FIALKA M-125

Eugen Antal, prof. RNDr. Otokar Grošek, PhD.,
Katedra aplikovanej informatiky a výpočtovej techniky
antal.87@gmail.com

Abstrakt

Hlavným cieľom tejto práce bolo vytvorenie učebnej pomôcky ku rotorovému šifrátoru Fialka M-125. V práci je uvedený popis jednotlivých častí stroja ako aj popis činnosti. Súčasťou je aj simulátor činnosti šifrátora (webová aplikácia) na platforme Java.

1. Úvod

Fialka je rotorový šifrovací stroj, vytvorený sovietskou armádou, ktorý bol prvýkrát uvedený do používania okolo roku 1965. Dizajn a fungovanie Fialky je založený na podobnom princípe ako Enigma, používaný nemeckou armádou počas druhej svetovej vojny, aj keď s mnohými vylepšeniami. Oficiálne označenie stroja je M-125, kým Fialka je meno šifrovacej procedúry. Stroj používa niekoľko rotorov na substitúciu znaku napísaného na klávesnici.
Fialka bola dlhú dobu utajená. Vydané a inými štátmi používané stroje boli pozbierané a neskôr zničené, len málo kusov sa zachránilo. Popis stroja a materiály neboli dlhú dobu dostupné pre verejnosť. Táto skutočnosť bola hlavnou motiváciou pri písaní tejto práce.

2. Popis Fialky

Šifrovací stroj Fialka na prvý pohľad vyzerá ako obyčajný písací stroj. Vo vnútri však skrýva pokročilý šifrovací mechanizmus, vďaka ktorému sa zaradil medzi vrcholné kryptografické stroje.
Pôvodná verzia Fialky bola M-125-xx, ktorá bola navrhnutá na používanie sovietskou armádou (klávesnica používala len cyriliku). Neskoršie verzie M-125-3xx boli rozšírené s niekoľkými vylepšeniami a tiež boli vybavené klávesnicou, ktorá obsahovala aj písmená latinskej abecedy.
Práca bola napísaná s použitím citovanej literatúry. Obrázky sú prevzaté z práce [1].

2.1. Dôležité časti Fialky

Na pravej strane v strede sa nachádza dôležitý prepínač, pomocou ktorého môžeme stroj použiť v nasledujúcich troch módoch:
O – použiť ako písací stroj
P – na rozšifrovanie správy
3 – na zašifrovanie správy

V strede pod krytom sa nachádza kódovacie zariadenie obsahujúce 10 rotorov. Rotory sa pohybujú pri každom stlačení klávesy. Sú pripojené z ľava na tzv. reflektor a z prava na vstupný disk.

Obr. 1. Pohľad na Fialku M-125

2.2. Rotory

Fialka používa desať jedinečných rotorov označených prvými desiatimi písmenami cyriliky, vsadených na hriadeľ. Každý rotor má 30 kontaktov na jednej strane prepojených príslušnou substitúciou a zároveň niekoľko blokovacích pinov. Je tu 30 možných pozícií blokovacích pinov na každom rotore. Každý pin je priradený k jednému písmenu na vonkajšej hrane. Prítomnosť alebo neprítomnosť pinu ovláda krokovanie rotora Fialky. Blokovacie piny zabraňujú ďalšiemu rotoru v pohybe.
Existujú dva typy rotorov, pevné a nastaviteľné. Pôvodne Fialku vydali s desiatimi pevnými rotormi. Každý rotor mal 30 kontaktov s premenlivým počtom blokovacích pinov.

