

"Instructions for Cipher Machine "Condenser PBJ"
(Czech Ministry of Internal Affairs) 18 Apr. 1924

SCREENED
R D 68419
By Amu Date 15 Dec 2023

Box # G22-0202-1
00000235450004
Folder # 4
Paper

ACC# 7195M
~~68419~~
~~2162-20~~
~~11/11/1923~~

FOLD

FOLD

Ministerstvo zahraničních věcí v Praze.

Čís. jedn. 2251/Ic/24.

I n s t r u k c e

K š i f r o v é m u s t r o j i

"C o n d e n s e r P B J"

čís. 38....

Přílohy:

- A./ Náčrty stroje.
- B./ Vzorce a příklady.
- C./ Denní hesla.
- D./ Roční hesla.

Do NOT Destroy Return to the NSA Technical Library when no longer needed	
4-69	
C-323	TL Copy No. 1

V Praze, 18. července 1924.

Č.j. 2251/Ic/24.

Věc: Šifrový stroj.

Přílohy: Instrukce.

Vyslanectví Československé Republiky

V

Šifrové oddělení ministerstva zahraničních věcí
zasílá Vám současně šifrový stroj Condenser PBJ No.....
konstruovaný leg. radou ing. P. B a r á č k e m .

Korpus stroje jest uložen v bedničce čís.....

Tajné součástky stroje jsou v balíčku čís.....
v malém dřevěném pouzdře.

m Instrukce k používání stroje o 19 tištěných stra-
nách s přílohami A,B,C a D se přikládají k tomuto přípisu.

Korpus stroje uložte pod jakýmkoliv uzávěrem, tajné
součástky však v nedobytné pokladně /tak jako dosavadní klíče/.

Stroje začněte používatí ihned k šifrovému styku s
ministerstvem zahraničních věcí, ke styku s čsl. legacemi bu-
dete jej používatí, jakmile obdržíte telegram in claris ve
znění: "2251 používejte". Strojem šifrujte zvláště nyní s po-
čátku cca dvě třetiny všech depeší. /Kod, který je nesnadno
vyměnitelný, musí býti šetřen/.

Příjem neporušené zásilky ohlaste ihned telegramem
in claris ve znění: "2251 došlo". Eventuelní závady zjištěné
při dodání šifrujte!

Nastanou-li při šifrování ve stroji poruchy, sejměte
s něho škály a válečky a zašlete korpus k opravě mechanikovi,
který se zabývá správou počítačích strojů.

Za ministra:



INSTRUKCE K ŠIFROVÉMU STROJI.

A/ Příprava textu k šifrování.

Text určený k šifrování se rozepíše do desítimístných skupin týmž způsobem, jak je popsán v návodu k fonetickému klíči tabulkovému v č. j. 38.389/Ic/24 v oddílu B až Be, to jest:

1. / Bigramy pr, př, ch, st, št, sk, šk, ck a čk nahradí se nejméně frekventovanými hláskami dle vzorce v příloze B. / Místo Y píše se všude I. Tečka a čárka nahrazují se značkou KO, otazník značkou CO. Příklady: Místo "stálý" píše se "qali", místo prání - fani, místo škola - wola, práce - face, německý - nemewi, chování-govani atd.

§ 1.

Desítimístné skupiny.

§ 2.

Bigramy a interpunkce.

§ 3.

2. / Text in claris upraví se tak, aby se v něm pravidelně střídaly souhlásky se samohláskami. Fonetisace. Na lichých místech fonetisovaného textu i kryptogramu budou jen souhlásky, na sudých jen samohlásky.

Následují-li tudíž v textu za sebou dvě souhlásky, vloží se mezi ně hluchá samohláska U. Na příklad: Místo "krásný" píše se "kurasuni", místo bez které - bezukutere, místo prostý člověk - foqiculove ku, snad odjede - sunadoduje de, z Argentiny - zarugenuti ni atd.

Hluché U.

Následují-li za sebou dvě samohlásky, vkládá se mezi ně hluchá souhláska X. Na př. se píše místo "dlouhý" - "duloxuhi", vystoupil - viqoxupilu, před odstoupením - fedoduqoxu penimu, proto Anglie - fotoxanugu lixe atd.

Hluché X.

Začíná-li text samohláskou, předešle se hluché X. Na př. místo "ad Vaše" napíše se a pak Začátky a konce.

§ 4.

našifruje "xaduvase". Končí-li text souhláskou, vloží se za ní ještě hluché U. Poslední skupina musí býti též desítimístná. Nedoplňuje se však značkou Ko, nýbrž opakováním poslední slabiky a pak - libovolně. Na př.: Bude-li v poslední skupině slovo "kurýr", napíše a našifruje se kurirurude nebo kuriruruho a podobně.

§ 5.

Dvojznačné hlásky. původní význam /na příklad ve slovech Francie-furanucixe, garancie - garanucixe, Quirinál - quixirinalu, Wilson - wilusomu, atd/, jednak jsou značkami pro často se vyskytující bigramy /na př. pròposice - foposice, štěstí - qeqi atd/. Jsou tudíž dvojznačné a obě eventuality čtení rozeznávají se ze smyslu. Totéž platí o hluchých hláskách U a X, které buď podržují svůj původní význam, nebo se nečtou / na př. ve slovech Xerxes - xeruxesu, koupil - koxupilu atd/.

§ 6.

Vlastní jména.

Klade-li se za vlastní jméno /dle šifrových předpisů str. 12 odst C / číslo, je nutno jím udati skutečný počet hlásek dotyčného vlastního jména a ne jeho počet hlásek po úpravě k šifrování.

§ 7.

Úprava čísel.

Šifrování číslic jest oproti dosavadní praxi /oproti tabulkovému klíči/ z části odlišné. Čísla vyskytující se v textu avisují se dešifréru skupinou NUME, načež se vpíše:

- 1./ Číslice udávající počet míst čísla.
- 2./ Číslo samo v normálním pořadu číslic.
- 3./ Kontrolní číslo t.j. součet jednotlivých číslic šifrovaného čísla, po př. jen jednotky tohoto součtu, je-li větší než devět. Upozorňuje se, že totéž platí i pro čísla o lichém počtu míst /číslíc/. Nula se před tato čísla /jak tomu bylo dosud u klíče tabulkového/ nevkládá.

Druhá změna spočívá v tom, že se při šifrování strojem čísla nefonetisují /viz příklad v příloze B/, t.j. nepřevádějí se na hlásky. Převod by zde byl zbytečný, poněvadž na stroji jsou mimo hlásek též číslice, jež na tabulkách nejsou. Výjimku činí pouze čísla prvé desítimístné skupiny kryptogramu /viz § 18/. Jedině tato se fonetisují dle vzorce v příloze B./

Text následující za číslem se připojí § 8.
 takto: Má-li šifrované číslu lichý počet míst, Text za číslem.
 musí následující po něm fonetisovaný text začínati samohláskou, má-li číslo sudý počet míst,
 začne souhláskou. Neobsahuje-li původní /nezfonetisovaný/ text potřebnou samohlásku nebo souhlásku, upotřebí šifrář na tato místa hluchého U nebo X. /Viz též vzorec "Šifrování číslic" v příloze B./

B./ Příprava stroje.

