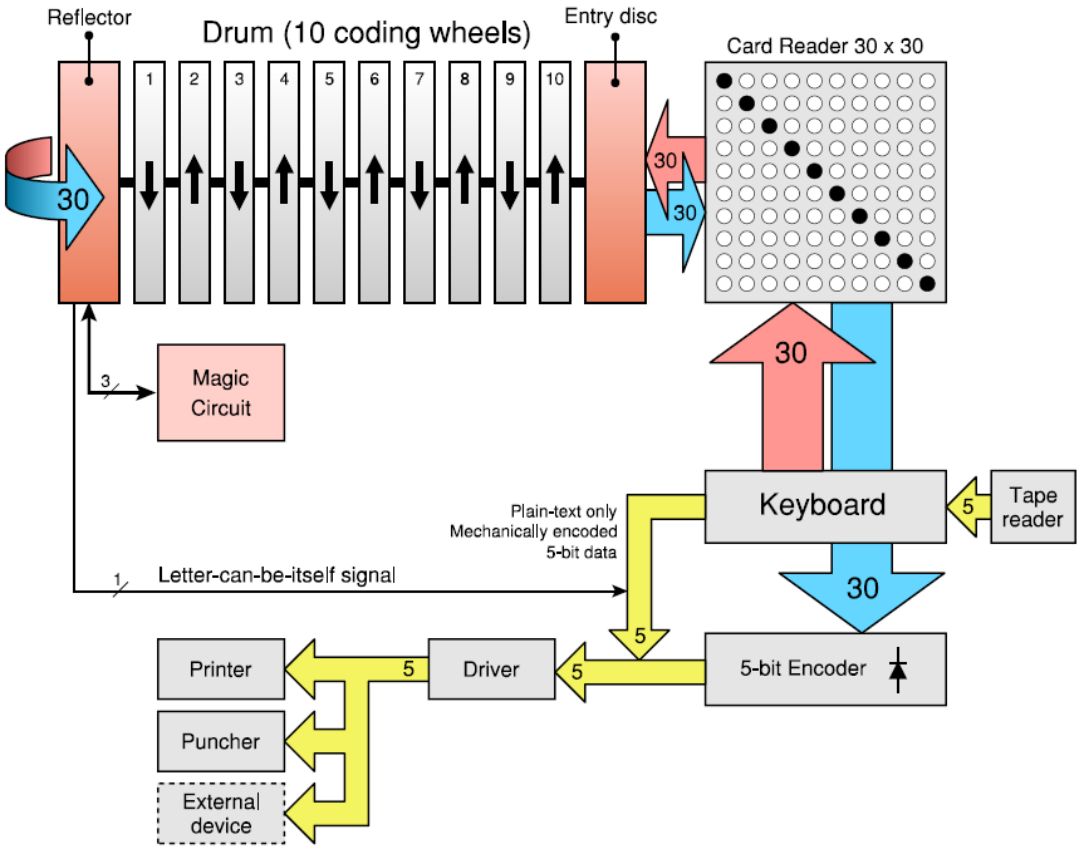
2.7 Technické detaily a blokové diagramy Fialky

Dizajn Fialky je veľmi podobný Enigme, avšak Fialka má množstvo iných doplnkov. V prvom rade plug board Enigmy bol nahradený čítačkou kariet, ktorá značne zjednodušovala nastavovaciu procedúru. Ďalej Fialka používa 10 rotorov a pokročilý krokovací mechanizmus. Podobne ako na Enigme, aj na Fialke je použitý reflektor na odraz prúdu späť do sady rotorov. Oproti Enigme je tu použitá tlačiareň na zobrazenie koncového výstupu.

Ďalším vylepšením Fialky je seba-zakódovatelnosť znaku.



Obr. 14. Blokový diagram Fialky M-125-xx (prevzaté z [1])

Klávesnica má 30 kláves. Stlačením klávesy sa vyšle elektrický prúd (signál) na čítačku kariet, ktorá sa správa presne tak, ako plug board na Enigme. Z čítačky kariet ide signál na vstupný disk, ktorý ho podá ďalej na súpravu rotorov. Na konci šifrovacieho zariadenia je

signál vrátený späť do súpravy rotorov, cez vstupný disk a čítačku kariet až na klávesnicu. Tu je napájanie do matice diód, ktorá to konvertuje na jedinečný 5 bitový formát, podobný (ale odlišný od) 5 bitovému Baudotovmu kódu. 5 bitové dáta z tohto kódera sú použité na riadenie tlačiarne a dierkovača. Okrem riadenia jedného z 30 spínačov, klávesnica obsahuje aj 5 bitový mechanický kóder, ktorý produkuje digitálny kód bežného textového originálu. Tento kód je používaný, keď je Fialka nastavená ako štandardné dialnopisné zariadenie (v bežnom textovom móde). Avšak 5 bitový kód bežného textu môže byť použitý aj na prepísanie 5 bitového dáta zašifrovaného písmena. Toto je kontrolované jedným kontaktom na reflektore. Keď prúd dosiahne tento konkrétny kontakt na reflektore, žiadny signál sa neposiela späť na rotory, namiesto toho sa používa 5 bitový kód originálneho písmena. Pravdepodobnosť toho, že znak bude zakódovaný sám na seba je 1:30.

