (hoax). Osobně jsem se dříve k této hypotéze přikláněl. Jenže články, které jsem na toto téma v nedávné době prostudoval, mne příliš nepřesvědčily. Osobně se mi zdá, že zde uváděné postupy jsou příliš komplikované a sofistikované a pokud někdo dokument v 17. století padělal, neměl nejmenší důvod takto složitě postupovat…

Již delší dobu na toto téma komunikuji s jedním s předních badatelů zabývajících se VM - panem J. B. Curychem, Čechem, který žije již delší dobu v Kanadě. Jím dosažené výsledky nejsou vůbec zanedbatelné o čemž svědčí to, že jsou citovány v heslu o VM v anglické verzi Wikipedie. Jak jistě víte, být ve Wikepdii to již něco znamená! Z tohoto důvodu jsem se s ním domluvil a postupně zde otiskneme jeho některé články z poslední doby, které naznačují, že s oficiální historií rukopisu (tedy alespoň s počátkem jejího vzniku) nemusí být vše úplně v pořádku. Je možné, že právě odhalení všech souvislostí, vazeb a vztahů mezi osobami, které jsou s počátkem VM spojeny, možná vnesou novou krev a stopy do jeho zkoumání.

A úplně na závěr doplním, že jsou zde informace k VM uvedeny i jako úvod ke článku, který bychom chtěli s Vlastimilem Klímou na toto téma napsat někdy na podzim (nebo dříve?). O vánocích 2007 jsme na téma VM podiskutovali, vyslovili nějaké hypotézy a během ukradených večerů v průběhu nového roku jsme je zase zavrhli. Tím nás VM dokonale "zaháčkoval" jako mnoho dalších badatelů. Pokud se chcete na VM podívat blíže, musíme vás upozornit, že je to z tohoto důvodu nebezpečné. Pokud mu propadnete, přejeme vám mnoho štěstí s luštěním ☺.

Začneme nejprve stručnou vstupní informací o VM, která je pouhou citací z knihy:

Vondruška, P.: Kryptologie, šifrování a tajná písma, OKO, Albatros, Praha 2006

1912

Americký sběratel Wilfrid M. Voynich objevil v roce 1912 v italském městě Frascati jednu z nejpodivnějších knih, která od té doby, tedy již téměř sto let, nedá spát lidem, kteří se zajímají o záhady. Dílo se podle něj nazývá Voynichův rukopis. Odvezl je do USA a poskytl rukopis odborníkům na kryptologii, aby se pokusili jej rozluštit. Ale pokusům o dešifrování tato kniha stále odolává. Není znám autor, doba vzniku, písmo ani jazyk, ve kterém je dílo napsáno.

Rukopis vyhlíží (má vyhlížet ?) jako práce z 13. století, a to podle použité kaligrafie, obrázků, materiálu, na němž je napsáno, a různých starodávných pigmentů.

Kniha má malý formát, ale je poměrně tlustá, má kolem 240 listů. Je bohatě ilustrovaná, ale jinak než ostatní středověké iluminované rukopisy. Obrázky vyhlížejí jako obrázky z vědecko-fantastické literatury. Má několik různých oddílů věnovaných např. botanice, zoologii a astronomii. Je plná kreseb rostlin, které z přírody neznáme. Jsou zde dále zobrazeny např. malé postavy, které se brodí jedovatě zelenými tůněmi, napájenými potrubím, připomínajícím tepny… Součástí je i rozsáhlá astrologická sekce s nákresy nebe, hvězd a zvířetníků.

Historie rukopisu je velmi nejasná. Poprvé se objevil u anglického učence Johna Deea, který byl prokazatelně jistou dobu na dvoře císaře Rudolfa II. Rukopis prý od něj tento panovník koupil za tehdy obrovskou částku 630 dukátů (asi 3,5 kg ryzího zlata). Po smrti císaře Rudolfa II. se rukopis dostal neznámým způsobem do rukou Jakuba Hořického (v originále Jacobus Horczicky de Tepenec). Toto je také první potvrzený majitel a jeho jméno je v rukopisu uvedeno (něco na způsob současného ex libri). Po jeho smrti (1622) se osud rukopisu stal neznámým a další zmínka pochází až z poloviny sedmnáctého století, kdy spis poslal doktor Marci (Joannus Marcus Marci de Kronland – rektor Karlovy univerzity) svému příteli, jezuitskému knězi a vědci Anastasiovi Kircherovi. Současně se spisem poslal i dopis, z něhož plyne, že rukopis koupil císař Rudolf II. Habsburský a že autorem spisu může být františkánský mystik a přírodovědec Roger Bacon, který žil ve třináctém století.

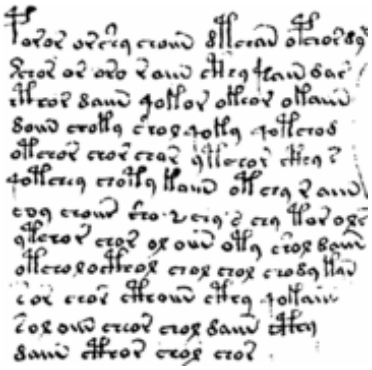
Tento dopis našel společně s rukopisem Voynich. Všechny výše zmíněné osoby prokazatelně existovaly a dopis je také originální. Od té doby byl rukopis pravděpodobně až do svého objevení po celou dobu v Itálii. V současné době je umístěn v Beineckově knihovně vzácných knih a rukopisů Yaleovy univerzity v New Havenu, pod označením MS 408.

B. Voynichův rukopis (Wikipedia)

Používá materiál z http://cs.wikipedia.org/wiki/Voynich%C5%AFv_manuskript
článku „Voynichův manuskript“

Voynichův manuskript

Voynichův manuskript (také Voynichův rukopis apod.) je záhadná ilustrovaná kniha, napsaná neznámým jazykem a v neznámém písmu. Byl pravděpodobně napsán mezi léty 1450 - 1520. Jedná se o objekt zájmu mnoha vědců. Kniha je pojmenována po Wilfridovi Michaelu Voynichovi, obchodníku s knihami, který rukopis získal v roce 1912. V současné době je text ve vlastnictví Yale.



Ukázka neznámého písma

Popis

Kniha patrně měla asi 272 stran v 17 arších, dochovalo se jich ale jen 240. Kniha je psána na pergamenu. Text je psán neznámým písmem (o 20 - 30 znacích s jednoduchou interpunkcí) a neznámým jazykem. Celá kniha má asi 35 000 slov, existují evidentně určitá pravidla, jaké grafémy následují po jakých grafémech, což svědčí o určitých pravopisných a gramatických pravidlech. Statistická analýza textu svědčí o tom, že pro použitý jazyk platí Zipfův zákon, průměrná délka každého slova je zhruba shodná s latinou a angličtinou. Každopádně jazyk použitý ve Voynichově manuskriptu je zcela odlišný od evropských jazyků, nicméně některé znaky svědčí o podobnosti se semitskými jazyky. Několik slov v rukopise je také psáno latinkou, a to jazykem, připomínajícím středověké jazyky oblastí kolem Středozemního moře. Je ale možné, že latinkou psané pasáže byly dopsány až později. Podle ilustrací se kniha dělí na několik částí, je pravděpodobné, že jde o traktát či traktáty z několika oblastí:

- Botanická část. Ilustrace obsahují obrázky běžně vypadajících evropských rostlin. Většina z nich je ale obtížně identifikovatelná, některé jsou dodnes zcela neidentifikovatelné.
- Astronomická část. Ilustrace obsahují astronomické diagramy, astrologické diagramy a symboly, náčrty zvěrokruhu. K některým diagramům jsou dopsány názvy měsíců v roce latinkou, a to v angličtině.
- Biologická část. Ilustrace zobrazují většinou miniatury nahých žen, koupajících se v jakýchsi podivných útvarech, některé z nich připomínají tělesné orgány. Některé z žen mají koruny.
- Kosmologická část. Ilustrace vzdáleně připomínají mapy jakési podivné krajiny či kosmologické náčrtky. Zobrazeny jsou hrady, snad sopky.
- Farmakologická část. Ilustrace zobrazují části rostlin (kořeny, listy), snad jde o farmaceutické recepty, o čemž může svědčit i to, že text je v této části rozdělen na krátké odstavce.
- Recepty (?). Bez ilustrací, text je rozdělen na krátké odstavce, oddělené odrážkami ve tvaru květu či hvězdy.

Historie

Text je dosud nerozluštěn, jeho historie je velmi kusá.

Jediný způsob, jak určit dobu vzniku knihy, je z účesů, oděvů a hradů zobrazených na ilustracích. Jak už bylo řečeno, doba vzniku je odhadována na období 1450 - 1520.

Prvním doloženým vlastníkem byl v Praze žijící alchymista Georg Baresch, žijící na počátku 17. století. Tento alchymista ale očividně nevěděl, jak knihu rozluštit, protože o ní prohlásil, že „mu jen neužitečně zabírá prostor v knihovně".

Po jeho smrti rukopis získal lékař a rektor Karlovy univerzity, učenec Jan Marcus Marci, který knihu zaslal učenému jezuitovi Athanasiu Kircherovi, odborníku na koptštinu.

Není známo, jaké informace Kircher o manuskriptu zjistil. Rukopis byl uložen v knihovně Papežské univerzity Gregoriany. Po následujících 200 let o knize nejsou žádné záznamy, nese však ex libris jezuitského učence Petera Jana Beckxe (1795 - 1887), kromě jiného rektora dotyčné univerzity, což může svědčit o tom, že se kniha přesunula do jeho soukromé knihovny, z níž byla v roce 1866 vykoupena jezuitským řádem.

V roce 1912 byla odkoupena již zmiňovaným knihkupcem Voynichem, po jeho smrti byl zděděn jeho manželkou, která zemřela v roce 1960, odkázajíc manuskript své přítelkyni Anne Nillové, která ho v roce 1961 prodala antikváři Hansi Krausovi, který ho v roce 1969 prodal Yale University.

Autor

Autor manuskriptu není znám, přestože o něm existuje mnoho dohadů.

Podle Jana Marka Marciho se rukopis pohyboval na dvoře Rudolfa II., který věřil, že jeho autorem je britský teolog Roger Bacon.

Není vyloučeno, že Rudolfu II. rukopis dal alchymista John Dee či jeho známější kolega a spolupracovník Edward Kelley, který je kromě jiného prvním, kdo zaznamenal enochiánštinu, údajný jazyk andělů.