K dalšímu se předesílá, že pojmenování § 9.
 jednotlivých součástí stroje /zvláště pokud se Součásti stroje.
 jich používá poprvé/ budou v uvozovkách. Umístění těchto součástí ve stroji je následující:
 /Viz též nákres stroje v příloze A./

Na vrchní stěně stroje jsou tyto součásti:

- 1./ "Hřídel" pro kliku na pravé straně.
- 2./ "Knoflík X" na levé straně pod značkou MZV. Posune-li se tento knoflík v levo, vysouvá se současně "zámek" na vrchní hraně.

3./ Pod zámkem je obdélníkový výřez vrchní desky, ve kterém je umístěno 10 lůžek /číslovaných od 0 do 9/ pro "škály" uložené v pouzdře a 10 "stavěcích knoflíků" posunovatelných v drážkách nahoru a dolů.

Na přední stěně stroje jsou tyto součástky:

1./"Vymazavač" /niklovaný/ u pravého okraje posunovatelný ve výřezu na pravo. Do původního postavení vrací se samočinně.

2./ "Okénkový rám" s desíti podélnými a desíti kruhovitými otvory. Uchopí-li se rám /palcem nahoře a ostatními prsty ze spodu/ na levém i pravém konci, vysune se volným, nenásilným tahem ze stroje a odkryje se tak deset "bubíneků", na něž se navlékají "válečky" umístěné v pouzdře.

§ 10.

Tajné součástky
v pouzdře.

Příprava stroje k šifrování záleží v nasazení všech součástek uložených v pouzdře. Připomíná se důrazně, že tyto součástky jsou tajné a musí býti bezpodmínečně po práci neb při každém jejím přerušení, za něhož zůstane stroj bez náležitého dohledu nebo přístupný komukoliv jinému než šifréru, sňaty se stroje a uloženy s pouzdrem tak jako jiné dosavadní šifrové klíče v nedobytné pokladně.

Při nasazování jich postupuje se takto:

§ 11.

Nasazení kliky.

Navleče se klika na hřídel rukojetí vzhůru. Kolíček na hřídeli zapadne do výřezu v klíci.

§ 12.

Uvolnění zámku.

Uvolní se zámek tím, že se knoflík X posune do nejkrajnější polohy v levo.

§ 13.

Vysunutí okénkového rámu.

Odkryjí se bubínky na přední ploše stroje tím způsobem, že se okénkový rám, který je chráněn, nenásilným tahem vysune.

§ 14.

Denní klíč.

V příloze C./ se vyhledá klíč dne, ve který se depeše odesílá /resp. při dešifrování - kdy byla odeslána/. Toto heslo udává seřazení škal a válečků k šifrování resp. dešifrování dotyčné depeše.

§ 15.

Vsazení škal.

Škály vloží se postupně / v seřazení udaném denním klíčem/ na lůžka mezi stavěcí knoflí-

ky prostým zasunutím jich zahrocených konců pod vrchní desku, načež se fixují zámkem t.j. posunutím knoflíku X do původní polohy na pravo.

V tomtéž seřazení navléknou se válečky § 16.
na bubínky tak, aby výřezy v jejich hoření Navlečení váleč-
vnitřním okraji zapadly do kolíčků na bubíncích. ků.
Před nasazováním váleček je nutno vymazati / za-
táhnouti vymazavačem na pravo/, aby kolíčky na bu-
bíncích stály nahoře. Velmi důležité je zkontro-
lovati, zda válečky úplně doléhají k zadní stěně
bubínek. Aby se při šifrování nevyvlékaly, musí Těsnění váleček.
na bubíncích přiměřeně těsniti. Je-li těsnění
příliš slabé t.j. sevrou-li se časem pružné konce
bubínek, bude nutno roztáhnouti je tupým konickým
šídlem uloženým v pouzdře.

C./ Šifrování zfonetisovaného textu.

Vše co je uvedeno v tomto a následujícím § 17. Příklad.
oddílu, je nutno současně sledovati a prakticky
zkoušeti na příkladech v příloze B./

Před prvou desítimístnou skupinou fonetiso- § 18.
vaného textu vpíše se prvá desítimístná skupina Prvá skupina
kryptogramu v této úpravě: kryptogramu.

1./ Na prvá čtyři místa vloží se dvě libovol-
né slabiky s tímto omezením, jehož účelem jest
rozlišiti pro dešifréra depeše šifrované strojem
od depeší šifrovaných kodem a tabulkami:

Depeše šifrované strojem mohou míti v první
slabice pouze některou ze souhlásek od S do Z t.j.
slabiky SA až ZU, poněvadž:

a./ Pro depeše šifrované kodem jest již reser-
vováno používání slabik BE až JU /v první slabice /.

b./ Pro depeše šifrované tabulkami používá se
v první skupině slabik od KA do RU.

Upozorňuje se zde, že je nutno dodržovati tato omezení i při volbě druhé slabiky první skupiny kryptogramu pro případ, že by první slabika byla při telegrafické transmisi zkomolena. Určení použité metody /klíče/ bude tím v druhé slabice potvrzeno a ve sporných případech ušetří se dešifréru zbytečné zkoušení všech tří používaných metod.

Datum.

2./ Na páté a šesté místo vloží se při šifrování strojem datum odeslání depeše převedené dle vzorce "fonetisace číslic" v příloze B./ na zvuknou slabiku, tímto způsobem:

§ 19.

Fonetisace číslic
prvé skupiny.

Prvá z obou číslic nahradí se ze vzorce souhláskou, druhá samohláskou. Poněvadž jsou ve vzorci vedle každé číslice dvě souhlásky /jedna ^{na}pravo, druhá na levo od číslice/, je nutno určit, které z nich použít. O tom rozhodne samohláska pro číslici druhou. Je-li tato samohláska na pravo od číslice, je nutno první číslici nahradit též souhláskou z pravé strany, je-li samohláska na levo, platí i pro první číslici souhláska stojící vedle ní v levo.

Na př.: Jest fonetisovati číslo 29. Vedle číslice 9 jest samohláska jen na pravo t.j. E, číslice 2 nahradí se tudíž také souhláskou z prava t.j. P /29 jest PE/. Obdobně 12 je BO, 25 je CA, 22 je CO, 28- PI, 16-NU, 01-MU, atd

Pořadové číslo
depeše.

3 / Na poslední čtyři místa vpíše se pořadové číslo depeše, fonetisované týmž způsobem, jak uvedeno sub 2./ Je-li toto číslo pouze dvojmístné, vpíše se slabika, která jej vyjadřuje jako pátá. Čtvrtá slabika je v tomto případě zcela libovolná. Je-li pořadové číslo trojmístné, budou čtvrtou slabikou vyjádřeny foneticky stovky čísla. Před jednomístná čísla vkládá se nula. Poslední platí i pro odst. 2 /

Poslední platí i pro odst. 2./

V cirkulárních depeších se pořadové číslo § 20.
nevkládá do první skupiny, nýbrž na konec krypto- Cirkulární
gramu za podpis /nefonetisované/. Pátá a čtvrtá depeše.
slabika první skupiny kryptogramu volí se v tomto
případě zcela nahodile. Důvod: při vložení pořá-
dového čísla, které je pro každého adresáta jiné,
do této skupiny musel by šifrář vypracovati tolik
různých kryptogramů pro týž text, kolik jest
adresátů.