Na Fialke s pevnými rotormi sa mohli uskutočniť (podobne ako na Enigme) nasledujúce nastavenia:

- Zmena poradia rotorov
- Zmena začiatočného znaku na jednotlivých rotoroch

V roku 1978 boli pevné rotory vymenené za nastaviteľné. V základnom nastavení každý nastaviteľný rotor fungoval ako pevný s tým istým označením. Oproti pevným rotorom bolo možné nastaviť:

- Posun blokovacích pinov na vonkajšom kruhu
- Jadro z jednotlivých rotorov sa dalo preložiť do iného rotora
- Zmeniť stranu jadra
- Zmena znaku na jadre jednotlivých rotorov

Obr. 2. Sada rotorov Fialky

2.2.1. Prepojenie rotorov

Šifrovací stroj Fialka používa desať rotorov, ako to už bolo spomenuté, ale boli nájdené tri rôzne série rotorov, pri ktorých boli iné prepojenia rotorov ako aj iné pozície blokovacích pinov. Rôzne série používali rôzne krajiny. Z troch sérií boli zatiaľ identifikované len dve:
3K – použité v Poľsku
6K – použité v Československu

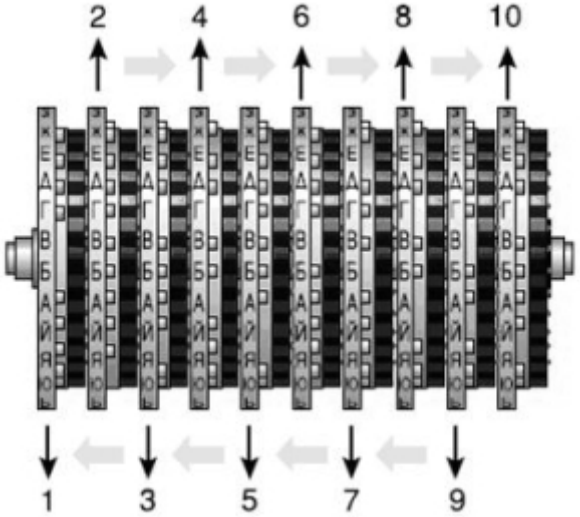
Prepojenie rotorov bolo dopredu určené zvlášť pre každú sériu. Tieto prepojenia, ako aj prítomnosť blokovacích pinov na jednotlivých pozíciách môžu byť znázornené v prepojovacích tabuľkách. Z prepojovacej tabuľky pomocou vstupujúceho znaku na rotor a označenia rotora môžeme určiť výstupný znak.

Tab. 1. Prepojovacia tabuľka pre sériu 3K

3K SERIES		Contact																												
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
		А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Ю	Я	И
Wheel	1	А	23	22	3	7	4	8	16	6	10	20	15	17	24	9	30	12	25	11	1	28	27	5	29	26	2	18	21	14	13	19
	2	Б	3	24	20	2	6	21	26	7	18	4	17	23	15	19	10	30	13	28	29	11	9	25	1	14	22	8	27	5	12	16
	3	В	20	5	7	15	21	27	4	1	22	17	23	13	30	6	26	10	16	14	19	18	29	24	3	12	9	11	2	28	8	25
	4	Г	16	21	28	11	27	3	15	12	24	30	9	17	6	20	25	8	1	29	19	18	14	10	5	23	26	7	6	22	2	13
	5	Д	10	15	1	22	15	16	29	8	17	6	5	16	6	30	23	5	26	13	25	10	12	21	27	20	7	11	24	9	2	28
	6	Е	9	14	13	20	24	8	2	6	5	19	11	28	30	3	18	15	7	25	16	1	12	23	27	29	17	30	21	4	22	26
	7	Ж	7	9	5	26	6	4	19	3	8	28	22	12	21	24	23	30	13	1	16	29	2	25	27	15	18	11	16	17	30	20
	8	З	29	27	15	18	8	2	25	17	6	23	9	18	24	1	14	21	17	10	3	11	27	7	16	4	19	26	5	30	28	20
	9	И	5	19	2	27	30	26	7	11	16	18	5	15	4	28	28	21	4	24	29	30	15	17	9	13	8	32	25	10	1	14
	10	К	20	24	8	25	19	1	17	5	15	27	9	12	22	10	18	9	16	30	4	14	7	29	11	2	29	26	28	21	6	19