Další teorií je, že Voynichův manuskript je podvrh beze smyslu, vytvořený jedním z majitelů.

Fotografická kopie první strany rukopisu od Voynicha ukazuje latinkou psanou poznámku, která byla později vymazána. Text může být čten jako jméno Jacobj à Tepenece, což by mohlo odkazovat k osobě lékaře Jakuba Hořčického z Tepence, známějšího pod jménem Jacobus Sinapius, který byl osobním lékařem Rudolfa II. a správcem jeho botanické zahrady. Voynich se ale domníval, že Hořčický nebyl autorem Voynichova manuskriptu, ale pouze jeho vlastníkem.

Barschovy dopisy naznačují, že autorem rukopisu byl orientalista Andreas Mueller a že jde o nesrozumitelný podvrh. Právník Rafael Soběhrd-Mnišovský, přítel Jana Marka Marciho, v roce 1618 tvrdil, že objevil nerozluštitelnou šifru, což může vést k domněnce, že Rafael Mnišovský napsal Voynichův manuskript jako názorný příklad své šifry. Pro tuto teorii není žádný důkaz, nicméně některé skutečnosti mohou naznačovat, že Mnišovského z podvrhu podezříval již Marci.

Amatérský kryptograf Leonell Strong se domníval, že Voynichův manuskript je „zvláštní dvojitý systém aritmetických postupů s mnohonásobnou abecedou“ a že text je napsán anglickým botanikem Anthony Aschamem.

Programátor Nick Pelling přišel s teorií, že autorem je italský architekt Filarete a že se jedná o jedno z jeho děl z oblasti inženýrství a že byl určen Osmanským Turkům. Jeho teorie je ale založena spíše na podružných indiciích.

H. R. SantaColoma publikoval teorii, podle níž Voynichův manuskript souvisí s počátkem objevení mikroskopu, jeho autorem je podle této teorie holandský vynálezce a přední alchymista na dvoře Rudolfa II. Cornelius Drebbel.

Kryptolog amerického námořnictva Prescott Currier přišel s teorií, že Voynichův manuskript je dílem dvou či více autorů, z nichž každý užíval jiný dialekt, jazyk či pravopis, nicméně používali stejné písmo.

Obsah rukopisu

Stejně jako u teorií o autorovi rukopisu je mnoho teorií o jeho obsahu a účelu.

Na první pohled by se mohlo jednat o středověký lékopis.

První část je zcela nepochybně herbář, nicméně jen několik rostlin může být zcela určitě identifikováno. Brumbaugh věřil, že jedna z ilustrací zobrazuje slunečnici, tedy rostlinu, vyskytující se v Novém světě. Kresba však není jasná, stejně tak může jít o kopretinu, heřmánek či téměř jakoukoli jinou rostlinu z čeledi hvězdnicovitých. Tato biologická tematika by sice mohla souviset s alchymistickým obsahem, nicméně alchymistické knihy obvykle obsahují speciální symboly a určitý tradiční okruh obrazců, které se ve Voynichově manuskriptu nevyskytují.

Expert na herbáře Sergio Toresella tvrdí, že šlo o tzv. alchymistický herbář - knihu, kterou užívali šarlatáni k oklamání zákazníků, aby působili dojmem odborníka. Tyto herbáře ale většinou byly psány obvyklým jazykem (zpravidla italsky) a běžnou abecedou, šlo by tedy o alchymistický herbář silně netypický.

Je také možné, že by šlo o astronomický či astrologický text či kombinaci, jakýsi sborník traktátů z různých oborů (o čemž svědčí široký okruh témat ilustrací).

Jazyk manuskriptu

Téměř stejné množství teorií je o jazyku, jímž je text napsán.

Kryptografové NSA, pracující s rukopisem v padesátých letech, se přikláněli k názoru, že jde o složitou šifru, přikláněli se k tomu, že šlo o polyalfabetickou substituční šifru, které byly v té době oblíbené. Krom toho Roger Bacon, jeden z možných autorů manuskriptu, byl odborníkem na šifry, v předpokládané době napsání byl mezi evropskými vzdělanci o šifry mimořádný zájem. Proti této teorii hovoří fakt, že manuskript dodržuje Zipfův zákon, což u většiny šifer není možné.

James Finn v knize Pandora's Hope (2004) tvrdí, že jde o vizuálně zakódovanou hebrejštinu. Jakmile jednou, podle této teorie bude manuskript přesně přepsán s použitím tzv. European Voynich Alphabet, tedy evropské voynichovské abecedy, bude možno mnoho slov číst jako hebrejštinu.

Jeden z prvních pokusů o rozluštění manuskriptu z roku 1921, vedený Williamem Newboldem z University of Pennsylvania, tvrdí, že viditelný text je sám o sobě nesmyslný, nicméně smysl mu dodávají drobné značky, patrné při zvětšení, založené na starobylém řeckém těsnopise.

Další teorií je, že manuskript je zaznamenán pomocí steganografie, tj. text je nesmyslný sám o sobě, nicméně význam nesou určité detaily (například druhé písmeno každého slova, počet písmen v řádku a podobně). Některé teorie naznačují, že by se mohlo jednat o Cardanovu mřížku.

Jazykovědec Jacques Guy tvrdí, že Voynichův manuskript je psán exotickým, avšak přirozeným jazykem, nicméně umělou abecedou. Slovní struktura je dle něj podobná sinotibetským jazykům, austroasijským jazykům a tajským jazykům.

Teorie o tom, že jde o živý orientální jazyk, zapisovaný novým písmem, je poměrně pravděpodobná. Tehdejší cestovatelé (zejména misionáři) cestující do Asie totiž považovali tamní písma za příliš složitá, což vedlo k tomu, že se mnohdy pokoušeli vytvořit pro daný jazyk nové, fonetické písmo, většinou založené na latince, byť to není pravidlem. Autorem by pak mohl být evropský misionář, žijící v Asii (což by mohlo souviset s tím, že text byl dlouhou dobu v držení jezuitského řádu, který se misií hojně zúčastňoval) či naopak v Evropě žijící Asiat, vychovaný nějakou misií. Hlavním argumentem pro tuto teorii jsou statistické výzkumy textu (zjevná absence některých jevů typických pro evropské jazyky, jako jsou členy, dále výsledky statistických výzkumů vykazují značnou podobnost s obdobnými výsledky na čínštině). Dále pro tuto teorii mohou mluvit dva velké červené symboly na titulní straně (podobný zvyk existoval v Číně) a některé astronomické obrazce, které údajně obsahují prvky typické pro čínský kalendář.

V roce 2003 oznámil Zbigniew Banasik, že text je psán mandžusky a navrhl přepis titulní strany do latinky s překladem mandžuských slov do angličtiny. Jeho doslovný překlad není příliš srozumitelný, avšak zdá se, že jde o prolog a začátek jakéhosi lékařského receptáře.

Další teorie hovoří o možné glosolálii (tedy mluvení či psaní nesrozumitelným jazykem), kresbě provedené spiritistickým médiem (stává se, že médium napíše text v neznámém písmu).

Leo Levitov tvrdí, že jde o umělý jazyk, vzniklý kombinací staré vlámštiny, staré francouzštiny a staré hornoněmčiny. Jde dle něj o liturgickou příručku sekty albigenských.

Mnoho teorií samozřejmě tvrdí, že jde o falzum.

Švýcarský skladatel Hanspeter Kyburz četl Voynichův manuskript jako hudební záznam a založil na něm jedno ze svých hudebních děl.

Externí odkazy

Galerie s vysoce kvalitními skeny stránek Voynichova manuskriptu
http://beinecke.library.yale.edu/dl_crosscollex/SetsSearchExecXC.asp?srchtype=ITEM
Voynich Central http://voynichcentral.com/
Velmi obsáhlé stránky o Voynichově manuskriptu
http://www.voynich.nu/index.html

Citováno z http://cs.wikipedia.org/wiki/Voynich%C5%AFv_manuskript

C. Záhadný Dr. Rafael Jan Hurych

V tomto článku se budu zabývat osobou Dr. Rafaela Mnišovského, známého tím, že dodal „informaci“ rektorovi Janku Markovi Marků (v latině Ioannes Marcus Marci), uvedenou v dopise Marciho Kircherovi, doprovázejícím zásilku Voynichova rukopisu (dále VM). Podle Wikipedie (anglické verze, ale opakováno ve francouzské, španělské a české):

. . . Právník Rafael Soběhrd-Mnišovský, přítel Jana Marka Marciho, v roce 1618 tvrdil, že objevil nerozluštitelnou šifru, což může vést k domněnce, že Rafael Mnišovský napsal Voynichův manuskript jako názorný příklad své šifry. Pro tuto teorii není žádný důkaz, nicméně některé skutečnosti mohou naznačovat, že Mnišovského z podvrhu podezříval již Marci (toto je citát z české Wikipedie; na anglické je toho více, ale zdroj informace není uveden ani v jedné z verzí, j.h.).

Na první pohled to vypadá jako nereálná historka, ale než ji budeme diskutovat, řekněme si něco o samotném Mnišovském. Marci ho jmenuje jen Dr. Raphael, ale protože udává, že učil češtině malého Ferdinanda III., je jasné, že jde o něj. Z toho také lze usoudit, že Kircher věděl, o koho jde, stejně jako věděl o Barešovi, kterého sice také Marci nejmenuje, ale který předtím poslal Kircherovi dva dopisy, z nichž jeden se dokonce zachoval.

Z českých pramenů víme, že se jmenoval ***Soběhrd-Mnišovský*** (v anglické literatuře je často chybně jmenován Mishowsky). Soběhrd bylo jeho původní jméno, které si ale dal změnit na kombinaci obou, patrně aby se odlišil od svých příbuzných, kteří byli vyznáním protestanti. On sám byl zaujatý katolík, který po bitvě na Bílé hoře nemilosrdně pronásledoval protestanty a zabavoval jim majetek.