Ďalšie 3 vodiče z reflektora sú prepojené s tzv. magic circuit, ktorý používa cyklus dĺžky 3, ktorý čiastočne zbaví Fialku jej reciprocity. Zvyšných 26 kontaktov na reflektore sú spojené do párov, podobne ako na Enigme a jeden znak (trinásty) sa šifruje sám na seba.

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

Tab. 6. Substitúcia z klávesnice na čítačku kariet (prevzaté z [1])

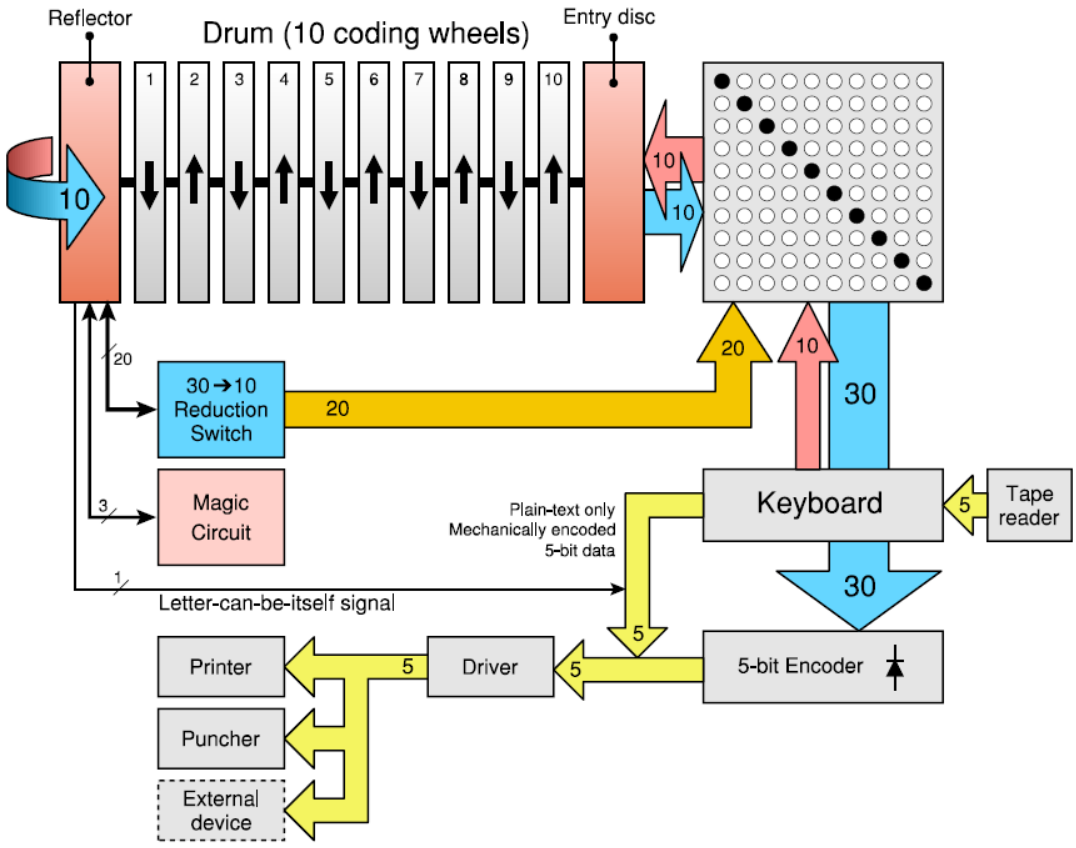
Card Reader ➔ Entry Disc																												
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
28	14	20	24	2	16	1	10	21	11	17	13	19	30	5	6	8	15	23	25	27	18	3	29	26	12	22	7	9	4

Tab. 7. Substitúcia z čítačky kariet na vstupný disk (prevzaté z [1])

	Reflector in Coding mode (3)																											
	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
Coding (3)	23	6	20	28	14	2	12	17	22	11	10	7	13	5	29	18	8	24	27	3	25	9	1	16	21	30	19	4	15	26
Decoding (P)	23	6	20	28	14	2	12	17	22	11	10	7	13	5	29	24	8	16	27	3	25	9	1	18	21	30	19	4	15	26
Plain text (O)	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

Tab. 8. Substitúcia na reflektore (prevzaté z [1])