Takto upravená skupina /v příkladě WOSONA- § 21.
LEKE/ "postaví se na knoflících" t.j. knoflíky se Stavění skupin
posunou postupně proti písmenům této skupiny: knof- na knoflících.
lík první proti W na první škále, druhý proti O na
škále druhé atd. Všimněte si však, že písmena O
jsou na této škále /jakož i na všech samohlásko-
vých/ dvě - jedno bílé, druhé červené. Knoflík
posune se tedy proti O té barvy, jakou má předchá-
zející souhláska t.j. W. W je červené, druhý
knoflík posune se tedy proti červenému O. Obdobně
se postaví třetí knoflík proti S na třetí škále.
Poněvadž S je červené posune se čtvrtý knoflík
proti červenému O. Pátý knoflík proti N /červené/
šestý proti červenému A, Sedmý proti L /bílý/ -
osmý tudíž proti bílému E. Devátý proti K /bílý/-
desátý proti bílému E.

Nyní se stáhne palcem vymazavač do nejkraj- § 22.
nější polohy na pravo, načež se uvolní /pustí/. Vymazávání.
Byl-li některý z válečků vytočen, vrátí se touto
operací, která bude v dalším textu krátce jmenová-
na "vymazáváním", do své základní polohy.

Po té se otočí klikou ve směru pohybu hodi- § 23.
nových ručiček t.j. na pravo. Skupina WSONALEKE, Převedení první
byla-li správně postavena na knoflících, objeví se skupiny do oken.
v oknech.

§ 24.

Následuje vlastní šifrování

Šifrování zfonetisovaného textu. Prvá jeho skupina t. j. zfonetisovaného textu. v příkladě vasenum42"postaví se na knoflících; otočí se klikou na pravo a šifra této skupiny GIFARICURU přečte se v oknech a napíše se pod svou příslušnou skupinu textu /pod vasenum42/. Čtení v oknech. Zde je nutno poznamenati, že si v oknech zásadně všímáme jen úplných slabik téže barvy. Souhlásek, vedle nichž v sousedním pravém okně jest jen pomlčka téže barvy / Q-, V-, L-, S-, L-/ si nevšímáme. Týmž způsobem šifruje se i druhá skupina textu a všechny ostatní. Knoflíky postaví se vedle číslic a hlásek skupiny 7537xexupe, otočí se klikou do prava, šifra DAJUHABAGU se přečte v oknech a napíše atd atd.

§ 25.

Stručná rekapitulace:

Stručná rekapitulace šifrování.

Prvou skupinu textu šifruj takto!

- 1./ Postav prvou /zvolenou/ skupinu kryptogramu na knoflících!
- 2./ Vymaž!
- 3./ Otoč klikou na pravo!
- 4./ Postav na knoflících prvou skupinu textu!
- 5./ Otoč klikou na pravo!
- 6./ Přečti v oknech šifru a napiš psacím strojem pod prvou skupinu textu!

Ostatní skupiny textu šifruj takto:

- 1./ Postav následující skupinu fonetisovaného textu na knoflících!
- 2./ Otoč klikou na pravo!
- 3./ Přečti v oknech šifru a napiš!

§ 26.

Jak nejrychleji šifrovati.

Dobře zapracovaný šifrář může si značnou část práce uspořít tím, že text nebude rozepisovati, nýbrž stavěti hned do stroje a pouze výsledky t. j. šifrové skupiny přečtené v oknech bude prepisovati na blanket k odeslání na telegrafní

úřad. K tomuto způsobu šifrování jest ovšem potřebí značné routiny a soustředěnosti. Bez těchto podmínek neuspoří šifrář čas a riskuje přesnost kryptogramu.

D./ Dešifrování kryptogramu.

Postup při dešifrování jest následující:

- 1./ Z prvé souhlásky prvé skupiny se zjistí byla-li depeše šifrována strojem. /S-Z/. § 27. Zjištění metody, klíče a pořad. čísla.
- 2./ Třetí, čtvrtá a pátá slabika se převedou dle vzorce v příloze B./ na čísla, která udají datum odeslání depeše a tím denní klíč a její pořadové číslo.

- 3./ Dle denního klíče v příloze C./ zasadí se do stroje škály a navléknou válečky. Nasadí se klika. Příprava stroje.

Jinak je postup při dešifrování pro všechny skupiny /vyjma prvé/ zcela stejný. Jako nová operace přistupuje zde točení klikou na levo /proti směru pohybu hodinových ručiček/.

Prvou skupinu textu obdržíš takto: § 28.

- 1./ Postav prvou skupinu kryptogramu na knoflících! Vlastní dešifrování, prvá skupina.
- 2./ Vymaž!
- 3./ Otoč klikou na levo!
- 4./ Postav na knoflících druhou skupinu kryptogramu!
- 5./ Otoč klikou na pravo!
- 6./ přečti v oknech prvou skupinu in claris a napiš ji pod druhou skupinu kryptogramu!

Všechny další skupiny textu obdržíš takto: § 29.

- 1./ Vymaž! /předcházející skupinu máš již z předešlé operace na knoflících/. Dešifrování dalších skupin.
- 2./ Otoč klikou na levo!
- 3./ Postav na knoflících nejbližší následující

skupinu kryptogramu!

4./ Otoč klikou na pravo!

5./ Prečti v oknech skupinu in claris a napiš!

E./ Teorie autoklávního šifrového stroje.

§ 30.

K pochopení šifrové metody stroje, které

je nutné k vyloušení omylů při šifrování a při uvědomělém řešení obtížnějších případů zkomolenin v kryptogramech, podává se zde teoretický výklad funkcí stroje:

§ 31.

Algebraická
čísla.

Každé písmeno, s nímž se při šifrování a dešifrování operuje, ať je to již šifra nebo písmeno in claris má v této šifrové soustavě povahu algebraického čísla a přísluší mu tudíž na škále i na válečku stejně označeném /číslovaném/ určitá, stálá číselná hodnota /valeur/. Totéž platí o číslicích používaných při šifrování čísel v textu in claris. Jich skutečná hodnota číselná jest táž jako hodnota písmen stojících na škálách vedle nich v pravo a na válečkách pod nimi.

Příklad: Vlož do stroje na první lůžko škálu čís. 7 a na první bubínek váleček čís. 7. Pozoruj, že písmena i číslice jsou na škále i válečku seřazena stejně. Vymaž!

Na prvním místě ve škále /nahore/ i na válečku v okně jest skupina 4MN. Každý z těchto tří elementů t.j. číslice 4 a písmena M i N mají zde číselnou hodnotu nula.

Podobně elementy:

1, H i Z na 2. místě škály i válečku mají hodnotu 1.			
0, K i X na 3.	dtto	dtto	2.
2, B i P na 4.	dtto	dtto	3.
3, D i T na 5.	dtto	dtto	4.
5, G i Q na 6.	dtto	dtto	5.
8, J i W na 7.	dtto	dtto	6.
9, L i R na 8.	dtto	dtto	7.

6, C i S na 9. místě škály i válečku rovnají se 8.

7, F i V na 10. dtto dtto 9.

Totéž platí pro všechny ostatní škály a válečky stejně označené /číslované/, tedy i pro samohláskové. Všechna čísla i písmena na prvním místě skal i válečků mají hodnotu nula, na druhém místě mají hodnotu 1 /jedna/, na třetím 2, na čtvrtém 3, na pátém 4 atd atd.

Otočíš-li klikou na pravo, přičítáš vlastně hodnotu elementu, u něhož stojí knoflík k hodnotě elementu postaveného před otočením v oknech. Výsledek t.j. součet objeví se v okně zase v algebraické své hodnotě. Překročí-li součet devět, platí jen jednotky součtu. Desítky se na levé, sousedí válečky /na rozdíl od strojů počítacích/ u tohoto šifrového stroje nepřenesují.