Jeho život je detailně popsán na stránce známého luštitele VM René Zandbergena. Nejde nám zde o zopakování celého jeho životopisu ale pouze o detaily, které se váží k VM. Podle českých záznamů se narodil v Horšovském Týně. Z tohoto důvodu informace *Eugenie Berežanskoj* v její práci „The Voynich Manuscript“ (2004), že se narodil v polské rodině, není asi přesná, ledaže by byl jeho rod původně z Polska. Víme, že studoval u Jezuitů v Praze a pak následně v Římě a Paříži. Někde jsem se dokonce dočetl, že studoval také v Krakově. Je opravdu možné, že nějaký čas v Polsku přece jen strávil. Důkaz toho, že polštinu znal velmi dobře, je jeho překlad knihy polského autora *Bartholomea Paprockého* „Diodachos“ (genealogii české a polské šlechty) do češtiny. Ale i zde jsou nejasnosti… Podle českého

vydání této knihy ji ale prý napsal Paprocký sám - Mnišovský prý jen dělal editaci a opravy. Asi se ale nezastavil jen u toho, protože například část o klášterech je přímo podepsaná jen jím samotným.


DIADOCHOS ID
EST SVCCESSIO:
Ginák Poslau
Bartholoměge Vapre
Paprockého Diodachos

Jeho kariéra začala ještě před třicetiletou válkou, ale pak po ní nabrala ještě na větší rychlosti. Šlechtický titul dostal brzo po bitvě na Bílé hoře a to hned měsíc po popravě českých pánů na Staroměstském náměstí. Zúčastnil se násilné katolizace Čech a Moravy, zabavoval pozemky uvězněných protestantů a i exulantů, které se pak prodávaly za babku nebo dávaly darem císařským generálům. Svůj erb dostal v roce 1628. Má dvě vertikálně oddělená pole, levé má tři vodorovné pruhy (červený, bílý a červený), pravé pole je žluté, na něm je poloviční, černý rakouský orel s vyplazeným červeným jazykem. Na vrcholu erbu je přílba s fábory (rakouské, tj. žlutočerné a české, tj. bíločervené) a nad nimi ještě zlatá koruna. Zatímco Sebuzín si opravdu koupil, Horšovský Týn byl jen prázdný titul, asi ho tam dal proto, že se tam narodil. Po té, co se stal královským prokurátorem, byl jmenován i *curator fisci*, tj. žalobcem ve věci zrady generála Valdštejna a hraběte Trčky. Oba byli de-facto zabiti a to bez soudu roku 1634 v Chebu a on měl ospravedlnit jejich vraždu. Je zajímavé, že jen sehnání „správných“ svědků mu trvalo 14 měsíců.

Co se týká jeho literárních schopností, kromě již zmíněné ne zcela jasné práci na knize Paprockého psal také latinské verše, které jsou údajně velmi dobré. Zajímal se o alchymii, obdivoval Michala Sendivogiuse, dlouhodobého alchymistu Rudolfa II. Dokonce mu prý k jeho vídeňskému dvoru doporučil dva alchymisty z Polska (Glaubera a Cypriana Kinnera). Podle českých zdrojů také Mnišovský tvrdil, že studoval 30 let alchymii a vyhledával pro Rudolfa II. rukopisy z různých klášterů (Braunau a Kremsmunster). Zemřel 21. listopadu 1644 a je pochován v kryptě u Sv. Salvátora v Praze, kde byl pohřben již před ním Horčický a kam později uložili i Marciho.

O Mnišovském se nikdy vážně neuvádělo (myslím tím v komunitě luštící VM), že by se věnoval kryptologii. Podívejme se však na toto blíže. Jeho rukopis *„Construction sive strues Trithemiana“* (Konstrukce podle Trithemiova síta, 1628) se dlouho uváděla jen jako učebnice češtiny. Dnes je rukopis uložen v Uppsale ve Švédsku, kam ji švédští vojáci přivezli z okupované Prahy v 17. století. Za tvrzení, že se jedná o učebnici češtiny, může částečně Dobrovský, který ji takto popsal ve své knize „Constructio grammaticae bohemicae secundum methodum thrithemianam a Raphaele Mnishowsky anno 1628“. To také jiní autoři po něm opakovali, např. *Carin Davidsson* v „Johannes Tritemius' Polygraphia als tschechisches Lehrbuch, Cod. Slav. 60 der Universitätsbibliothek in Uppsala“, 1959). Dokonce se objevilo tvrzení, že byla psána Mnišovským pro jeho žáka Ferdinanda III.

Je sice pravda, že v podtitulku Mnišovský skutečně slibuje, že kniha naučí kohokoliv mluvit česky v krátké době: „Qui nullum unquam idiomatis bohemici calluit verbum, per eam in momento scribet convenienter bohemice quantum volet“. Čteme-li dále, zjistíme více. Na to

upozornil výzkumník Rafal Prinke z Polska. Mnišovský totiž říká o knize ještě toto: „Occultus occulti scribendi modus quem nemo mortalium queat penetrareo“ (Metoda tajného písma, které žádný smrtelník nemůže rozluštit). Odtud tedy snad pochází ona poznámka v anglické Wikipedii, že se „chlubil, že vynalezl nerozluštitelnou šifru“. Tato poznámka prozrazuje, k čemu vlastně kniha měla opravdu sloužit.

Na Internetu jsou dostupné dvě stránky z této knihy – viz můj článek „Analýza možných autorů rukopisu VM“. Na kopii nevidíme nic, co by připomínalo nějakou učebnici, spíše vypadá jako nějaký slovník, kde nalevo jsou české výrazy a napravo odpovídající překlad v latině. Co nás ale zaujme, je střední sloupec, kde je vždy jen jedno písmeno a tato písmena jsou pro každý řádek jiná, prakticky je zde celá abeceda, seřazená odshora dolů. Na Internetu jsem našel slovenské zdroje, které považují Mnišovského knihu za první českou učebnici kryptografie.

Napsal jsem tedy svému známému českému kryptologovi *Pavlovi Vondruškovi* a ten mi potvrdil, že vzorek skutečně vypadá jako kódová kniha, a dokonce mne upozornil na podobnou šifru právě od Trithemia zvanou *AVE MARIA*, která nahrazuje jednotlivá písmena originálního otevřeného textu celými kódy! No prosím, i Mnišovský cituje Trithemia, zde se sice jedná o něco složitější variaci (pokud lze objektivně soudit jen ze dvou stránek knihy), ale zdá se, že jsme na správné stopě. Původní šifra Ave Maria sice nedává text, který by měl smysl, ale pro laiky to vypadá jako normální latinská modlitba, protože používá jako kódová slova právě ta, která jsou typická pro modlitbu. Jedná se tedy o ochranu nejen šifrováním, ale i o jednoduchou steganografickou metodu (tedy snahu utajit, že zpráva obsahuje šifrový text). Mnišovský systém předělal na slova česká, ale už vůbec ne náboženského významu, ale spíše slovům z každodenního života. Ovšem každému Čechovi by bylo hned jasné, že to nedává smysl. Navíc na stránce věnované písmenu „a“ jsou např. jen přídavná jména, což by asi hodně pomáhalo i při vyřešení šifry. (Poznámka: používám zde slovo *kód* a *šifra* zcela volně, ne tedy zrovna přesně podle definice. Ale kódu „Ave Maria“ se například všude říká jen šifra a přesto je to jasně kód :-).)

Takže otázka zní: „Byla Mnišovského kniha učebnice češtiny nebo naopak kódová kniha?“ Podtitulek říká vše: šlo asi o to, aby císařský žák vypadal, jako když mluví česky a protože u vídeňského dvora se česky nemluvilo, mohlo mu to docela dobře projít. Skrytý účel knihy byl ovšem jinde, ale to autor nemohl tak přímo napsat. I Trithemius se dostal do potíží se svou knihou tajných písem (on tomu říkal steganografie, která dnes znamená něco zcela jiného).

Co to vlastně ta šifra Ave Maria byla? Pro každé písmeno originálního textu se použilo kódové slovo. Zatímco Trithemius používal pořád stejná slova, Mnišovský jich má 24 pro každé písmeno. Ovšem Ave Maria vypadala nenápadně, díky komplikované latinské gramatice si ji mohli lidé lehce splést s modlitbou k panně Marii (odtud i jméno). Nakonec i církevního znalce latiny to mohlo splést, i tam se drmolí různé výrazy bez logického spojení a často se opakují. Mnišovský to vylepšil tím, že použil pro jedno písmeno pokaždé jiné slovo a tehdy u dvora ne příliš používaný jazyk, češtinu. Tím udělal kostrbaté zašifrované věty ještě méně nápadné, hlavně pro cizince. Je možné, že ještě vymyslel nějaké pravidlo, podle kterého se pro to samé písmeno vybíralo pokaždé jiné slovo na stejné stránce kódovací knihy. Mohl také kódovat jedním slovem hned dvě písmena najednou (tzv. bigramy).

Nahrazovat jedno písmeno celým slovem ovšem znamenalo, že zašifrovaný dopis byl enormně dlouhý. Pokud jsme ale neviděli zbytek Mnišovského knihy, nemůžeme říci, jak dalece byla jeho metoda ještě víc pokročilá, na rozdíl od Trithemia. Ale protože víme, že už Paprockého knihu také vylepšil, dá se tušit, že šel ještě dále. Dekódování, tj. zpětný proces,

byl poněkud pracný, ledaže by na to měl zase nějaký trik. Ovšem takovou knihu jistě nemohl publikovat, pak by jeho „nerozluštitelnou“ šifru mohl použít – a hlavně rozluštit – každý :-). A další otázka: „zůstal Mnišovský jen u toho?“ Žil přece ještě 16 let . . .

Náš objev vede k dalšímu podezření: věděl Mnišovský o VM víc, než jen co Marci cituje ve svém dopise? Mohl být například právě on tím vlastníkem VM před Barešem? Dokonce se zdá, že by „podpis“" Horčického ve VM, který Voynich objevil, mohl napsat sám Mnišovský (více v mém dalším článku, „Ještě o Dr. Rafaelovi“). Nemyslím, že chtěl udělat podvod, jen označit, že před ním vlastnil rukopis Horčický. Dnes už lze ve VM rozeznat jen slovo „Tepenec“, zatímco první slovo, „Jacobi“ (Jakuba) viděl jasně už jen Voynich, neboť chemické poškození rukopisu pracovalo za posledních sto let pořád dál a dál.