2.2.2. Krokovanie rotorov

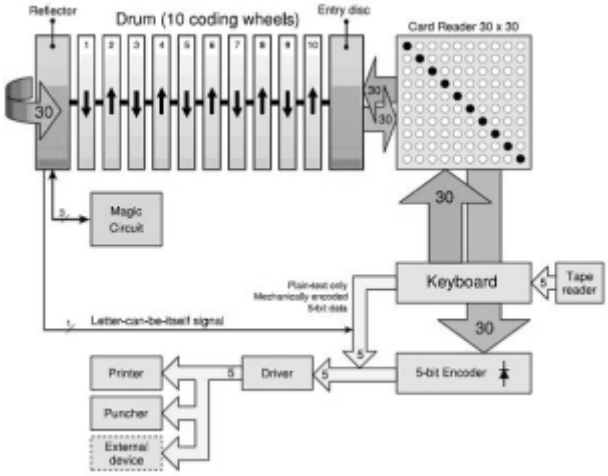
S každým zadaným znakom cez klávesnicu sa rotory vo vnútri Fialky nastavia na novú pozíciu, čo spôsobilo nové prepojenie rotorov pre každý nový znak. Fialka používa striedavý krokovací mechanizmus. To znamená, že na pohyb rotorov sa používajú dve mechanicky nezávislé časti. Preto rotor nikdy neovplyvní pohyb jeho vedľajšieho rotora. Namiesto toho je spojený s rotorom o jeden ďalej a priľahlé rotory sa pohybujú v opačnom smere. Keď sa jeden rotor pohybuje v smere hodinových ručičiek, potom vedľajší rotor sa pohybuje smerom proti hodinovým ručičkám.
Rotory v poradí zľava označme s číslami od 1 do 10.



Obr. 3. Označené rotory Fialky a smer ich pohybu

Prakticky sú to dva nezávislé pohyby rotorov. Párne sa otáčajú nezávisle od nepárnych.
Keď sa pozeráme z hora, párne rotory sa vzďaľujú od klávesnice pričom rotor č. 2 je rýchli. Rýchli znamená, že rotor sa pohybuje pri každom stlačení klávesy.
Každým stlačením klávesnice sa bude hýbať rotor č. 2 a naháňať rotor č. 4, ktorý potom naháňa rotor č. 6 atď.
Keď je blokovací pin v určitej pozícií na rotore, všetky rotory napravo od neho nebudú krokované. Kvôli tomu že sa krokovací mechanizmus nachádza na druhej strane rotorov ako aktuálne nastavený znak, z prepojovacej tabuľky musíme hľadať prítomnosť blokovacích pinov o pár znakov posunutých. V prípade párnych rotorov je to posunuté o 17 znakov v smere hodinových ručičiek. V prípade nepárnych rotorov je to posunuté o 20 znakov v smere hodinových ručičiek.
Keď sa pozeráme z hora, nepárne rotory sa pohybujú smerom ku klávesnici. Rotory sú poháňané zprava, takže v tomto prípade rotor č. 9 je tým rýchlym. Poháňa rotor č. 7, ktorý poháňa č. 5 atď. , až kým nakoniec nie je poháňaní rotor č. 1. Znova, blokovací pin zabráni krokovaniu rotorov na ľavo od neho.

3. Fungovanie Fialky



Obr. 4. Blokový diagram Fialky

Vstupom šifrovacieho stroja je klávesnica, ktorá má 30 kláves. Pri stlačení klávesy je vyslaný elektrický prúd z klávesnice, cez súpravu šifrovacích zariadení. Najprv sa však aplikuje substitúcia znaku na klávesnici. Signál potom prejde cez čítačku kariet čo dovolí dvojici písmen aby sa vymenili. Signál z čítačky kariet je poslaný na vstupný disk, kde sa aplikuje ďalšia substitúcia znaku. Vstupný disk pošle signál ďalej desiatemu rotoru, ten deviatemu, ten ôsmemu atď., až kým signál nedôjde k reflektoru, ktorý je úplne na ľavo. Na reflektore je aplikovaná ďalšia substitúcia, kde je potom signál vrátený späť cez súpravu rotorov na vstupný disk a čítačku kariet až na klávesnicu. Na odrazený signál sú aplikované inverzné substitúcie. Ako výstup sa vytlačí zašifrovaný znak.