Příklady ze škály a válečku čís. 7: Při šifrování příkladu v příloze provádějí škála a váleček čís. 7 tyto početní operace:

$$W + v = 6 - 9 = 15 \text{ t.j. zde } 5 = G \text{ nebo } Q \text{ nebo } 5.$$

$$G - 7 = 5 - 9 = 14 \text{ t.j. zde } 4 = D \text{ nebo } T \text{ nebo } 3.$$

$$D - r = 4 - 7 = 11 \text{ t.j. zde } 1 = H \text{ nebo } Z \text{ nebo } 1.$$

$$H - x = 1 - 2 = 3 = B \text{ nebo } P \text{ nebo } 2.$$

$$B - 2 = 3 - 3 = 6 = J \text{ nebo } W \text{ nebo } 8.$$

Z obou souhlásek platí při šifrování ona, která má vedle sebe na pravo /v okně/ samohlásku téže barvy. Číslice by platily jen tehdy, kdyby kryptogramy měly býti číselné. Poněvadž náklad na ně byl by oproti fonetickým dvojnásobný /slovo by nesmělo obnášeti více než 5 číslic/, jich používání v praxi se nezavádí.

Otočíš-li klikou na levo, odečítáš vlastně hodnotu elementu, u něhož stojí knoflík od hodnoty elementu postaveného před otočením v okně. Výsledek t.j. rozdíl objeví se zase v okně v hodnotě

§ 32.

Algebraické sečítání /při šifrování/.

§ 33.

Algebraické odečítání /při dešifrování/.

algebraické. Důležité jest toto: Odečítá-li se hodnota větší od hodnoty menší, vyjde místo záporného rozdílu jeho kladný doplněk do desíti.

Při dešifrování příkladu v příloze B řeší se strojem na škále a válečku čís. 7 tyto rovnice:

$$-W - G = -6 - 5 = -1 \text{ t.j. zde } 9 = f \text{ nebo v nebo } 7.$$

$$-G - D = -5 - 4 = -1 \text{ t.j. zde } 9 = f \text{ nebo v nebo } 7.$$

$$-D - H = -4 - 1 = -3 \text{ t.j. zde } 7 = l \text{ nebo r nebo } 9$$

$$-H - B = -1 - 3 = 2 = k \text{ nebo x nebo } 0 \text{ /nula/}$$

$$-B - W = -3 - 6 = 3 = b \text{ nebo p nebo } 2.$$

Ve výsledku platí při dešifrování z obou písmen /souhlásek/ vždy ono, které má vedle sebe v okně na pravo samohlásku téže barvy. Předcházela-li v dešifrovaném textu skupina NUME, platí místo hlásek číslice.

§ 34.

Šifrování škála-
mi.

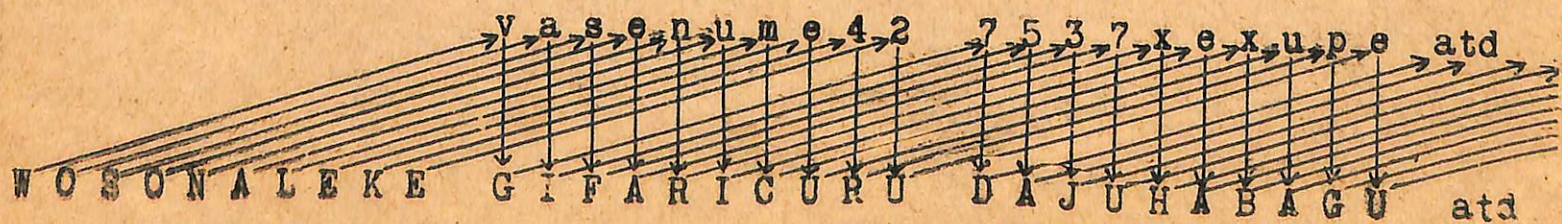
Z toho, co uvedeno v § 32 a 33 vyplývá:

1./ Rovnice v příkladech uvedené, jakož i všechny ostatní při šifrování i dešifrování je možno řešiti na příslušných škálách bez použití stroje. Prakticky není sice možné tohoto zdlouhavého postupu k šifrování používat, jest však nevyhnutelné seznámiti se s ním z důvodů uvedených v § 30.

§ 35.

Řetězy.

2./ Šifry následující za sebou ob deset míst t.j. stojící na témže místě desítmístných skupin, tvoří řetěz, jehož každý článek /šifra/ jest součtem předcházejícího článku /desáté předcházející šifry/ a příslušného písmene in claris. Každá škála a váleček /stejně číslované/ vytvářejí jeden z desíti řetězů, jež znázorňuje toto schema:



§ 36.

Prakticky /ne však matematicky/ lze

aplikovati toto schema a rovnice z něho vyplývající na celé desítimístné skupiny i jejich části na těchže místech skupin a řídit se pak těmito skupinovými schematy a rovnicemi ve všech případech při šifrování i dešifrování.

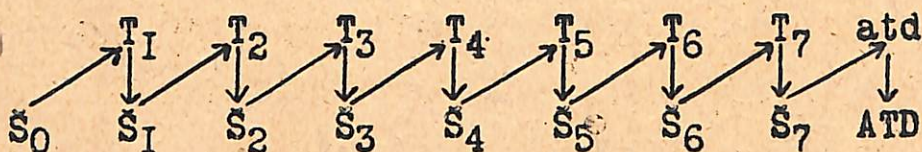
Praktická schéma-
ta a rovnice.

Nazveme za tímto účelem:

1./ Prvou skupinu fonetisovaného textu T_1 , druhou T_2 , třetí T_3 , čtvrtou T_4 atd atd.

2./ Prvou /zvolenou/ skupinu kryptogramu $\bar{S}_0$, a další /našifrované/ postupně $\bar{S}_1, \bar{S}_2, \bar{S}_3, \bar{S}_4, \bar{S}_5$ atd.

Šifrování desítimístných skupin i jejich částí Při šifrování.
bude se dít dle tohoto schéma a těchto rovnic:



$\bar{S}_0 + T_1 = \bar{S}_1, \bar{S}_1 + T_2 = \bar{S}_2, \bar{S}_2 + T_3 = \bar{S}_3, \bar{S}_3 + T_4 = \bar{S}_4$ atd

čili všeobecně:

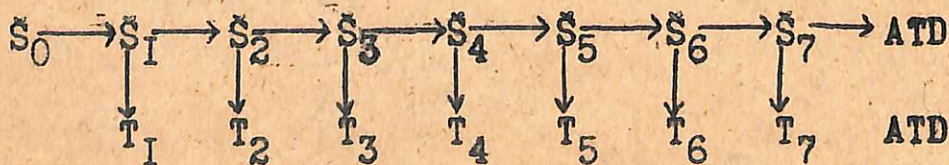
$$\bar{S}_n + T_{n+1} = \bar{S}_{n+1}$$

šifra předcházející skupiny in
claris postavená v oknech

následující skupina in claris po-
stavená na knoflicích přičte se
otočením klikou na pravo

výsledek v oknech t.j. šifra této
skupiny in claris

Dešifrování bude se dít dle tohoto schéma a Při dešifrování.
těchto rovnic:



$-\bar{S}_0 + \bar{S}_1 = T_1, -\bar{S}_1 + \bar{S}_2 = T_2, -\bar{S}_2 + \bar{S}_3 = T_3$, atd atd

čili všeobecně:

$$-\bar{S}_n + \bar{S}_{n+1} = T_{n+1}$$

předcházející skupina posta-
vená na knoflicích se po vyma-
zání otočením na levo odečte

následující skupina postaví se
na knoflicích a přičte /na pravo/

výsledek v oknech t.j. text

F./ Řešení zkomolenin.