Máme zde dokonce určité shody okolností: Horčický a Mnišovský byli současníci (Horčický: *1575, +1622 ; Mnišovský: *1580 +1644). Oba dva byli členy císařského dvora a měli i společné zájmy, například alchymii. Oba, Mnišovský i Bareš, studovali v Itálii a pokud Mnišovský skutečně napsal jméno Horčického do VM, musel zřejmě v té době rukopis vlastnit. A proč ne, přece sháněl Rudolfovi staré rukopisy! Pak by ovšem jeho „historka“ v Marciho dopise byla víc než dvorní klep, ale na druhé straně by to znamenalo, že zřejmě neřekl Marcimu celou pravdu, rozhodně ne tu o jeho vlastnictví rukopisu. Jenže jestliže neřekl celou pravdu, můžeme věřit tomu zbytku, co řekl? A nakolik by celá pravda změnila současnou provenanci (historii původu) rukopisu? Co když opravdu věděl, kdo byl autor VM nebo alespoň kde a kdy byl rukopis napsán? Je tedy vůbec pravda to, co Mnišovský řekl o Baconovi, Johnu Dee a Rudolfovi II.? A jestliže ne, proč to asi říkal? A kdo vymazal Horčického jméno a proč? Opravdu, dost otázek, ale málo odpovědí.

Teď, když víme, že Mnišovský byl natolik zručný v kryptologii, že o ní napsal i učebnici, můžeme se leccos dohadovat. Nejen, že sháněl pro Rudolfa rukopisy, ale při té příležitosti našel i VM, který mu však nedal, ale nechal si ho, protože se snad chtěl pokusit o vyluštění sám. (Šlo by snad i uvažovat nad tím, že napsal VM sám…). Jak dalece se snažil jej vyluštit, to už se asi nikdy nedovíme, ani to, zda skutečně navrhl nerozluštitelnou šifru, jak sám tvrdí (viz výše). Že to nebyla ta v jeho knize, je jasné :-). Pokud můžeme posuzovat, jím popsaný systém vyřešitelný je. Text by byl pro Čecha nápadně kostrbatý, přídavná jména zřejmě nahrazují vždy jen jedno písmeno a nakonec i to, že text je v češtině, by usnadnilo práci při dešifrování. Ovšem už objev, že jeho kniha není učebnice, ale kódová kniha a i to, že to byl možná on, co napsal Horčického jméno do VM, nám stačí k tomu, abychom začali o různých zveřejněných detailech původu VM pochybovat. Rozhodně byl Mnišovský víc, než jen rozšiřovatel dvorních klepů a nakonec i to, že kupodivu věděl, že jeho historka je právě o Barešově rukopisu, je značně podezřelá.

Když Marci citoval Mnišovského, napsal „řekl mi“ a to tedy znamená, že mu to pověděl před rokem 1644 (kdy zemřel). Bareš napsal svůj první dopis Kircherovi v roce 1637, kdy už také VM měl a poslal mu ukázky. Mohl tedy dostat VM od Mnišovského, když tento ještě žil. Bareš znal Marciho už před rokem 1622 a zemřel asi kolem roku 1662. Můžeme z toho usoudit, kdy asi Bareš VM získal? Nejspíše tedy v letech 1622 až 1637. Je také zajímavé, že Mnišovský skončil psaní své knihy v roce 1628, téměř uprostřed tohoto intervalu. Nevím, kdy řekl svou historku Marcimu, ale asi ve stejné době a Marci ji opakuje Kircherovi až v roce 1666, jak detailně si ji asi zapamatoval? Mnišovský také asi neřekl Marcimu, odkud tu historku má, zřejmě asi ne od Bareše, který by ji jinak asi řekl Marcimu sám.

Protože se Mnišovský zajímal a o kryptografii a věděl o VM, tak jistě sledoval další osud rukopisu (a teda i jeho řešení) dost detailně. Jestli to byl on, kdo koupil (anebo jinak získal)

VM od Horčického, mohl se dokonce historku dozvědět i od něj a mohl právě jeho jméno do VM napsat sám. Když pak prodal rukopis Barešovi, mohl předtím jméno Horčického vymazat. Mohl mu sice říci celou historku po pravdě, ale zřejmě to neudělal a neřekl mu vůbec nic. Proč? Možná, že opravdu víc nevěděl. Ani Marci se o Horčickém nezmiňuje. Je vůbec možné, že by nikdo nic o VM nevěděl?

Na druhé straně, pokud Mnišovský napsal VM sám a je to podvrh (*hoax)*, jak se v současnosti často předpokládá a je to uvedeno i ve Wikipedii, pak i jeho historka musela být nepravdivá, patrně už od samého začátku. Zdá se ale, že opravdu autorem VM nebyl, jeho písmo se liší, viz můj článek „Analýza možných autorů rukopisu VM“. Přesto ale mohl alespoň VM vlastnit nějakou dobu. Takže mohl vědět více a to by mohlo dát celou historku původu VM do nového světla.

Odkazy

[1] Hurych, J. B.: THE MYSTERIOUS DR. RAPHAEL.
URL <http://hurontaria.baf.cz/CVM/a19.htm>.

[2] Hurych, J. B.: THE RESEARCH OF THE VOYNICH MANUSCRIPT: The Strategies and the Results. URL <http://hurontaria.baf.cz/CVM/a20.htm>.

[3] Hurych, J. B.: MORE ABOUT DR. RAPHAEL MNISHOWSKY.
URL <http://hurontaria.baf.cz/CVM/a22.htm> .

[4] Hurych, J. B.: ZÁHADNÝ DR. RAFAEL.
URL <http://hurontaria.baf.cz/VM/v2050.htm>.

[5] Hurych, J. B.: JEŠTĚ O DR. RAFAELOVI.
URL <http://hurontaria.baf.cz/VM/v2052.htm>.

D. Z dějin československé kryptografie, část VI., Československé šifrovací stroje z období 1955 – 1960. Šifrovací stroj ŠD – 2 (2. díl).

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

Šifrovací stroj ŠD – 2 byl elektromechanický diskový šifrátor s vlastní tvorbou hesla určený pro šifrování off-line. Do Československa byly v roce 1957 dodány ze SSSR dva funkční kusy tohoto stroje včetně příslušenství s označením CM – I. Rozměry tohoto šifrátoru byly 511mm krát 514mm krát 282,5mm a váha byla 41,5 kg. K příslušenství stroje patřila sada 26 kusů komutačních vložek šifrových disků, transformátor, sada nářadí a nástrojů, sada náhradních dílů a plátěný povlak. Pro uschování a převoz byl šifrovací stroj ŠD – 2 s příslušenstvím uložen ve dvou dřevěných transportních bednách. V první transportní bedně o rozměrech 531mm krát 596mm krát 331,5mm byl uložen vlastní šifrátor, podstavec, ruční klika, transformátor a plátěný povlak. Hmotnost této plné bedny byla 55 kg. Ve druhé transportní bedně o rozměrech 455mm krát 269mm krát 358,5mm byla uložena sada komutačních vložek, sada nářadí a nástrojů a sada náhradních dílů. Hmotnost plné druhé bedny byla 20 kg. Celková hmotnost kompletního zabaleného stroje byla 75 kg.

Šifrátor ŠD – 2 , celkový pohled

Elektrické napájení šifrátoru ŠD – 2 bylo možné ze zdrojů střídavého i stejnosměrného proudu. Uskutečňovalo se buď přímo ze zdroje střídavého proudu s napětím 127 V nebo přímo ze zdroje stejnosměrného proudu s napětím 110 V. Další možností bylo napájení přes transformátor ze sítě střídavého proudu s napětími v rozmezí od 100 V do 230 V. V tomto případě bylo nutno přepínačem na transformátoru nastavit správnou hodnotu pracovního napětí 100V, 110V, 127V, 140V, 160V, 200V, 220V nebo 230V.

Šifrovací stroj ŠD – 2 se skládal z těchto hlavních částí:
Klávesnice
Hnací jednotka
Šifrovací blok
Tiskací a děrovací zařízení
Snímač děrné pásky a dekombinátor
Základní deska (podstavec) stroje

1. Klávesnice

Klávesnice byla určena pro vkládání písmen textů zpracovávaných na šifrovacím stroji ŠD – 2. Při práci klávesnice se spínaly kontakty příslušných elektrických obvodů pro průchod proudu do elektromagnetů tiskacího mechanismu a dále se uskutečňovalo spuštění hlavního hřídele stroje. Do konstrukce klávesnice patřil klávesnicový, spouštěcí a blokovací mechanismus, zajišťovací zařízení, dva bloky dotekových kontaktů a pohyblivý dotekový žlábek. Všechny mechanismy a zařízení klávesnice byly instalovány na společné základové desce klávesnice. Klávesnicový mechanismus měl 26 pák odpovídajících dvaceti šesti klávesám označeným písmeny mezinárodní abecedy, červenou klávesu návrat vozíku NK a klávesu mezerník:

Q W E R T Z U I O P
A S D F G H J K L
Y X C V B N M NK
Mezerník

Každá páka odpovídající písmenové klávese i páka odpovídající mezerníku měla posuvnou lištu se třemi výběžky. Tato lišta byla vedena na dvou čepech zanýtovaných na páce a lišta se na nich mohla volně pohybovat. Na každé liště byly dva z výběžků určeny pro spínání kontaktů, které byly umístěny na dvou můstcích připevněných k základové desce klávesnice. Na předním můstku bylo 14 kontaktů odpovídajících klávesám mezera, W, R, Z, I, P, A, D, G, J, L, X, V, N. Na zadním můstku bylo 13 kontaktů odpovídajících klávesám Q, E, T, U, O, S, F, H, K, Y, C, B, M. Všechny klávesnicové páky byly nasazeny na společné ose a jejich vracení do výchozí horní polohy bylo zajištěno mechanicky pomocí pružin.
Nezávislá klávesa návrat vozíku NK byla určena pro posunutí pohyblivé části vozíku z libovolné polohy do krajní pravé polohy.

Spouštěcí mechanismus klávesnice byl určen pro uvolnění pohyblivého dotekového žlábku a spuštění hlavního hřídele stroje a dále pak pro zajištění dotekového žlábku v základní poloze po skončení pracovního cyklu.

Blokovací mechanismus byl určen pro zablokování kláves tak, aby mohla být v činnosti zmáčknuta nejvýše jedna klávesa. Dále sloužil k zajištění zmáčknuté klávesy ve spodní poloze v době přesunu vozíku.