Tab. 2. Prepojenie klávesnice

X	1	2	3	4	5	6	7	8	9	10
Y	17	15	30	14	26	21	6	19	1	15
X	11	12	13	14	15	16	17	18	19	20
Y	29	20	4	28	24	2	22	23	18	12
X	21	22	23	24	25	26	27	28	29	30
Y	7	5	27	8	10	9	16	13	11	3

X - vstup, Y - výstup

Tab. 3. Prepojenie vstupného disku

X	1	2	3	4	5	6	7	8	9	10
Y	28	14	20	24	2	16	1	10	21	11
X	11	12	13	14	15	16	17	18	19	20
Y	17	13	19	30	5	6	8	15	23	25
X	21	22	23	24	25	26	27	28	29	30
Y	27	18	3	29	26	12	22	7	9	4

X - vstup, y - výstup

3.1. Šifrovanie

Ako prvý krok si treba nastaviť poradie rotorov a na každom si nastaviť niektorý z 30 znakov, ako začiatočný stav. Po stlačení klávesy nastanú nasledujúce udalosti v poradí:

- Substitúcia z klávesnice na čítačku kariet Tab. 2.
- Substitúcia z čítačky kariet
- Substitúcia z čítačky kariet na vstupný disk Tab. 3.
- Aplikácia substitúcie na rotoroch od 10. k 1.
- Substitúcia na reflektore Tab.4. a Tab. 5.
- Aplikácia inverznej substitúcie na rotoroch od 1. k 10.
- Inverzná substitúcia zo vstupného disku na čítačku kariet
- Inverzná substitúcia priamo z čítačky kariet
- Inverzná substitúcia z čítačky kariet na klávesnicu
- Vytlačenie znaku
- Rotory sú krokované (podľa blokovcích pinov, pozícií a ostatných nastavení)

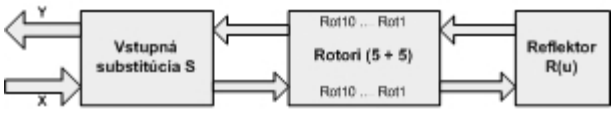
Substitúcia jednotlivými rotormi v prípade M-125-xx je nasledujúca:

- Pridaj aktuálnu pozíciu rotora
- Aplikuj substitúciu z tabuľky prepojenia rotorov Tab. 1.
- Odrátaj aktuálnu pozíciu rotora

3.2. Dešifrovanie

Na dešifrovanie znaku je nutné si nastaviť pôvodné nastavenia rotorov ako pred zašifrovaním prvého znaku. Ako vstup treba zadať postupnosť znakov zašifrovaného textu.
Jediný rozdiel medzi zašifrovaním a dešifrovaním znaku je, že na reflektore sa aplikuje substitúcia z inej tabuľky ako pri zašifrovaní. Aby Fialka mohla zašifrovať znak sám na seba, sú na reflektore pozmenené tri kontakty, čo Fialku zbaví čiastočne jej reciprocity. Pravdepodobnosť zašifrovania znaku sám na seba je 1:30.

3.3. Základná schéma Fialky



Obr. 5. Schéma šifrátora Fialka

Vstupná substitúcia
$S = S_3 S_2 S_1(x)$ (1), kde
S_1 – prepojenie klávesnice (pevne zabudované, Tab. 2.)
S_2 – čítačka karty (zakódovaná v karte, voliteľné podľa knihy denných kľúčov, pri absencii karty je identické zobrazenie)
S_3 – prepojenie vstupného disku (pevne zabudované, Tab. 3.)