§ 37.

Postup při řešení zkomolenin.

Upozorňuje se, že je naprosto nesprávné

a neekonomické přerušovati dešifrování při každé zkomolenině. Nejprve se dešifruje celý kryptogram - zcela mechanicky, bez čtení, potom se přečtou a napíše nebo oddělí jednotlivá slova snadno čitelných partií a teprve po tomto rozluštění zhruba řeší se nesnadno čitelná a zkomolená místa. Valná většina z nich vyplýne ze smyslu rozluštěných partií sama.

§ 38.

Druhy zkomolenin.

Zkomoleniny mohou býti dvojího druhu:

1./ Vzniklé nesprávným šifrováním.

2./ Vzniklé při telegrafické transmisi nebo eventuelním opisováním odesílatelem.

K určení obou druhů zkomolenin a demonstrování, jak se řeší, uvádí se zde kryptogram /zpřílohy B/ na několika místech úmyslně zkomolený.

Kryptogram:

Prvý dešifrovaný text:

Prvý přečtený text:

WOSONALEKE GIFARICURU
vasenum42
Vaše nume

DAJU HABAGU HIFARUFEFU BOGOFEQENE WOBUCUHUJU
7537xexupe rutifijedo xufahinume 2189bunuzu
2753 experti přijedou Prahy nume 18

JINIVIRAWÉ DOZAHOVORO TUKAKUFEVO VURUDOZIPI
nazadahofe sunesuhede nivasedojo guramufopo
2./ přesné 3./ pro

JEZUJEQOGO COMENAGACU
radizaculi xoburatemu
porady 1./ obratem.

§ 39.

Zkomolenina vzniklá špatným šifrováním.

Místa v příkladě zkomolená jsou číslována.

Zkomolenina 1./ vznikla nesprávným šifrováním, což je zřejmo z toho, že se chyba /místo zaculi má býti zasuli t.j. zašli/ nepřenáší na pátou následující nebo předcházející slabiku. Šifrář zde postavil stavěč místo před U červené před U bílé. Chyba takováto dá se opravit jedině správným předpokladem, supposicí /není však možno jiným způsobem než ze smyslu správnost supposice přezkoušeti a potvrditi.

Zkomoleniny toho druhu, jako je 2./a 3./ , § 40.

nemohou vzniknouti nesprávným šifrováním, nýbrž Zkomoleniny
porušením dobře šifrovaného kryptogramu při opi- transmise.
sování nebo telegrafické transmisi. Jsou charak-
terisovány tím, že se chyba přenáší vždy také na
následující skupinu /na totéž místo/. Úkolem je
kteroukoli z obou zkomolenin / buď v první nebo ve
druhé skupině/ správně uhodnouti. Druhá se pak
dešifruje již strojem. Správný výsledek ve druhé
skupině potvrzuje zároveň správnost supposice ve
skupině první.

Příklad: Řešení zkomoleniny 2./ bunuzunazadaho § 41. Zkomole-
nina čís. 2./

Prvý způsob: Podaří se supponovati, že místo

nu má býti re /burezuna = března/. Našifrujeme
7 a 8mou škálou a válečkem správný text /re/ a
zjistíme tak chybu v kryptogramu dle rovnice:

Prvý způsob.

$$\check{S}_n + T_{n+1} = \check{S}_{n+1}$$

t.j. QE + re = NU /místo HU má býti tedy NU/

Chyba v kryptogramu je nalezena a druhá chyba v
rozluštěném textu / v následující skupině/ opra-
ví se dle rovnice:

$$-\check{S}_n + \check{S}_{n+1} = T_{n+1}$$

t.j. -NU + RA = ji /místo zadaho má býti zadaji
t.j. žádají/

Smyslová správnost slova "žádají" potvrzuje správnost
supposice "března".

Druhý způsob: Podaří se správně uhodnouti Druhý způsob.
druhou zkomoleninu t.j. že místo zadanu má býti
zadaji t.j. žádají. Chyba v kryptogramu zjistí se
na 7 a 8 škále a válečku z rovnice:

$$\check{S}_{n+1} - T_{n+1} = \check{S}_n \text{ nebo } -T_{n+1} + \check{S}_{n+1} = \check{S}_n$$

t.j. RA - ji = NU nebo -ji + RA = NU

Místo HU má býti NU a z toho resultuje oprava pr-
vé zkomoleniny: dle rovnice:

$$-\check{S}_n + \check{S}_{n+1} = T_{n+1}$$

t.j. -QE + NU = re

/místo bunuzuna má býti
burezuna t.j. března/.

§ 42. Zkomolenina č. 3. /
Řešení.

Prvé řešení.

Řešení zkomoleniny 3. /suhedenivasedojoguramu:

Prvý způsob řešení: Za slovy "žádají přesné" má
býti pravděpodobně "sdělení" /suhedeni = sudelení/.

Kryptogram opraví se dle rovnice:

$$\dot{S}_n + T_{n+1} = \dot{S}_{n+1}$$

t.j. VIRAWÉ + sudele = HOROVO /a ne HOVORO/

Z toho oprava druhé skupiny dle rovnice:

$$-\dot{S}_n + \dot{S}_{n+1} = T_{n+1}$$

t.j. -HOROVO + KUFEVO = sehofo

Místo sehojo má býti sehofo. Po této opravě je možné ihned přečísti smyslem správný text "Vašeho programu", což zároveň potvrzuje správnost supposice "sdělení".

Druhé řešení.

Druhý způsob řešení: podaří se supponovati, že místo vasedojoguramu má býti vasehofoguramu t.j. Vašeho programu a kryptogram se opraví dle rovnice:

$$\dot{S}_{n+1} - T_{n+1} = \dot{S}_n \text{ nebo } -T_{n+1} + \dot{S}_{n+1} = \dot{S}_n$$

t.j. KUFEVO - sehofo = HOROVO - sehofo + KUFEVO = HOROVO

Místo HOVORO má býti v kryptogramu HOROVO. Dle tohoto výsledku opraví se chyba předcházející skupiny z rovnice:

$$-\dot{S}_n + \dot{S}_{n+1} = T_{n+1}$$

t.j. -VIRAWÉ + HOROVO = sudele /místo suhede - sudele/
Správný výsledek "sdělení" potvrzuje správnost supposice "Vašeho programu".

§ 43. Stanovení zkomol. místa.

Zkomolené místo v kryptogramu stanoví se takto: V dešifrovaném textu se hledí odlišit slabiky správné, markantní tím, že mohou býti částmi slov fonetisovaného textu, od zkomolených, které pravidelně tohoto znaku postrádají. Zkomolené slabiky jsou od sebe vzdáleny o deset míst /pět slabik./ Je-li prvá chyba třetí slabikou ve skupině

je druhá chyba též ve třetí slabice skupiny následující. V kryptogramu je pak nutno hledati chybu nad prvním z obou zkomolených míst /zkomolena je šifra prvního chybného místa /.

G./ Roční klíč.

Součástky škal a válečků, na nichž je po § 44. Lamely. dvou písmenech a jedné číslici, jmenují se "lamelami". Jich seřazení na stejně označených /číslovaných/ škalách a válečcích musí býti totéž. Srovnej na př. škálu a váleček čís. 5. Lamely následují za sebou /na škále shora dolů a na válečku inclusive od výřezu na jeho hoření okraji ve směru pohybu hodinových ručiček - na pravo/ v pořadí 0,2,7,9,5 atd.