Zajišťovací zařízení zamezovalo spuštění hlavního hřídele stroje při eventuálním současném zmáčknutí dvou nebo několika kláves. Tento mechanismus byl umístěn pod klávesnicovými pákami naproti specielním nožům nanýtovaným na těchto pákách. Tělesem zajišťovacího zařízení byla lišta, která měla podélnou drážku a příčné drážky pro průchod nožů klávesnicových pák. Uvnitř lišty bylo umístěno 33 páček kyvně zavěšených na osičkách. Každá tato páčka měla na další osičce volně se otáčející rolnu. Na koncích lišty byly upevněny bočnice se stavěcími šrouby opatřenými kontramaticemi. Těmito stavěcími šrouby se nastavovala správná vůle mezi rolnami a noži klávesnicových pák. Při plném zmáčknutí

libovolné klávesové páky odsunul její nůž tlakem s ním sousedící rolny vlevo i vpravo až k dorazům. Rolny byly v této poloze k sobě navzájem těsně přitisknuty a zamezovaly pohybu nožů jiných klávesnicových pák při jejich případném zmáčknutí. Při současném zmáčknutí libovolných dvou nebo více kláves se jejich nože zaklínily mezi rolny a nedovolily dále promáčknout klávesnicové páky, takže nedošlo k jejich doteku se spouštěcími kontakty.

2. Hnací jednotka

Pohon mechanismů šifrovacího stroje ŠD – 2 byl prováděn elektromotorem označeným SL-369U/A1 (zde uvedené označení je přepsáno z azbuky do latinky). Tento univerzální elektromotor pracoval buď na stejnosměrný proud při nominálním napětí 110V nebo na střídavý proud při napětí 127V. Po zapnutí do sítě stejnosměrného proudu pracoval elektromotor jako derivační motor a jeho otáčky se regulovaly odporem 510 ohm zapojeným do budícího vinutí. Při napájení střídavým proudem elektromotor pracoval podle schématu sériového motoru s elektrokontaktním regulátorem. Současně s kontaktem regulátoru se zapojoval regulační odpor 820 ohm a kondenzátor 0,05 mikrofarad. Přepnutí motoru ze stejnosměrného proudu na střídavý a opačně se provádělo výměnou snímací nožové zástrčky na jejímž povrchu bylo uvedeno označení příslušného druhu proudu. Efektivní výkon na hřídeli motoru při práci na stejnosměrný proud byl 30,8W při 3000 otáčkách za minutu a při práci na střídavý proud byl 44W při 4300 otáčkách za minutu. Kotva motoru se otáčela proti směru hodinových ručiček při pohledu ze strany kolektoru, tedy zezadu. Vinutí elektromotoru bylo spojeno s elektrickými obvody devítikontaktní zástrčkou. Při práci elektromotoru na stejnosměrný proud se rychlost otáčení kotvy zajišťovala několikastupňovým odporem zapínaným postupně do obvodu budícího vinutí. Při práci na střídavý proud se vyžadovaná rychlost otáčení motoru a její stabilita udržovala elektrokontaktním regulátorem. Těleso tohoto elektrokontaktního regulátoru bylo nasazeno na konec hřídele elektromotoru ze strany kolektoru a bylo připevněno dvěma stavěcími šrouby.

Hnací jednotka šifrátoru ŠD – 2 se kromě popsaného elektromotoru skládala z hlavního hřídele, tří převodových hřídelů a hřídele automatického posunu vozíku, které byly umístěny na společném tělese náhonu odlitém z hliníkové slitiny. Na tomto tělese náhonu byl upevněn motor a dále šnek spojený s hřídelem elektromotoru diskovou Hardyho spojkou a rovněž mechanismus automatického řízení posunu vozíku. Na tělese náhonu bylo také počítadlo pracovních cyklů stroje, impulsní kontaktní sběrnice, polohovací páka s pružinou a spouštěcí páka pro spouštění hlavního hřídele a vozíku.

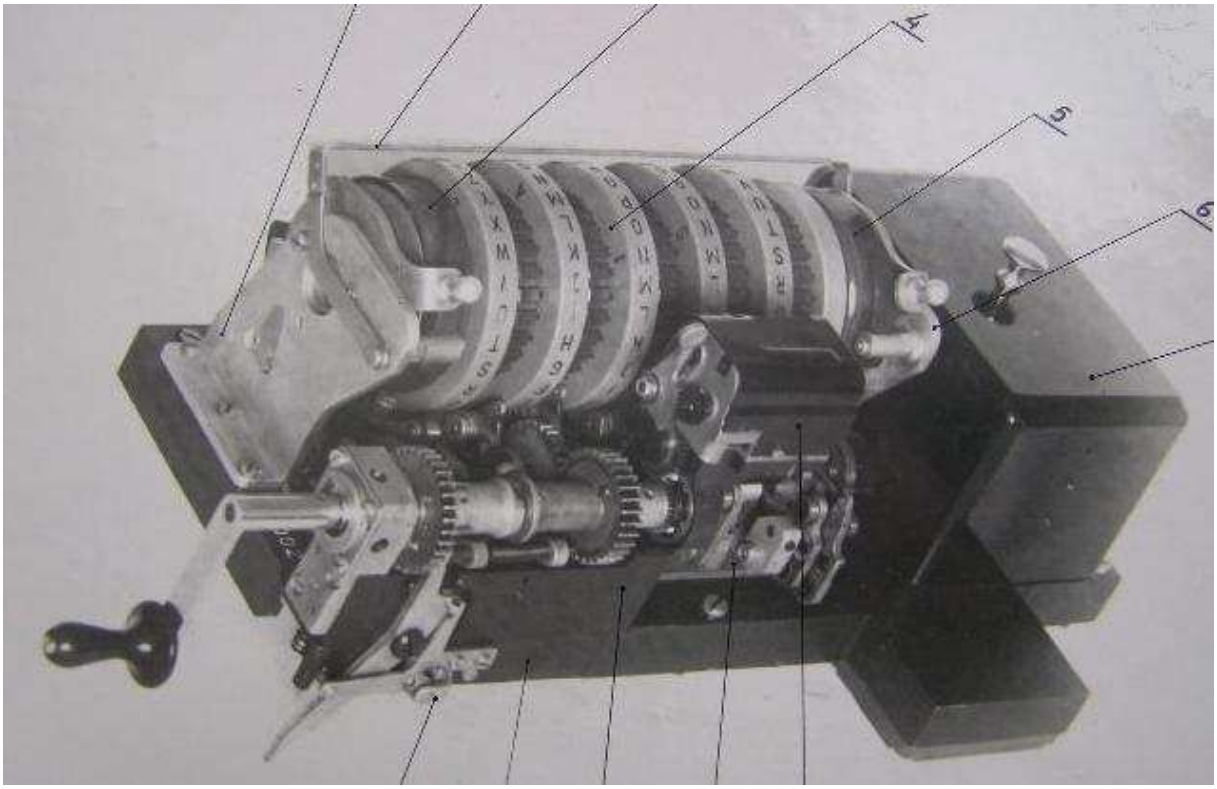
Hlavní hřídel náhonu se uváděl do pohybu od elektromotoru přes šnekový převod s poměrem 1 : 6,4. Šnek byl umístěn v tělese náhonu na kuličkových ložiscích a s hřídelem elektromotoru byl spojen Hardyho spojkou. Šnekové ozubené kolo zabíralo se šnekem šikmozubé ozubené kolo a bylo pevně spojeno s čelem zubové spojky. Hlavní hřídel byl upevněn na tělese náhonu ve dvou kuličkových ložiscích a uváděl se do pohybu pouze po spojení obou zubových čel ozubené spojky. V každém pracovním cyklu stroje uskutečňoval hlavní hřídel jednu otáčku. I ostatní převodové hřídele se otáčely stejnou rychlostí jako hlavní hřídel a každý z nich byl uložen ve dvou kuličkových ložiscích upevněných v tělese náhonu. Hřídel automatického posunu vozíku byl rovněž uchycen ve dvou kuličkových ložiscích a při práci elektromotoru se neustále otáčel v protisměru hodinových ručiček při pohledu ze strany hlavního hřídele. Mechanismus automatického řízení posunu vozíku se uváděl do činnosti pravým čelem pohyblivé části vozíku.

Náhon automatiky se nazýval blok mechanismů umístěný na litém hliníkovém podstavci, který uskutečňoval předávání pohybu od základního náhonu na děrovač a snímač děrné pásky. Všechny hřídele tohoto náhonu se otáčely na kuličkových ložiscích upevněných

na podstavci. Při konstrukci tohoto mechanismu byla použita kardanová spojka a kardanový hřídel, který se při práci elektromotoru otáčel nepřetržitě a s převodem 1 : 1 předával otáčivý pohyb hřídeli snímače a jednootáčkové spojce hřídele k náhonu děrovače.

3. Šifrovací blok

Šifrovací blok sloužil k převodu otevřeného textu na text šifrový při šifrování a k převodu šifrového textu na otevřený text při dešifraci. Přeměna textů se uskutečňovala cestou elektrických impulsů, které procházely od kontaktových sběrnic klávesnice k elektromagnetům tiskacího mechanismu přes elektrické obvody šifrátoru, jejichž schéma zapojení se měnilo po každém kroku zašifrování jednoho znaku. Při práci pouze s otevřeným textem, pomocí přepínače druhů práce, se tyto šifrovací obvody vypínaly ze společného elektrického schématu stroje a mezi příslušnými kontakty klávesnice a tiskacím mechanismem se nastavily přímé elektrické cesty. Vnější vzhled šifrovacího bloku při pohledu zezadu s nasazenou ruční klikou je znázorněn na přiloženém obrázku. Zde je vidět, že na podstavci šifrového bloku byl upevněn reversní (tedy obousměrně vratný) náhon s nasazenou ruční klikou, který končil pohybovým mechanismem. Nad pohybovým mechanismem bylo počítadlo znaků a skupin. Pod hřídelem reversního náhonu je vidět blokovací zařízení.