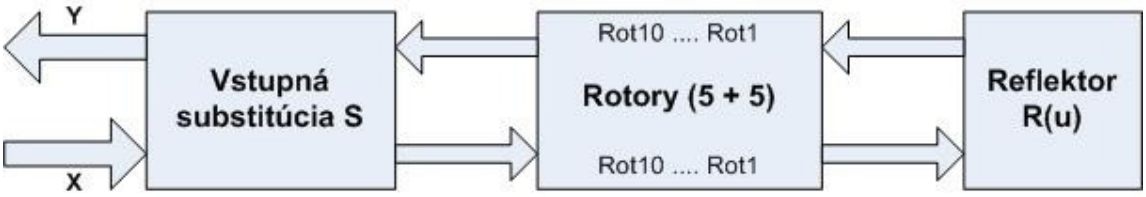
Neskoršie verzie Fialky sú zložitejšie, funguje u nich aj spätná kompatibilita (V základnom nastavení aj model M-125-3xx funguje ako predošlí model M-125-xx). K novším verziám boli pridané nové funkcie, ktoré zvyšujú možnosti ich využitia.



Obr. 15. Blokový diagram Fialky M-125-3xx (prevzaté z [1])

Je síce pravdou, že nové verzie obsahujú mnohé vylepšenia, ale väčšina súčiastok je prítomná v každej verzii. Všetky modely Fialky majú čítačku diernej karty, ktorá je integrovaná s klávesnicou. Čítačka generuje 5 bitové dáta z diernej karty a podáva to mechanickej klávesnici, ktorá ho konvertuje na signál. Táto istá mechanika je použitá na generovanie 5 bitových dát bežného textu pri písaní na klávesnici.

2.7.1 Základná schéma Fialky



Obr. 16. Schéma šifrátora Fialka M-125-xx

- Vstupná substitúcia

$$S = S_3 S_2 S_1(x) \quad \text{, kde}$$

S_1 – prepojenie klávesnice (pevne zabudované, Tab. 6.)

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. 7.)

- Substitúcia rotorov Rot_{10} ... Rot_1 je dané z Tab. 3. alebo z Tab. 4.

- Substitúcia na reflektore:

$$R(u) = \begin{cases} S_1(u), kde S_1 \ je \ dané Tab. 9. \\ S_2{}^2(u), kde S_2 \ je \ dané Tab. 10. \end{cases}$$

Tab. 9. 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. 10. Substitúcie na reflektore

X	16	18	24
Y	18	24	16

X - vstup, y - výstup

Šifrovacia funkcia teda môže byť zapísaná ako:

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

2.7.2 Postupnosť udalostí pri fungovaní Fialky

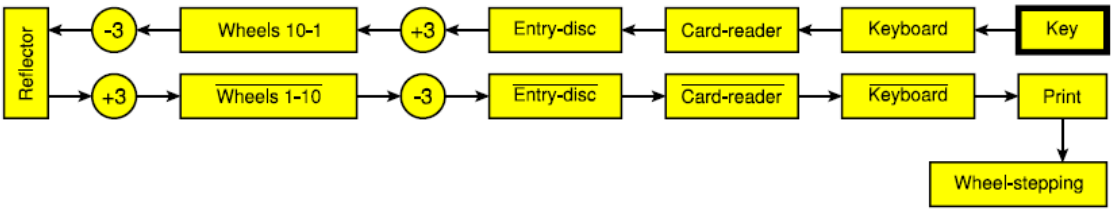
Pre pochopenie fungavania Fialky je dôležité poznať rôzne udalosti a postup ich diania. Udalosti sa uskutočňujú v nasledujúcom poradí:

- stlačenie klávesy
- zmena znaku na cyrilský znak
- substitúcia z klávesnice na čítačku kariet (Tab. 6.)
- substitúcia priamo z čítačky kariet
- substitúcia z čítačky kariet na vstupný disk (Tab. 7.)
- +3 (rozdiel medzi kontaktom 1 na vstupnom disku a nastaveným znakom na rotore)
- aplikácia substitúcie pre každý rotor od 10 k 1
- -3 (rozdiel medzi nastaveným znakom na rotore a medzi kontaktom 1 na reflektore)
- substitúcia na reflektore (rôzny reflektor pre zašifrovanie a dešifrovanie) (Tab. 8.)
- +3 (rozdiel medzi kontaktom 1 na reflektore a nastaveným znakom na rotore)
- aplikácia inverznej substitúcie pre každý rotor od 1 k 10
- -3 (rozdiel medzi nastaveným znakom na rotore a medzi kontaktom 1 na vstupnom disku)
- inverzná substitúcia zo vstupného disku na čítačku kariet (Tab. 7.)
- inverzná substitúcia priamo z čítačky kariet
- inverzná substitúcia z čítačky kariet na klávesnicu (Tab. 6.)
- vytlačenie znaku
- rotory sú krokované (podľa blokovcích pinov, pozícií a ostatných nastavení)