Nyní, při dodání stroje tamnímu úřadu jsou § 45. lamely seřazeny dle prvního vzoru v příloze D./ na- Roční klíč a jeho změny. depsaného "Původní sestava". Tato sestava a všechny ostatní v příloze D./nadesané I změna, II změ- Důležité! na atd. nazývají se ročními klíči, poněvadž se jich bude používati beze změny vždy delší čas na rozdíl od denních hesel /seřazení škal a válečků/ v příloze C./ Škálami a válečky bude se za nynějšího "původního seřazení" lamel šifrovati až do té doby, kdy tamní zastupitelský úřad obdrží od šifrového odd. MZV telegram znějící :

" 2251 proved Xtou změnu".

Po obdržení tohoto rozkazu přeřadí šifrář zastupitelského úřadu lamely na škálách i válečcích ihned dle změny v příloze D./ udané telegramem. Roční i denní klíče jsou u všech zastupitelských úřadů /vyslanectví/ podělených stroji stejné. Jelikož se tím risiko prozrazení zvyšuje, je nutno přílohy C./ a D./ zvlášť pečlivě /v nedobytné pokladně/ uschovávat.

Uschovávání klíčů.

Změna ročního hesla /přeřazení lamel/
provede se takto:

Přeřazení skal.

a./ Ve škálách: Vyšroubuje se knoflík /na hořením konci škály/, vysunou se uzávěrka i lamely a tyto se znovu navléknou v novém seřazení dle příslušné "změny" v příloze D./ Upozorňuje se, že je nutno lamely navlékati počínaje poslední číslicí příslušné kolony sestavy tak, aby po navlečení všech pořad lamel ve škále byl totožný s pořadím číslic v koloně sestavy.

Přeřazení válečků.

b./ Na válečcích: Z válečku se odšroubuje kroužek upevňující nahoře lamely a tyto se vysunou. Po té se váleček vloží do "niklovaného bubínku" uloženého v krabici a lamely se znovu navlekou v tomtéž pořadí jako na škálách. Prvá lamela -/na př. lamela 7 u válečku číslo 0/- nasune se do drážky stojící proti výrezu ve vnitřním hořením okraji válečku -/jinak možno říci do drážky proti číslici 0 na rukojeti/. Ostatní lamely nasunou se postupně v pořadí udaném sestavou ve směru pohybu hodinových ručiček t.j. na pravo, při čemž se "niklovým bubínkem" v ruce otáčí ve směru šipky na jeho podstavci t.j. na levo. Na to se lamely upevní našroubováním kroužku. /Aby nevypadávaly, je potřebí dobře je zatlačit do lůžek./

Upozotňuje se, že se nesmějí přemísťovati z jedné škály na druhou nebo z válečku na váleček. Technicky je nemožno vyrobti všechny lamely a drážky v naprosto stejných rozměrech. Přeřazování by tudíž mohlo míti za následek vypadávání lamel užších než jsou drážky. Z toho důvodu nejprve ukonči přeřazení na jednom válečku /škále/, než-li rozšroubuješ druhý, aby se lamely různých skal a válečků nemohly pomíchat.

Pro případ, že by se přes všechnu opatrnost a kontrolu při nasazování a šifrování některá z lamel ztratila upozorňuje se, že lamely téhož čísla mají též stejná písmena na všech škalách i válečcích. Přesvědčí se! Ztráta dala by se tedy provisorně /do zaslání nové lamely šifrovým oddělením MZV/ nahraditi kartonovou vložkou, na kterou by si šifrář sám číslíci a písmena vepsal.

§ 46.
Ztráta lamely.

H./ Některá upozornění o zacházení se strojem.

Stavěče je nutno posunovati přesně proti § 47.

písmenům /číslíci/ na škalách. Stavěč vychýlený ze správné polohy o malou vzdálenost /nepatrně/ vrací se do původní, základní polohy sám. Zacházení se stavěči.

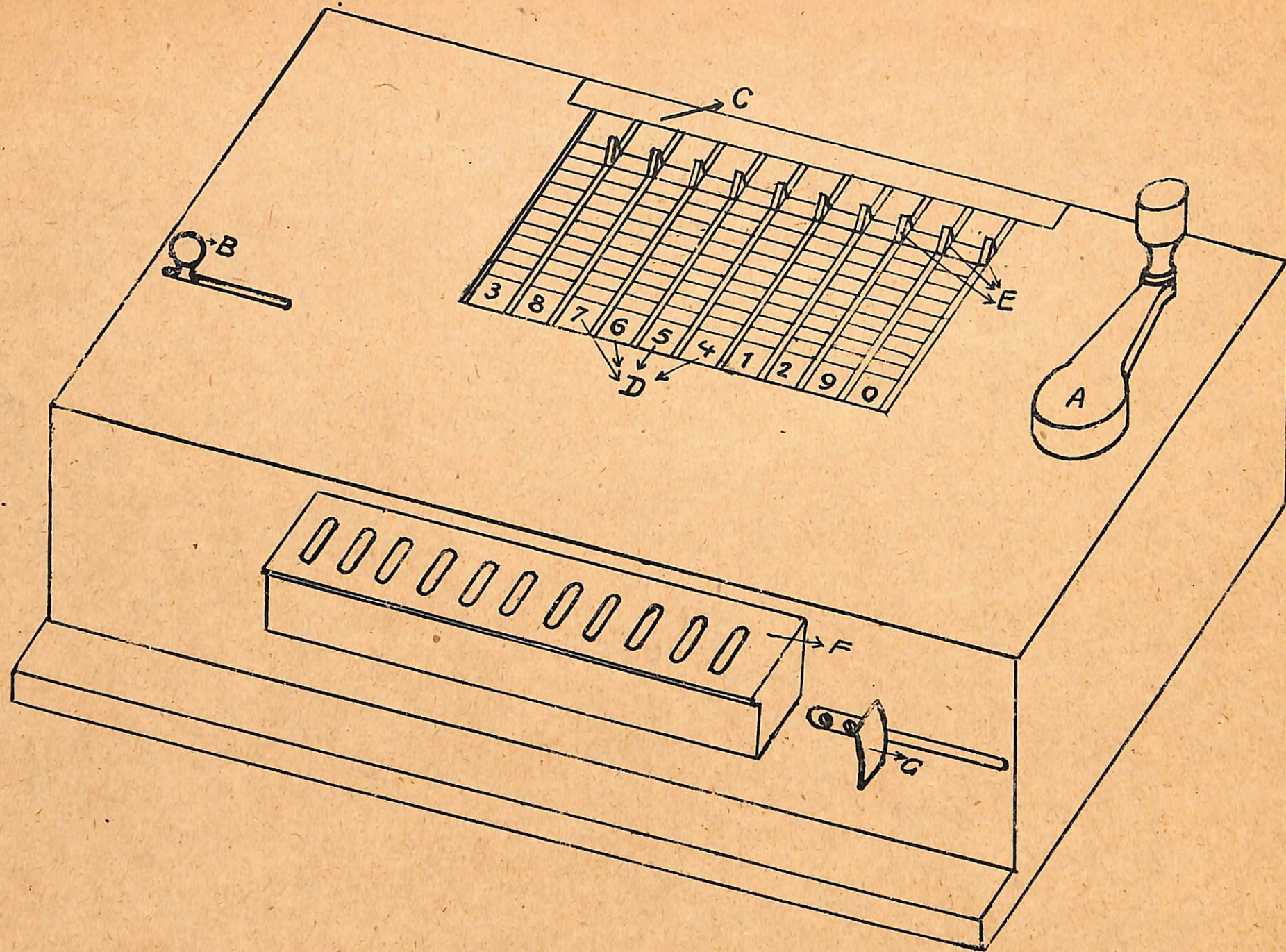
Vychýlí-li se však ze správné polohy o cca poloviční vzdálenost dvou písmen /postaví-li se mezi dvě písmena/, dostane se do mrtvého bodu, z něhož se samočinně nevrací k žádnému z obou sousedních písmen a také žádné z nich nenašifruje resp. ne-dešifruje. Váleček se v této poloze stavěče vůbec nepohne. Zkoušku tuto se strojem prováděti se nedoporučuje,