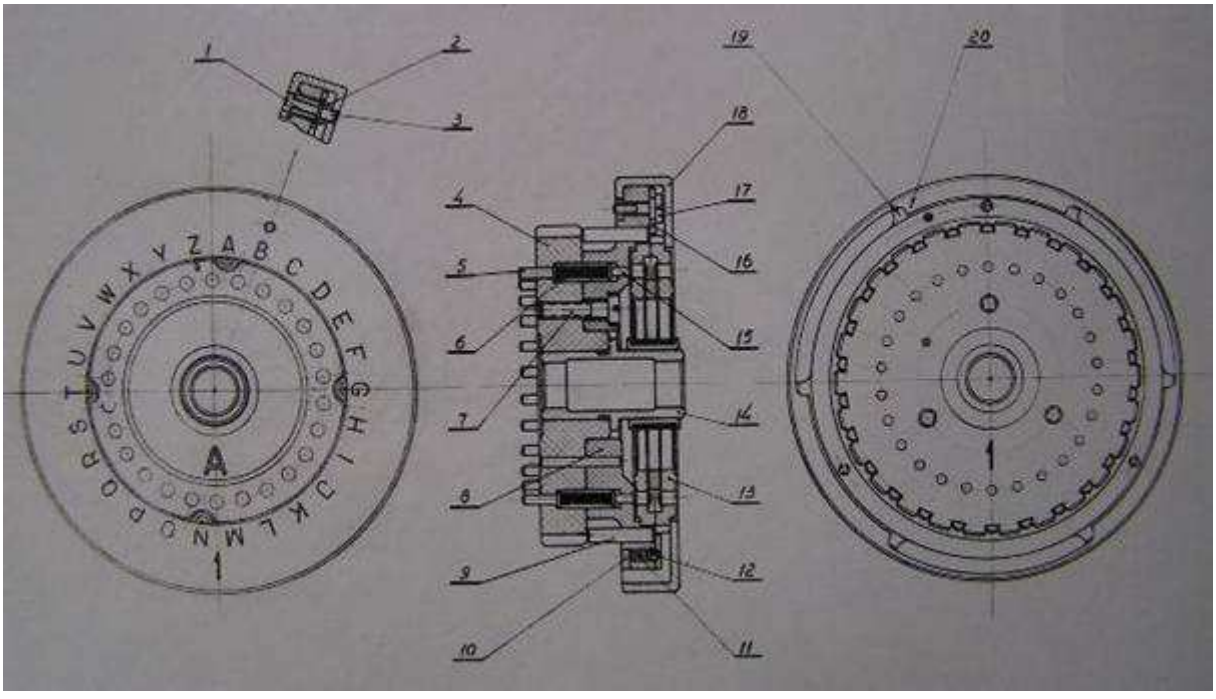
Šifrovací blok

Blok disků měl na každé straně bočnici, ke které byl připevněn nepohyblivý disk. Mezi těmito pevnými disky byl na snadno vyjímatelné ose umístěn pracovní komplet pěti pohyblivých šifrových disků. Za blokem disků je vidět blok komutátoru opatřený krytem. Pod blokem komutátoru byl zespodu na podstavci šifrovacího bloku čtyřmi šrouby připevněn velmi důmyslný přepínač druhu práce, na kterém bylo možno nastavit 3 polohy označené C pro práci pouze s otevřeným textem, Š pro šifrování otevřeného textu a D pro dešifraci šifrového textu. Při práci v režimu C se tímto přepínačem vypínaly šifrovací obvody šifrovacího bloku

z celkového elektrického zapojení stroje a při práci v režimech Š a D se naopak šifrovací obvody šifrovacího bloku zapínaly. Při režimu Š se na klávesnici zablokovala klávesa Q, zapojilo se zařízení na dělení textu na pětimístné skupiny a na hlavní hřídel se připojil hnací mechanismus šifrovacího bloku. Při režimu D se na klávesnici zablokovala klávesa mezery, vypnulo se zařízení na dělení textu na pětimístné skupiny a zablokoval se děrovač pásky.

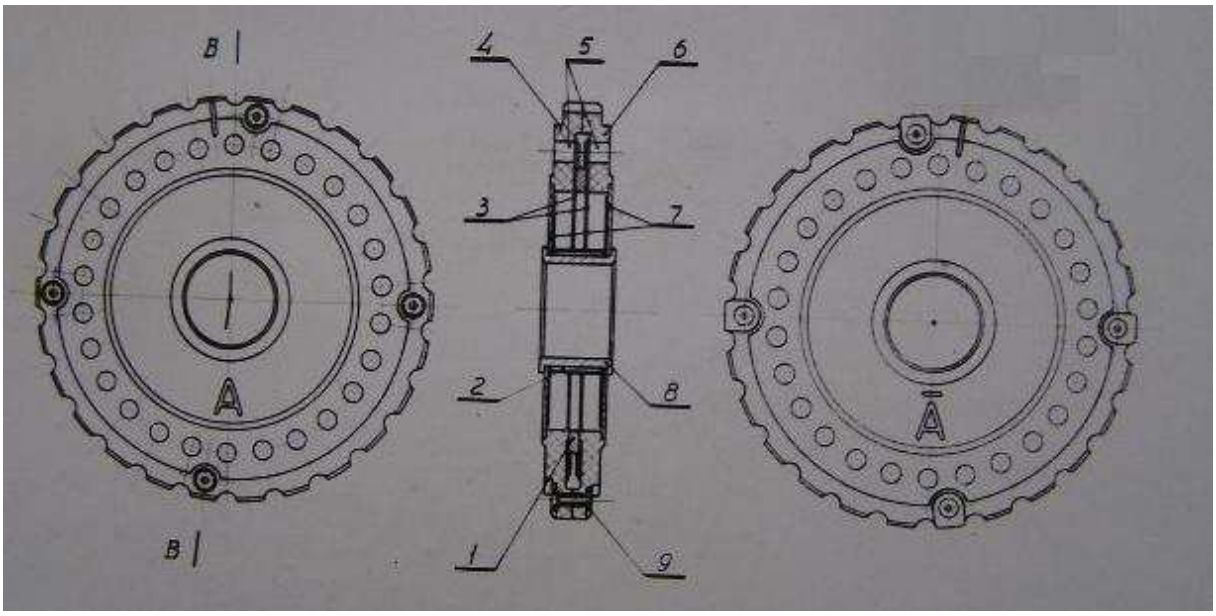
Reversní náhon šifrovacího bloku sloužil jednak pro převádění otáčivého pohybu hlavního hřídele náhonu stroje na hřídel pohyblivého mechanismu šifrovacího bloku a dále pak umožňoval otáčení tohoto hřídele pomocí ruční kliky v obou směrech. Hřídel reversního náhonu se otáčel ve dvou kuličkových ložiscích a jeho první ozubené kolo bylo v záběru s ozubeným kolem hlavního hřídele náhonu stroje. Toto první ozubené kolo vykonávalo v každém pracovním cyklu při libovolné poloze přepínače druhu práce právě jednu otáčku. Druhé ozubené kolo na hřídeli reversního náhonu se mohlo pohybovat v podélném směru a při nastavení přepínače druhu práce do polohy Š nebo D se posunulo do záběru s prvním ozubeným kolem pomocí svého spojkového zubu. Protože toto druhé kolo bylo v neustálém záběru s ozubeným kolem hřídele pohybového mechanismu šifrovacího bloku, zajišťovalo pohyb tohoto hřídele při každém zašifrování či dešifraci jednoho znaku o jednu otáčku. Současně toto druhé kolo předávalo pohyb přes další dvě ozubená mezikola počítadlu znaků a skupin. Při přepnutí přepínače druhu práce do polohy C se pomocí mechanického vačkového a pákového mechanismu toto druhé ozubené kolo posunulo na hřídeli reversního náhonu vlevo a tím vypnulo pohybový mechanismus šifrovacího bloku a počítadlo znaků a skupin. V případech, kdy bylo třeba posunout pohyblivé šifrové disky dopředu nebo je vrátit zpět nebo bylo nutno provést několik cyklů bez pohybu jiných mechanismů šifrovacího stroje ŠD – 2, uváděl se mechanismus šifrovacího bloku do pohybu ručně pomocí odnímatelné kliky. Klika po nasazení a důmyslném zaaretování zaujala volně svislou polohu, která je vidět na obrázku a ve které se obvykle nacházela při práci stroje.

Blokovací zařízení, které bylo upevněno ke spodní části podstavce šifrovacího bloku, mělo vyloučit možnost práce v režimech Š a D při odpojení pohybového mechanismu šifrovacího bloku. K takovým případům mohlo docházet například po neúplném posunu šifrových disků pomocí ruční kliky.