Substitúcia jednotlivými rotormi z opačného smeru (t.j. sprava doľava) je nasledujúca:

- pridaj aktuálnu pozíciu rotora (číselné označenie z Tab.1 ale s -1 (od 0 do 29))
- pridaj nastavenie kruhu (ring-setting)
- odrátaj nastavenie jadra (core-setting)
- aplikuj substitúciu z matice prepojenia rotorov (Tab. 3. a Tab. 4.)
- pridaj nastavenie jadra
- odrátaj nastavenie kruhu
- odrátaj aktuálnu pozíciu rotora (číselné označenie z Tab.1 ale s -1 (od 0 do 29))

Substitúcia jednotlivých rotorov v opačnom poradí (t.j. zľava doprava) je identická predošlému postupu okrem jedného kroku: inverzná matica prepojenie rotorov je aplikovaná vo 4. kroku.



Obr. 17. Schéma fungovanie Fialky (prevzaté z [1])

2.8 Vytváranie kľúčov - nastavenie Fialky

Kľúčové nastavenie Fialky sa skladá z

- knihy denných kľúčov
- knihy kľúčov správ
- knihy identifikátora správ

Kniha denných kľúčov obsahuje denné kľúče pre jeden mesiac. Denný kľúč pozostáva z tabuľky kľúča a z karty (deravej pásky). Tabuľka kľúča definuje pre systém fixných rotorov ich poradie ako aj začiatočné nastavenie. Ako to z názvu vyplýva, denný kľuč je platný 24 hodín. Väčšinou sa mení o 00:01.

Príklad denného kľúča k Fialke M-125-3XX pre 14. mesiac:

ИДЖЗА ВКБГЕ 14
ОСАНЕ РТБВЕ
БДВИА ГЕЗКЖ
2II22 I22I2
КУЛКЮ ЫХВУГ

Kniha kľúčov správ obsahuje počiatočné nastavenie rotorov na použitie pre každú správu. Kľúč správy sa nikdy nepoužíva dvakrát.

Počet možných kľúčov:

- 30! – na čítačky kariet
- 10! – poradie rotorov
- 30^{10} – 30 možných posunov na každom rotore

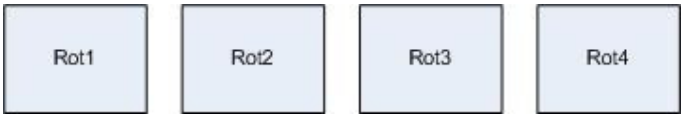
Teda počet nastaviteľných kľúčov je 30! x 10! x 30^{10} =
5683759001280889336795212889561497600000000000000000000 = $2^{178,6}$

2.9 Skrátená verzia Fialky

Pre jednoduchšie znázornenie fungovania šifrátora, som vytvoril skrátenú verziu Fialky M-125-xx. Pomocou tejto verzie si môžeme uviesť jednoduchší príklad na šifrovanie a dešifrovanie. Zároveň môžeme sledovať jednotlivé kroky pri fungovaní.

2.9.1 Voľba počtu rotorov a znakov

Aby sme dodržali princíp stroja požijeme 2 rotory. Jeden na otáčanie v smere hodinových ručičiek, druhý na otáčanie proti smeru. Pre znázornenie krokovania a funkcie blokovacích pinov pridáme ešte 2 rotory. Máme teda 4 rotory ktoré označíme v poradí z ľava od 1 do 4.



Obr. 18. Zvolené rotory pre skrátenú verziu

Teraz si zvoľme smer otáčania jednotlivých rotorov. Párne rotory s číslom 2 a 4 sa budú otáčať v smere hodinových ručičiek. Nepárne rotory s číslom 1 a 3 sa budú otáčať v opačnom smere.
Pozn.: Fialka na pohyb používa dve mechanicky nezávislé časti, jednu na otáčanie rotorov v smere hodinových ručičiek, druhú pre opačný smer. To znamená že v našom prípade pri krokovaní je spojený rotor č. 1. s rotorom č. 3. a rotor č. 2. s rotorom č. 4.

Pri voľbe počtu znakov musíme dodržať nasledujúce kritériá pre dĺžku cyklov:

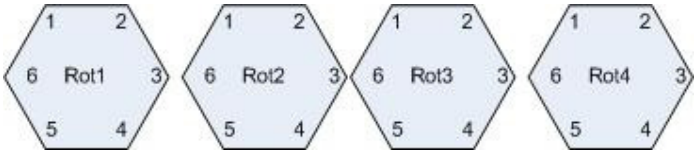
- 1 znak na seba
- 3 znaky na cyklus dĺžky tri
- 2 znaky na cyklus dĺžky dva

Teda minimálny počet znakov je v našom prípade 6.