Otočení klikou na levo nebo na pravo musí § 48.

býti vždy úplné t.j. klika musí po otočení státi paralelně se škálami. Úplné otočení rozpozná se dle zvuku, kterým je provázeno a jenž je způsoben západkou uvnitř stroje. Je-li klika z této základní polohy vychýlena /byť i nepatrně/, nesmí se jiné součástky stroje /na př. knoflíky a vymazávač uváděti do pohybu. Nebezpečí poruchy! Zacházení s klikou.

V zájmu trvale správného fungování stroje § 49.

je nutné vymazávati tahem a ne prudkým trhnutím. Zacházení s vymazávačem a strojem. Poznámky v § 44-46 platí zde stejnou měrou, jako u všech strojů počítačích.



Legenda:

A./ klika

B./ Knoflík X

C./ zámek

D./ škály

E./ knoflíky /sta-
věče/

F./ Okénkový rám.

G./ Vymazač.

Vzorce a příklad šifrování.

Bigramy a interpunkce:

Fonetisace číslic:

Složení první skupiny kryptogramu:

pr - f
 př - f
 ch - g
 st - q
 št - q
 sk - w
 šk - w
 ck - w
 čk - w
 ? - ko
 y - i

bu 1 n-
 co 2 p-
 di 3 q-
 fe 4 r-
 ga 5 s-
 h- 6 tu
 j- 7 vo
 k- 8 wi
 l- 9 xe
 m- 0 za

Libovolné | Datum | Pořadové číslo.
 S až Z

Šifrování číslic:

A./ Příklad čísla o lichém počtu míst.
 B./ Příklad čísla o sudém počtu míst.

A./ NUME35690.

→ počet míst čísla
 → číslo samo
 → součet jeho číslic
 → samohláska textu nebo hluché U

B./ NUME2684.

→ souhláska textu nebo hluché X

P ř í k l a d :

10. jistého měsíce odesílá se depeše znějící:

Ad Vaše č.j. 2753: Experti přijedou do Prahy 18. března.

Žádají přesné sdělení Vašeho programu pro porady. Zašlete obratem.

Poznámky: 1./ Předpokládejte, že pořadový denní klíč k sestavení škal a válečku pro tento den zní:

7 6 5 0 3 2 9 4 1 8

2./ Prvá skupina kryptogramu bude sestavena na př.

takto: W O S O | N A | L E K E
 to značí: šifrováno 10 8 4
 strojem | tum | pořadové číslo

Provedení:

Příprava textu:
Kryptogram:

vasenum42 7537xexupe rutifijedo
 WOSONALEKE GIFARICURU DAJUHABAGU HIFARUFEFU
 xufahinume 2I89burezu nazadajife sunesudele
 BOGOFEQENE WOBUCUNUJU JINIVIRAWA DOZAHOROVO
 nivasehofo guramufopo radizasuli xoburatemu
 TUKAKUFEVO VURUDOZIPIA JEZUJEGIGO COMENAOOCU

DENNÍ KLÍČE.

L e d e n . .	Ú n o r .	B e z e n .
I 7812963450	I 9834507216	I 3270145698
2 7038549216	2 9618305274	2 5016783492
3 3076921854	3 1234765890	3 3890527416
4 7250983614	4 7830569412	4 5418907632
5 5274189630	5 3016549872	5 1476589032
6 9830167254	6 7890165432	6 7234985610
7 3618945072	7 5094167238	7 7032169458
8 9832765410	8 9236507814	8 1852763490
9 5496103278	9 9074523816	9 5470321896
10 9816345072	10 7850149236	10 5278361094
11 1852769034	11 9452783610	11 5418763290
12 7236109458	12 7618543092	12 9034581276
13 5278349016	13 3872961054	13 3478961250
14 7634125890	14 9456721038	14 7258903416
15 9852307416	15 9674523810	15 9814367250
16 5612987034	16 7854923610	16 9412385670
17 5814903276	17 3410589276	17 5816327094
18 7254163890	18 9870321654	18 9632741850
19 3096587412	19 3472905816	19 1856349270
20 1450927836	20 3894105672	20 3850721694
21 5210769438	21 3470129856	21 3498725610
22 3074921658	22 9032587614	22 5632107498
23 3256701498	23 5014963872	23 3094785612
24 7850361294	24 5812907436	24 1678523094
25 7832965014	25 1234567890	25 1470529638
26 7650329418	26 1274905836	26 9452183076
27 5038147296	27 1692703854	27 1058923674
28 9874163052	28 1690347852	28 1850923476
29 7418569230	29 3274501896	29 9214587630
30 5096187432		30 7236149850
31 3472501896		31 5014729638

D E N N Í K L Í Č E.

D u b e n .	K v ě t e n .	Č e r v e n .
I 1072385694	I 7018345296	I 1072569834
2 5276381094	2 5638749012	2 7418305296
3 5436721098	3 1670345892	3 3270549618
4 3694127058	4 7012345698	4 7238509416
5 7698305412	5 3096125874	5 7836921450
6 9810327654	6 1238749056	6 3612987450
7 3470189652	7 1870963452	7 9470123856
8 9210387456	8 1258763490	8 7610943852
9 5078361492	9 5436701892	9 1278543690
10 7834965012	10 9812547036	10 9614583270
11 5276109438	11 3258147096	11 1270349856
12 1854763290	12 1098325476	12 1238507694
13 9278543610	13 1298765430	13 7218965034
14 7436109852	14 9854761230	14 1832907654
15 5876903412	15 3094721658	15 3872569014
16 1074385692	16 5812709436	16 1032985476
17 3872945016	17 5278149036	17 7450129638
18 3652781094	18 5874901632	18 9250167438
19 9658703412	19 9418325670	19 5670149832
20 7856103492	20 5476129038	20 7410965238
21 9658307214	21 9830567412	21 5076943812
22 5418703296	22 1458769032	22 9876543210
23 9458127036	23 3274509618	23 9018723654
24 7294381056	24 3658109472	24 3210549876
25 5674389210	25 3254769810	25 5674381092
26 5472903816	26 5870321496	26 5472903816
27 7614523890	27 9650781234	27 3214789650
28 5816729034	28 1034729658	28 5674389210
29 9650147832	29 7016589432	29 5436987012
30 9810763254	30 9250147638	30 1034529678
	31 5896103274	

D E N N Í K L Í Č E.