Pohyblivý šifrovací disk - nákres

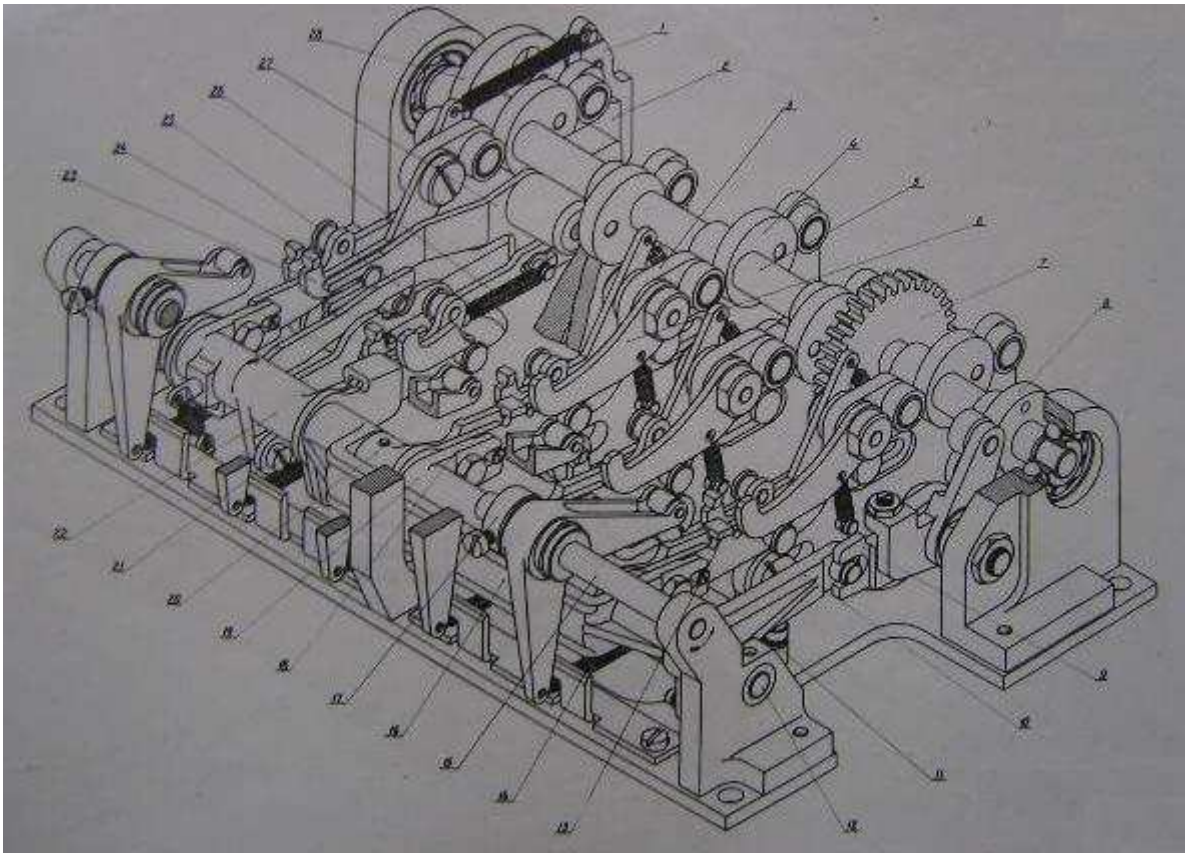
Mezi pevnými disky šifrovacího bloku se nastavovala pracovní sada pěti kusů pohyblivých šifrových disků nasazených na osu v daném pořadí. Každý šifrový disk se skládal ze dvou částí – základního tělesa a komutační vložky. Základní těleso bylo sestaveno ze dvou kruhových částí spojených šroubky. Z vnější strany obou těchto částí bylo rovnoměrně do kružnice rozmístěno 26 pohyblivých pružinových kontaktů vzájemně propojených. Na jedné straně základního tělesa bylo pouzdro, do kterého se vkládala komutační vložka a zajišťovala se aretovacím krytem pouzdra. Na vnějším obvodu krytu pouzdra bylo označení 26 poloh písmeny A až Z. Základní těleso pouze přenášelo kontakt mezi vloženou komutační vložkou v jeho pouzdře a komutační vložkou umístěnou v sousedním pohyblivém nebo pevném disku. Komutační vložka byl disk s 26 zářezy po obvodu, který měl na obou stranách 26 plochých kontaktů rovnoměrně uspořádaných do kružnice. Každý kontakt na jedné straně byl izolovaným vodičem spojen s právě jedním kontaktem na straně druhé, což představuje 26! možností. Obě strany komutační vložky byly k sobě snýtovány dutými nýty a jedna strana byla označena velkým písmenem mezinárodní abecedy, např. A, a druhá strana stejným písmenem s pruhem nahoře. Vodiče uvnitř každé komutační vložky byly ke kontaktům přiletovány a mezi obě strany byla vložena ještě zvláštní izolační vrstva. Komutační vložka se volně nasazovala do pouzdra základního tělesa disku a to buď jednou nebo druhou stranou dovnitř a mohla v něm zaujímat libovolnou z 26 základních poloh. Zářezy po obvodu komutační vložky přitom zapadly mezi výsuvné zoubky, které byly uspořádány do kružnice v otvorech na dně pouzdra v počtu 26 kusů. Vysunutý přitom musel být alespoň 1 zoubek, aby se mohla komutační vložka zaaretovat ve své základní poloze. Maximálně mohlo být vysunuto všech 26 zoubků. Hlavní funkcí těchto výsuvných zoubků bylo totiž řízení krokování šifrových disků.



Komutační vložka – nákres

Při šifrování, resp. dešifraci, v každém pracovním kroku po proběhnutí elektrického signálu diskovou soustavou dvou pevných a pěti pohyblivých disků, ve kterých bylo umístěno celkem 6 komutačních vložek, se vzájemné polohy pohyblivých šifrových disků změnily. Část disků se posunula o 1 nebo 2 polohy a část zůstala stát. Řízení pohybu šifrových disků se provádělo pomocí výše popsaných zoubků, jejichž počet a způsob rozmístění na každém šifrovém disku byl dán zvláštní klíčovou tabulkou. Algoritmus pohybu sady šifrových disků vycházel z počátečního stavu rozmístění zoubků na discích, z pořadí šifrových disků na ose a

z počátečních poloh pohyblivých šifrových disků. Poslední z těchto 3 parametrů byl dán pro každou zprávu tabulkou jednorázových klíčů. Aby bylo možno rozmístit zoubky na disku podle klíčové tabulky, byl opět každý z 26 otvorů pro zoubky na dně pouzdra základního tělesa šifrového disku označen písmeny A až Z, které byly vyryty v kružnici v abecedním pořadí nad otvory pro zoubky. Pro umísťování šifrových disků na osu v určitém pořadí měl každý z nich pořadové číslo od 1 do 5, které bylo vyryto na vnější straně základního tělesa a na krytu pouzdra pro komutační vložku základního tělesa. Ke každému šifrátoru ŠD – 2 bylo dodáno celkem 26 kusů komutačních vložek označených písmeny A až Z z jedné strany a písmeny A až Z s pruhem ze strany druhé. Z těchto 26 kusů komutačních vložek se do šifrových disků vkládalo 6 kusů, z nichž jedna se vkládala do levého výstupního pevného disku a ostatní do pohyblivých disků. Výběr komutačních vložek, jejich umístění do pevného disku a do 5 pohyblivých disků, jejich poloha jednou nebo druhou stranou i jejich základní úhlové polohy v příslušných discích byly dány speciální denní klíčovou tabulkou. Výměna komutačních vložek v discích se prováděla pomocí speciálního náprstku na ukazovák pravé ruky, jehož výstupkem se zatlačila pojistka a ostatními prsty pravé ruky se pootočil a sejmul kryt pouzdra pro komutační vložku. Tento náprstek byl uložen v příslušné přihrádce skříňky pro nástroje a nářadí patřící k šifrovému stroji ŠD – 2. Po sejmutí krytu pouzdra se vyjmula původní komutační vložka a bylo-li to nutné, provedlo se nové rozmístění zoubků. Nová komutační vložka se vkládala do pouzdra tak, aby její strana s označením uvedeným v klíčové tabulce byla otočena navrch, a natočila se do určené základní úhlové polohy tak, aby nastavovací ryska, která byla po obou stranách komutační vložky, směřovala proti příslušnému písmenu z kruhu písmen označujících otvory pro zoubky.



Mechanika krokování šifrových disků – nákres

Pohyblivé šifrovací disky se na ose vkládaly mezi bočnice s pevnými disky. Pevné disky šifrovacího bloku sloužily pro elektrické propojení šifrových disků s komutátorem a

přepínačem druhu práce a jejich pomocí se rovněž uzavírala osa pohyblivých šifrových disků v pracovní poloze. Levá i pravá bočnice byla připevněna třemi šrouby k podstavci šifrovacího bloku a obě bočnice měly duté přírubové osy, na které se navlékaly pevné disky, a do žlábků na koncích těchto přírubových os se vkládala osa s nasazenými pohyblivými šifrovými disky. Levý pevný disk šifrovacího bloku měl v pouzdře umístěnou komutační vložku, která se v něm nastavovala do polohy dané klíčovou tabulkou. Na dně pouzdra tohoto pevného disku byly výčnělky uspořádané do kružnice a označené abecedně písmeny A až Z, do kterých zapadly zářezy vybrané komutační vložky. Pravý pevný disk komutační vložku neměl, měl však stejně jako levý 26 pružinových kontaktů, které byly propojeny s odpovídajícími výstupními zdířkami komutátoru.

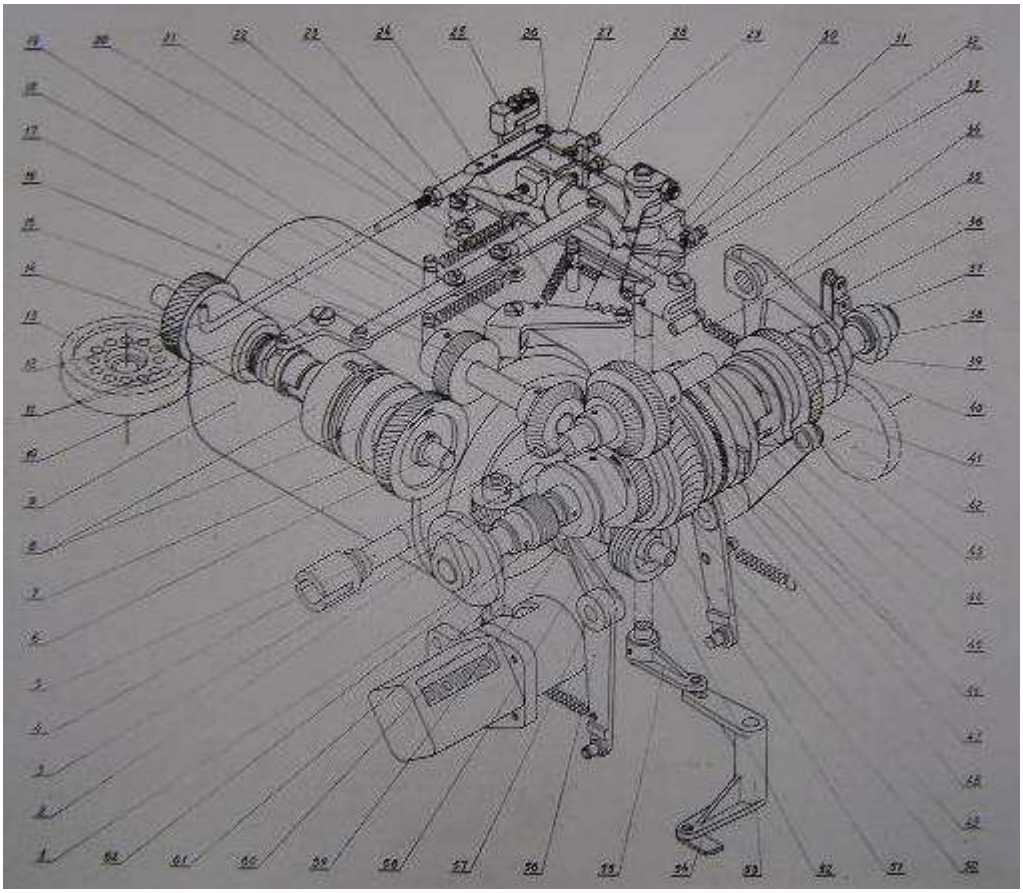
Pohybový mechanismus byl zkonstruován pro zajištění krokování pohyblivých šifrových disků a byl umístěn pod sadou těchto disků na podstavci šifrovacího bloku. Pohyb každého pohyblivého šifrového disku se uskutečňoval pohybovým mechanismem umístěným pod ním a byl řízen prostřednictvím zoubků na discích pomocí systému pák, které byly umístěny na společné ose. Prostřední (tj. třetí) pohyblivý šifrový disk se pootáčel v každém pracovním cyklu stroje o jeden krok, ostatní disky se pohybovaly podle toho, jak byly rozmístěny zoubky na discích o žádný, jeden nebo dva kroky. Přesný popis krokovacího mechanismu je velmi rozsáhlý a nepřehledný, proto jej zde neuvádím. Zoubky na discích byly pomocí ohmatávacích a převáděcích pák mechanicky spojeny s posouvacími pákami a řídily je. Pro nastavení pohyblivých šifrových disků do příslušných základních poloh měl pohybový mechanismus tzv. fixátor, který zajišťoval disky po dobu jejich nečinnosti proti nahodilému pootočení vlivem ohmatávacích pák nebo vlivem tření mezi kontakty sousedních disků při otáčení.