Substitúcia rotorov Rot_{10} ... Rot_1 je dané z Tab. 1.

Substitúcia na reflektore:

$$R(u) = \begin{cases} S_1(u), kde S_1 \ je \ dané Tab.4. \\ S_2^{\ 2}(u), kde S_2 \ je \ dané Tab.5. \end{cases} \quad (2)$$

Tab. 4. Substitúcie na reflektore

X	1	2	3	4	5	6	7	8	9
Y	23	6	20	28	14	2	12	17	22
X	10	11	12	13	14	15	17	19	20
Y	11	10	7	13	5	29	8	27	3
X	21	22	23	25	26	27	28	29	30
Y	25	9	1	21	30	19	4	15	26

X - vstup, y - výstup

Tab. 5. Substitúcie na reflektore

X	16	18	24
Y	18	24	16

X - vstup, y - výstup

Šifrovacia funkcia teda môže byť zapísaná ako:

$$y = S_1^{-1} S_2^{-1} S_3^{-1} Rot_{10}^{-1} ... Rot_1^{-1} R(u) Rot_1 ... Rot_{10} S_3 S_2 S_1(x) \quad (3)$$

4. Simulátor šifrátora

Na simuláciu šifrovacieho stroja bola vytvorená webová aplikácia na platforme Java, napísaná v prostredí NetBeans IDE 6.1.
Aplikácia umožňuje simuláciu Fialky verzie M-125-xx. Implementované je prepojovanie rotorov série 6K, ktorá sa používala v bývalom Československu. Pre lepšie využitie tejto série boli použité znaky latinskej abecedy namiesto cyrilskej. Aktuálna verzia aplikácie ešte nezahŕňa čítačku kariet, namiesto toho je použité identické zobrazenie znakov.

4.1. Nastavenia aplikácie

Nastavenia môžeme rozdeliť do troch kategórií

- Nastavenie vstupu
- Výber šifrovacieho módu
- Nastavenia pri používaní

Ako vstup si môžeme vybrať z dvoch možností: klávesnica alebo textové pole. Defaultne je nastavená klávesnica. Naraz môže byť použitá len jedna z možností, ale počas použitia sa dá hocikedy zmeniť. Pri výbere klávesnice sa zobrazí v strede okna jeden panel s 30 možnými vstupmi. Po kliknutí na klávesu sa ako výsledok zobrazí zašifrovaný znak.
Pri prepnutí na textové pole panel klávesnici zmizne z okna.

Pred použitím aplikácie si najprv musíme zvoliť jednu z možností šifrovacieho módu:

- Plain Text – funguje ako písací stroj
- Decoding - dešifrovanie
- Coding – šifrovanie

Pri šifrovaní alebo dešifrovaní môžeme nastaviť poradie jednotlivých rotorov, ako aj začiatočné znaky na jednotlivých rotoroch.

Literatúra

[1] P. REUVERS, M. SIMONS: Codename Fialka, 2005 Dostupné na http://www.xat.nl/fialka/man/index.htm
[2] O. GROŠEK, M.VOJVODA, P. ZAJAC: Klasické šifry. STU Bratislava, 2007. ISBN 80-227-2653-5
[3] O.GROŠEK, M. VOJVODA, M. ZANECHAL, P. ZAJAC: Základy kryptografie. STU Bratislava, 2006. ISBN 80-227-2415-7
[4] T. PERERA: Fialka museum, 2005. Dostupné na http://tomperera.com/enigma/mfmn.htm
[5] T. PERERA, D. HAMER: Enigma museum. Dostupné na http://www.w1tp.com/enigma
[6] http://freenet-homepage.de/SASundChiffrierdienst/dv040-1-321.html
[7] http://jproc.ca/crypto/russian_m125_fialka.html
[8] http://www.ilord.com/fialka.html