Zvoľme si „a“ „b“ „c“ „d“ „e“ „f“ a označme ich s číslami v poradí od „a“ do „f“.
Naša abeceda neobsahuje medzeru.

Znak	a	b	c	d	e	f
Označenie	1	2	3	4	5	6

Tab. 11. Použitá abeceda a jej označenie



Obr. 19. Zvolené rotory so šiestimi kontaktmi

Definujme si denné nastavenie stroja:

1. poradie rotorov
2. nastavený znak na rotore

Počet možností pre nastavenie poradia rotorov je 4!. Keď berieme do úvahy aj 6 možných posuvov na každom rotore, celkový počet nastavení bude: $4! \times 6^4 = 24 \times 1296 = 31104$.

2.9.2 Voľba prepojení

Prepojenie znakov na klávesnici, vstupnom disku a reflektore boli pevne zabudované, preto som si náhodne zvolil tieto prepojenia. Zvolil som si tiež prepojenia v jednotlivých rotoroch a rozloženie blokovacích pinov.

Tieto údaje sú znázornené v nasledujúcich tabuľkách:

Vstup	1	2	3	4	5	6
Výstup	3	6	4	1	2	5

Tab. 12. Prepojenie klávesnice

Vstup	1	2	3	4	5	6
Výstup	5	4	2	3	6	1

Tab. 13. Prepojenie vstupného disku

Vstup	1	2	3	4	5	6
Výstup pri šifrovaní	2	1	3	5	6	4
Výstup pri dešifrovaní	2	1	3	6	4	5

Tab. 14. Prepojenie na reflektore

Vstup	1	2	3	4	5	6
Rotor1	6	3	5	2	4	1
Rotor2	5	3	1	6	2	4
Rotor3	3	6	4	1	5	2
Rotor4	4	1	3	2	6	5

Tab. 15. Prepojenie rotorov

Pozn.: Čítačka kariet je vynechaná zo skrátenej verzie, absencia karty spôsobuje identické zobrazenie jednotlivých znakov.

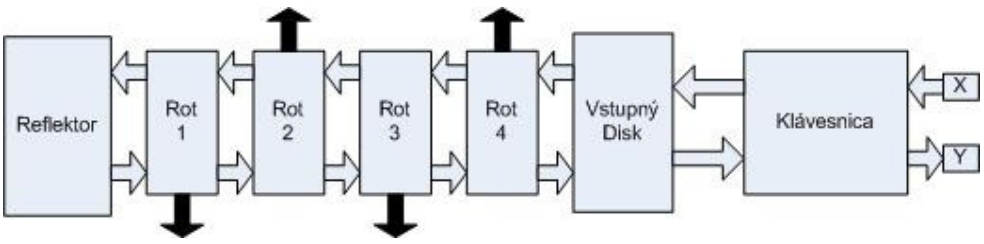
Blokovacie piny som si zvolil tiež náhodne. Táto verzia bude obsahovať pevne nastavené pozície pinov. Pohyb rotora č. 2 závisí od prítomnosti blokovacieho pinu na rotore č. 4. a pohyb rotora č. 3. závisí od prítomnosti pinu na rotore č. 1.

Pozn.: Prítomnosť blokovacích pinov budeme sledovať v danom kroku na pozícii rotora. Na pôvodnej Fialke sa sleduje prítomnosť pinov o 17 (párny rotor) resp. 20 (nepárny rotor) miest ďalej v smere hodinových ručičiek. Napr.: keď je rotor č. 1. (nepárny) nastavený na 3. pozíciu tak prítomnosť pinu na 23 kontakte (3+20) zabraňuje rotoru č. 3, č. 5, ... v pohybe.

Vstup	1	2	3	4	5	6
Rotor1	1	0	1	0	1	0
Rotor2	0	1	0	0	0	1
Rotor3	0	0	0	1	0	0
Rotor4	1	1	0	0	1	0

Tab. 16. Rozloženie blokovacích pinov 1- prítomnosť, 0- absencia

2.9.3 Výsledný blokový diagram



Obr. 20. Blokový diagram skrátenej verzie, X - vstup , Y - výstup, čierna šípka označuje smer otáčania rotorov