Komutátor byl určen pro komutaci šifrovacích obvodů na vstupu do šifrovacího bloku. Těleso komutátoru bylo 4 šrouby připevněno k podstavci šifrovacího bloku a bylo opatřeno krytem, který byl na tělese spolehlivě zajištěn dvěma planžetovými pružinami. Těleso komutátoru obsahovalo dvě řady třinácti dvojic zdířek. Levá řada dvojic vstupních zdířek byla označena VSTUP a pravá řada dvojic výstupních zdířek označena VÝSTUP. Obě řady dvojic zdířek byly označeny abecedně A až M levé zdířky a N až Z pravé zdířky. Označení bylo vždy na pravé straně příslušné zdířky. Zdířky s označením VSTUP byly vodiči spojeny s kontakty nepohyblivé části přepínače druhu práce a zdířky s označením VÝSTUP byly propojeny s kontakty pravého pevného disku. Každá z 26 zdířek levé skupiny VSTUP musela být kabelem zakončeným banánky propojena s právě jednou zdířkou pravé skupiny VÝSTUP. Propojení bylo dáno permutací uvedené ve speciální klíčové tabulce.

Přepínač druhu práce byl umístěn zespodu na podstavci šifrovacího bloku a byl určen pro přepínání elektrických obvodů stroje do tří režimů buď C nebo Š nebo D. Při režimu C, tj. při práci pouze s otevřeným textem, se šifrovací obvody šifrovacího bloku tímto přepínačem vypínaly ze společného elektrického schématu stroje. Při režimu šifrování Š procházely elektrické impulsy od klávesnice k tiskacímu či děrovacímu mechanismu přes přepínač do obvodů šifrovacího bloku směrem od skupiny zdířek VSTUP komutátoru k levému pevnému disku a při režimu dešifrování D stejnými obvody ale opačným směrem od levého pevného disku ke komutátoru. V přepínači druhu práce jsou dvě nepohyblivé lišty s kontakty a dvě pohyblivé lišty s kontakty. Každá pevná lišta obsahovala 3 řady třiceti kontaktů umístěných vedle sebe ve stejných roztečích. Obě pohyblivé lišty měly 3 řady deseti pružných kontaktů, jejichž rozteč byla trojnásobná oproti rozteči kontaktů na pevných lištách. Kontakty pevných lišt byly spojeny s kontakty levého pevného disku a s kontakty zdířek VSTUP komutátoru. Při práci stroje pak pohyblivé lišty přepínače druhu práce zaujímaly vždy právě jednu ze tří poloh, které odpovídaly režimu práce buď C nebo Š nebo D.

4. Tiskací zařízení a děrovač pásky

Tiskací zařízení bylo podobné jako u elektromechanických psacích strojů. Tiskací mechanismus měl 27 elektromagnetů, z nich 26 řídilo činnost dvaceti šesti písmenových typových pák a jeden mezeru. Všechny typové páky byly osazeny na jedné společné obloukové ose a tiskly pouze velká písmena A až Z. Ve stroji se používala černá psací páska široká 13mm. Pohyb psací pásky ve vodorovném směru zajišťoval mechanismus pro automatický posuv pásky po natištění každého znaku a pro změnu směru pohybu pásky po úplném rozmotání jedné z cívek. Pro držení a posun papíru sloužil tzv. vozík, který měl pevnou a pohyblivou část. Na zadní vodící liště vozíku byl umístěn krokovací mechanismus a mechanismus pro automatické dělení textu na pětimístné skupiny. Na zvláštní otočné konzole byla nasazena stavěcí páka, která zabraňovala opačnému pohybu vozíku vpravo při možných nárazech během práce. Krokovací mechanismus zabezpečoval rovnoměrný krokový pohyb pohyblivé části vozíku podél řádku o pevnou velikost rozteče posunu 2,8mm. Zařízení pro automatické dělení tištěného textu na pětimístné skupiny při režimu práce Š byl sofistikovaný mechanismus, který se skládal z lišty s devíti výstupky, která byla připevněna na pohyblivé části vozíku, a ohmatávací páky, která byla kloubově připevněna na posuvné liště.



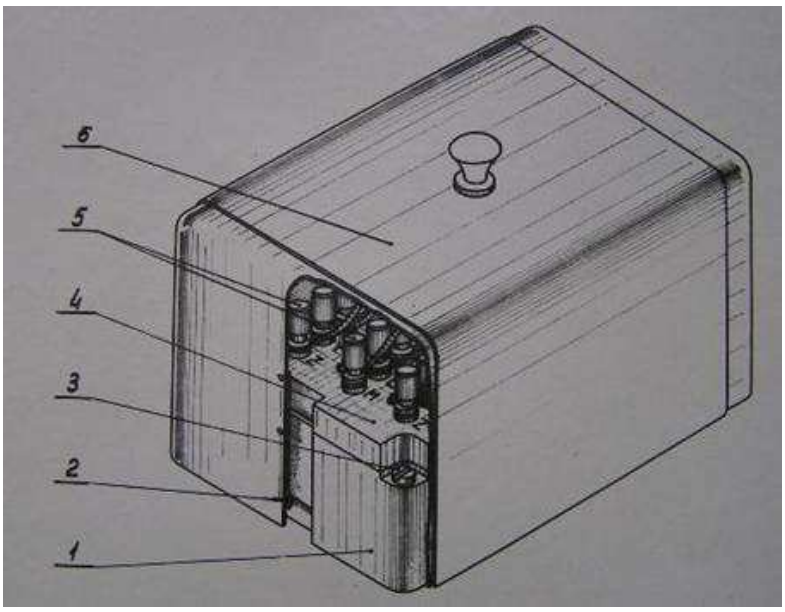
Mechanika hlavního hřídele - nákres

Na podstavci tiskacího zařízení byl upevněn kombinátor, který se skládal z pěti obloukovitých kombinačních lišt upevněných v tiskacím zařízení na dvou osách. Kombinátor umožňoval získávat mechanicky při činnosti každého z 27 elektromagnetů tiskacího zařízení pětibitovou kombinaci příslušného písmene nebo mezery pro děrovač děrné pásky. Používán byl kód MTA-2 odpovídající kódu CCITT 2. K pěti lištám kombinátoru byl připevněn mechanický děrovač pětistopé děrné pásky se šesti průbojníky, které vysekávaly pět stop a jednu vodící. Pohon děrovače byl odvozen z hlavního hřídele stroje. Cívka s děrnou páskou

byla umístěna na podstavci stroje. Napravo na podstavci stroje za přepínačem druhu práce byl umístěn přepínač druhu výstupu se třemi polohami: poloha P – výstup textu pouze děrováním na telegrafní děrnou pásku, poloha PK – stroj tiskne výstupní text na papír a současně jej děruje na děrnou pásku, poloha K – stroj tiskne výstupní text pouze na papír.

5. Snímač děrné pásky a dekombinátor

Snímač děrné pásky převáděl kódové kombinace jednotlivých písmen na mechanický pohyb lišt dekombinátoru, který nahrazoval zadávání příslušného písmene z klávesnice. Hlavní části snímače byly: hlavní hřídel snímače se start/stop spojkou, spouštěcí a vypínací zařízení, zařízení blokující činnost snímače při zpětném pohybu vozíku, zařízení zajišťující zastavení hlavního hřídele snímače při absenci perforace na pásce a zařízení pro posun pásky.



Komutátor - nákres

Snímač se spouštěl zmáčknutím knoflíku PUSK a zastavoval zmáčknutím knoflíku STOP. Ve snímači bylo 5 ohmatávacích kolíků, z nichž každý byl spojen s jednou z lišt dekombinátoru, jejichž pohyb mechanicky nahrazoval zmáčknutí příslušného znaku na klávesnici. Snímač využíval pouze 27 kombinací (kombinace 26 písmen a mezeru) z 32 možných. Zbylých 5 kombinací snímal jako prázdný znak a nereagoval tedy na kombinace písmenové a číselné změny.

6. Základní deska stroje

Podstavec šifrovacího stroje ŠD – 2 představuje základní desku, na níž byly upevněny všechny mechanismy stroje. Podstavec byl z hliníkové slitiny a měl pravoúhlý tvar. Na jeho zadní straně byl namontován elektrický filtr s krytem, který obsahoval 4 kondenzátory a 4 indukční cívky a měl odrušovat elektrické obvody stroje. Na levé straně základní desky byla umístěna krabice pro odpad z děrovače pásky a dále spouštěcí knoflík děrovače. Na pravé straně základní desky byly kromě dvou výše popsaných třípolohových přepínačů ještě dvě objímky pro pojistky (první 1A pro okruh elektromagnetů a druhá 2A pro okruh elektromotoru) a svorka pro uzemění základní desky.

V československé šifrové službě se pro šifrovací stroj ŠD – 2 používal krycí název AMETYST a pro tentýž stroj CM – 1 v SSSR krycí název VASILEK. Protože tento stroj nebyl v Československu nikdy používán, představuje dnes již zcela zapomenutou epizodu.

E. O čem jsme psali v březnu 2000 – 2007

Crypto-World 3/2000

Crypto-World 3/2001

Crypto-World 3/2002

Crypto-World 3/2003

Crypto-World 3/2004

Crypto-World 3/2005

Crypto-World 3/2006

Crypto-World 3/2007

F. 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/