Č e r v e n e c.	S r p e n .	Z á ř í .
I 90I2783456	I 98I4723056	I 9854I03276
2 32589074I6	2 7854I23690	2 52963074I8
3 54709638I2	3 3072I69854	3 3874I25690
4 54I6307892	4 369078I452	4 907438I652
5 58I2763490	5 I256387094	5 I830749256
6 387094I652	6 7852I09634	6 92385470I6
7 3256I09478	7 I674903258	7 I658709432
8 72I4903658	8 349258I076	8 92I8705436
9 I096345278	9 32I6789054	9 50I6327498
IO 78I0963452	IO 987254I036	IO 9852I07634
II 5890I47632	II 54I8903672	II 3052I67894
I2 52I0987436	I2 9278I05634	I2 3056 7298I4
I3 5032I67894	I3 705634I298	I3 54I8963270
I4 I658307492	I4 7694I83052	I4 I034987256
I5 5094I63872	I5 9470I85632	I5 5634709872
I6 30589674I2	I6 I678523094	I6 I094583276
I7 50947832I6	I7 72I8365094	I7 I456327098
I8 78I4905236	I8 I672385490	I8 347092I856
I9 34587092I6	I9 56743098I2	I9 9032I67854
20 967230I458	20 7238I45096	20 70I8563294
2I 94725830I6	2I 305296I478	2I I890765432
22 38569270I4	22 94327650I8	22 7690I85432
23 I458307692	23 92307856I4	23 30I2749856
24 I692503478	24 I078549632	24 72943650I8
25 34I8925076	25 92763058I4	25 30I4765298
26 I652307498	26 549072I836	26 I470983256
27 3254I07698	27 I472389056	27 34I2569078
28 5478I69032	28 329056I478	28 50I8723496
29 347890I652	29 I438507692	29 I876543290
30 38547096I2	30 709436I852	30 3654I8 9072
3I 74569832I0	3I 327456I098	

D E N N Í K L Í Č E .

Ř í j e n .	L i s t o p a d .	P r o s i n e c .
I 5470I69238	I 329074I856	I 7496I83052
2 I427589036	2 7892I65430	2 345678I092
3 I234569870	3 9276I45038	3 I870529436
4 50I2743698	4 703654I892	4 9652I47038
5 72589436I0	5 389054I276	5 507236I894
6 7698I05234	6 32I8567094	6 789652I034
7 9850I67432	7 I098765432	7 3890I67254
8 58I4963072	8 50923478I6	8 57I2903674
9 32I8567094	9 I250987436	9 925470I836
I0 927634I058	I0 I092783654	I0 567890I234
II 54I6903872	II 7830I49652	II 30945278I6
I2 345692I078	I2 I496527830	I2 5298I43670
I3 98I4305672	I3 52I0349678	I3 7890I25634
I4 32I4567890	I4 9850I23476	I4 90I2547638
I5 I894703256	I5 54I0389672	I5 I894503672
I6 547236I890	I6 56783492I0	I6 I236947850
I7 I294365078	I7 I290347658	I7 7892I65430
I8 38569472I0	I8 305298I476	I8 9672I83450
I9 3690I87452	I9 765892I035	I9 7092I43658
20 72369058I4	20 529674I830	20 96305472I8
2I 507638I294	2I 54I8709236	2I 52983074I6
22 58I4907632	22 3698I27450	22 70569832I4
23 I452907638	23 765230I498	23 789650I432
24 74369850I2	24 9276I03458	24 92I8503476
25 I470385296	25 7890I23456	25 58703694I2
26 50I4763298	26 96I2347058	26 74509836I2
27 I850749632	27 36709852I4	27 I476325098
28 907856I432	28 I056743892	28 34I0589276
29 I492367850	29 90I2345678	29 72905634I8
30 96I4327058	30 I430589276	30 74305698I2
3I 56327098I4		3I 9432I87056

ROČNÍ KLÍČE.Původní sestava:

Samohlás. / souhláskové škály a válečky
 0 2 4 6 8 | 1 3 5 7 9 → čísla skal a válečků

2	7	3	8	5	7	5	0	4	3
7	8	2	5	3	9	3	2	1	8
3	5	7	2	8	3	6	7	0	1
8	2	5	3	7	1	7	9	2	4
5	3	8	7	2	6	4	5	3	9
6	9	9	0	1	0	1	3	5	2
0	6	4	1	9	4	8	6	8	7
1	4	0	6	4	2	0	8	9	6
4	0	1	9	6	5	9	1	6	0
9	1	6	4	0	8	2	4	7	5

I. změna

0	2	4	6	8	1	3	5	7	9
8	2	7	5	3	7	8	1	6	4
2	5	3	7	2	6	7	2	8	5
5	3	8	2	7	8	4	3	5	0
3	7	2	8	5	5	6	4	2	3
7	8	5	3	8	4	5	7	3	9
1	4	6	9	9	0	3	5	7	2
0	9	4	0	1	1	2	8	9	8
4	0	9	1	6	2	9	0	4	1
6	1	0	6	4	3	0	9	1	6
9	6	1	4	0	9	1	6	0	7

II. změna

0	2	4	6	8	1	3	5	7	9
7	8	2	8	3	9	3	9	0	8
5	7	3	5	2	7	0	8	1	9
2	5	7	3	7	8	2	7	3	6
3	2	5	7	8	6	1	4	2	5
8	3	8	2	5	5	4	0	6	7
0	9	6	6	4	1	5	2	4	3
1	1	0	4	9	0	9	1	5	2
4	6	1	9	0	2	6	3	7	4
6	4	9	0	1	3	8	5	9	1
9	0	4	1	6	4	7	6	8	0

III. změna:

0	2	4	6	8	1	3	5	7	9
7	8	5	2	7	3	6	2	0	8
5	7	2	8	3	0	9	8	1	7
2	5	3	7	8	6	1	0	7	6
3	2	8	3	5	7	0	1	6	9
8	3	7	5	2	9	3	4	5	0
9	6	4	0	9	1	2	9	4	5
4	0	6	9	1	2	4	7	8	1
0	1	9	6	4	4	8	5	9	2
1	4	0	1	6	8	5	6	3	4
6	9	1	4	0	5	7	3	2	3

IV. změna:

0	2	4	6	8	1	3	5	7	9
7	8	5	2	7	3	6	7	5	9
8	2	7	3	5	0	4	8	1	6
2	3	8	5	3	4	2	9	0	5
3	5	2	7	8	8	3	5	6	1
5	7	3	8	2	7	5	6	2	0
0	9	1	4	6	4	2	8	3	2
1	4	0	6	4	2	8	1	4	3
9	1	6	9	0	6	1	2	9	4
4	6	9	0	1	9	0	3	7	8
6	0	4	1	9	1	9	0	8	7

V. změna:

0	2	4	6	8	1	3	5	7	9
2	7	8	7	8	4	6	8	7	5
3	3	2	8	5	5	2	7	6	3
5	5	3	2	7	0	3	4	8	1
7	8	5	3	2	2	5	3	9	0
8	2	7	5	3	1	4	2	5	6
9	4	6	6	0	3	7	1	4	2
0	1	9	4	9	6	8	0	1	7
6	1	0	1	9	3	9	5	9	3
1	4	9	0	1	4	9	6	2	9

VI. změna:

0	2	4	6	8	1	3	5	7	9
7	8	5	2	3	8	3	4	6	5
2	7	8	3	5	9	0	8	3	6
3	5	2	7	8	0	7	5	4	3
5	3	7	8	2	7	1	6	5	2
8	2	3	5	7	1	2	0	7	4
1	6	4	9	0	6	8	9	8	7
0	1	6	4	9	1	4	9	0	1
6	9	0	6	1	5	3	6	7	9
4	0	9	1	4	6	5	3	2	8
9	4	1	0	6	4	5	3	2	8