Vstupom zariadenia je klávesnica obsahujúca šesť zvolených písmen.
Po zadaní vstupného znaku sa aplikuje substitúcia na klávesnici z Tab. 12. (S1)
Znak prejde cez vstupný disk, kde sa aplikuje substitúcia z Tab. 13. (S2)
Vstupný disk podá znak ďalej na rotor č. 4. , ten ho podá ďalej na rotor č. 3, ten na rotor č. 2, ten na rotor č. 1. Na každom rotore je uskutočnená substitúcia pre príslušné nastavenie.
Rotor č. 1. podá znak na reflektor kde je realizovaná ďalšia substitúcia z Tab. 15. (R(u)) .
Znak je zároveň odrazený naspať cez rotor č. 1, č. 2, č. 3., č. 4., cez vstupný disk až na klávesnicu. Na odrazený signál sa aplikuje inverzná substitúcia z príslušných tabuliek.
Formálne môžeme šifrovaciu funkciu zapísať ako

$$y = S_1^{-1} S_2^{-1} Rot_4^{-1} Rot_3^{-1} Rot_2^{-1} Rot_1^{-1} R(u) Rot_1 Rot_2 Rot_3 Rot_4 S_2 S_1 (x)$$

Pozn.: Substitúcia znaku na jednotlivých rotoroch je nasledujúca:

- priráta sa nastavená poloha rotora
- aplikuje sa substitúcia z Tab. 15.
- odráta sa nastavená poloha rotora

(nastavená poloha rotora v našom prípade je príslušné označenie z Tab. 11.)

Po zašifrovaní znaku nasleduje krokovanie rotorov.

2.9.4 Šifrovanie a dešifrovanie

Príklad :

- Nastavme si nasledujúce poradie rotorov: „1-2-3-4“
- Na každom rotore si zvoľme ako počiatočne písmeno prvý kontakt „a“ („1“). („1-1-1-1“)

Dostali sme správu, ktorú chceme pri daných nastaveniach (pri danom kľúči) zašifrovať a následne dešifrovať.
Správa: „abd“

- Správu napíšme v číselnej podobe z Tab. 11.
  „abd“ = „124“
- Teraz zašifrujme prvý znak „1“:
  1. Na klávesnici sa číslo „1“ vymení za číslo „3“ z Tab. 12.
  2. Na vstupnom disku sa vymení číslo „3“ za číslo „2“ z Tab. 13.

3. Pripočíta sa k „2“ aktuálna pozícia rotora č.4., ktorý je v našom prípade „1“.
   Teda vstup je „3“.
   Na rotore č. 4. sa zmení „3“ na „3“ z Tab. 15.
   Odráta sa aktuálna poloha rotora č.4. - „1“. Výstup „2“.
4. Pripočíta sa k „2“ aktuálna pozícia rotora č.3. - „1“. Teda vstup je „3“.
   Na rotore č. 3. sa zmení „3“ na „4“ z Tab. 15.
   Odráta sa poloha „1“. Výstup „3“.
5. Pripočíta sa „1“. Vstup: „4“
   Na rotore č. 2. sa zmení „4“ na „6“ z Tab. 15.
   Odrátame „1“, výstup je „5“
6. Pripočíta sa „1“. Vstup: „6“
   Na rotore č. 1. sa zmení „6“ na „1“ z Tab. 15.
   Odráta sa poloha „1“, výstupom je „6“
   (1-1 = 0 = 6 v mod6)
7. Na reflektore sa zmení č. „6“ na číslo „4“ z Tab. 14.
8. Pripočíta sa k „4“ aktuálna pozícia rotora č.1. - „1“. Teda vstup je „5“
   Na rotore č. 1. sa zmení „5“ na „3“, inverzná substitúcia z Tab. 15.
   Odráta sa poloha „1“, výstupom je „2“
9. Pripočíta sa k „2“ aktuálna pozícia rotora č.2. - „1“, vstup: „3“
   Na rotore č. 2. sa zmení „3“ na „2“, inv. sub. z Tab. 15.
   Odráta sa „1“, výstupom je „1“.
10. Pripočíta sa k „1“ aktuálna pozícia rotora č.3. - „1“, vstup: „2“
    Na rotore č. 3. sa zmení „2“ na „6“, inv. sub. z Tab. 15.
    Odráta sa „1“, výstupom je „5“.
11. Pripočíta sa k „5“ aktuálna pozícia rotora č.4. - „1“, vstup: „6“
    Na rotore č. 4. sa zmení „6“ na „5“, inv. sub. z Tab. 15.
    Odráta sa „1“, výstupom je „4“.
12. Inverzná substitúcia čísla „4“ na vstupnom disku z Tab. 13, výstup: „2“
    Inverzná substitúcia čísla „2“ na vstupnom disku z Tab. 12, výstup: „5“

    Teda sme znak „a“ zašifrovali na znak „e“.

- Krokovanie rotorov:
  1. Párne rotory s číslom 2 a 4

Krajný rotor č. 4 sa pohybuje pri každom stlačení klávesy, a posunie sa v smere hodinových ručičiek o jedno miesto, nová pozícia rotora bude teda „6“ (aktuálna poloha „1“ – jedno miesto).

Z Tab.16. zistíme absenciu pinu na 6. kontakte 4.-ho rotora.

Teraz sa posunie rotor č. 2, tiež o jedno miesto, v tom istom smere. Nová pozícia je „6“.

2. Nepárne rotory s číslom 1 a 3

Krajný rotor č. 1 sa pohybuje pri každom stlačení klávesy, posunie sa proti smeru hodinových ručičiek o jedno miestom teda nová pozícia rotora bude „2“ (aktuálna poloha „1“ + jedno miesto).

Z Tab.16. zistíme absenciu pinu na 2. kontakte 1.-ho rotora.

Teraz posunieme rotor č. 3 tiež o jedno miesto v tom istom smere. Nová pozícia je „2“.

Nová aktuálna pozícia rotorov teda bude „2-6-2-6“

Zašifrovanie znakov je popísane v nasledujúcej tabuľke:

Poloha rotorov	1-1-1-1	2-6-2-6	3-5-3-6
Vstup	a – „1“	b – „2“	d – „4“
Substitúcia na klávesnici	1 – 3	2 – 6	4 – 1
Substitúcia na vstupný disk	3 – 2	6 – 1	1 – 5
Substitúcia na rotore 4	3 – 3	1 – 4	5 – 6
Substitúcia na rotore 3	3 – 4	6 – 2	3 – 4
Substitúcia na rotore 2	4 – 6	6 – 4	6 – 4
Substitúcia na rotore 1	6 – 1	6 – 1	2 – 3
Substitúcia na reflektore	6 – 4	5 – 6	6 – 4
Inverzná substitúcia na rotore 1	5 – 3	2 – 4	1 – 6
Inverzná substitúcia na rotore 2	3 – 2	2 – 5	2 – 5
Inverzná substitúcia na rotore 3	2 – 6	1 – 4	3 – 1
Inverzná substitúcia na rotore 4	6 – 5	2 – 4	4 – 1
Inverzná substitúcia vstupný disk	4 – 2	4 – 2	1 – 6
Inverzná substitúcia klávesnici	2 – 5	2 – 5	6 – 2
Výstup	e – „5“	e – „5“	b – „2“
Poloha rotorov po krokovaní	2-6-2-6	3-5-3-6	4-4-4-5

Tab. 17. Postupnosť pri zašifrovaní znakov „abd“

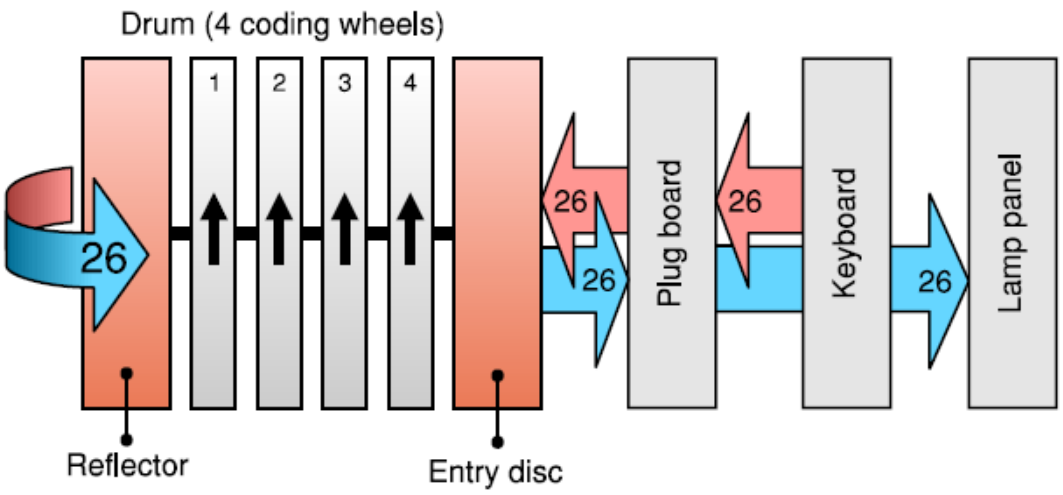
Dešifrovanie funguje na tom istom princípe. Jediný rozdiel je, že substitúcia na reflektore sa aplikuje z inej tabuľky ako pri zašifrovaní. Dôležité je, aby sme pred začiatkom dešifrovania nastavili rotory tak, ako pred zašifrovaním prvého znaku.

Poloha rotorov	1-1-1-1	2-6-2-6	3-5-3-6
Vstup	e – „5“	e – „5“	b – „2“
Substitúcia na klávesnici	5 – 2	5 – 2	2 – 6
Substitúcia na vstupný disk	2 – 4	2 – 4	6 – 1
Substitúcia na rotore 4	5 – 6	4 – 2	1 – 4
Substitúcia na rotore 3	6 – 2	4 – 1	1 – 3
Substitúcia na rotore 2	2 – 3	5 – 2	5 – 2
Substitúcia na rotore 1	3 – 5	4 – 2	6 – 1
Substitúcia na reflektore	4 – 6	6 – 5	4 – 6
Inverzná substitúcia na rotore 1	1 – 6	1 – 6	3 – 2
Inverzná substitúcia na rotore 2	6 – 4	4 – 6	4 – 6
Inverzná substitúcia na rotore 3	4 – 3	2 – 6	4 – 3
Inverzná substitúcia na rotore 4	3 – 3	4 – 1	6 – 5
Inverzná substitúcia vstupný disk	2 – 3	1 – 6	5 – 1
Inverzná substitúcia klávesnici	3 – 1	6 – 2	1 – 4
Výstup	a – „1“	b – „2“	d – „4“
Poloha rotorov po krokovaní	2-6-2-6	3-5-3-6	4-4-4-5

Tab. 18. Postupnosť pri dešifrovaní znakov „abd“

3 Enigma

3.1 Technické detaily a blokové diagramy Enigmy



Obr. 21. Blokový diagram Enigmy: (prevzaté z [1])

Jadro Enigmy je súprava pohybujúcich sa rotorov, ktorá sa nazýva drum a nachádza sa medzi vstupným diskom a reflektorom. Enigma používa klávesnicu ako vstup, a lampový panel ako výstup. Klávesnica má 26 kláves. Pri stlačení klávesy je vyslaný elektrický prúd z klávesnice, cez súpravu šifrovacích zariadení. Signál najprv prejde cez plug board čo dovolí dvojici písmen aby sa vymenili. Signál z plug boardu je poslaný na vstupný disk, ktorý pošle signál ďalej pravému rotoru (číslo 4), ten pošle tretiemu atď., až k reflektoru, ktorý je na ľavej strane. Vo vnútri reflektora je každý kontakt prepojený s ďalším kontaktom (spolu 13 párov kontaktov), ktorý efektívne odráža prúd naspäť do súpravy rotorov. Prúd prejde všetkými štyrmi rotormi (tento krát opačným smerom), vstupným diskom a plug boardom, kým na konci rozsvieti jeden z 26 lámp.

Výhodou používania reflektora je reciprocita operácie. Inými slovami, celý proces sa dá obrátiť. Na rozšifrovanie správy musí byť dešifrovacie zariadenie nastavené presne tak, ako je šifrovacie zariadenie. Táto metóda však má jednu nevýhodu: žiadne písmo nemôže byť zakódované samo na seba.

4 Zhrnutie rozdielov medzi Fialkou a Enigmou

Názov	**Enigma**	**Fialka**	**Číslo poznámky**
Počet rotorov	3-4	10	1.)
Pretáčanie rotora	pomalé	rýchle	2.)
Smer pretáčania	jeden	dva	3.)
Výstup	Lampový panel	Tlačiareň, dierkovač	4.)
Seba-zakódovanie znaku	nie	áno	5.)

Tab. 19. Zhrnutie rozdielov medzi Fialkou a Enigmou

1.) Fialka používa viac rotorov, čo značne zvýši maximálny počet permutácií.

2.) V prípade Enigmy, pravý krajný rotor sa krokuje s každým stlačením klávesy. Keď pravý krajný rotor sa raz úplne otočí, posunie rotor na ľavo od neho o jeden krok. Fialka používa na krokovanie dve mechanicky nezávislé časti. Konkrétny rotor pohyb susedného rotora nikdy neovplyvní, ovplyvní ale pohyb rotora o jedno miesto ďalej. Krokovanie nasledujúcich rotorov závisí na prítomnosti blokovacích pinov.

3.) Rotory na Enigme sa otáčajú v jednom smere, kým na Fialke sa priľahlé rotory otáčajú v opačnom smere.

4.) Enigma používa ako výstup lampový panel, podľa výsledného znaku sa rozsvieti jedna lampa.

Fialka posiela výstupný znak na riadenie tlačiarne a dierkovača.

5.) Na Enigme sa znak nikdy nemôže byť zakódovaný sám na seba, aby stroj nestratil svoju reciprocitu. Používa len cykly dĺžky 2 .

Na Fialke tento problém vyriešili a pomocou jedného obvodu zanechali aj reciprocitu.

Používa cykly dĺžky 2 a jeden cyklus dĺžky 3.

5 Záver

Rotorové šifrátory predstavujú teoretický aj technický vrchol kryptografických strojov. Vývojový vrchol bezpochybne predstavujú tie, ktoré boli skonštruované pre použitie v druhej svetovej vojne. Sem sa zaraďuje aj Enigma, ktorá patrí medzi najznámejšie rotorové šifrátory a ktorá zahrala dôležitú úlohu počas vojny.
Enigma však mala aj slabé stránky. Svedčí o tom aj to, že v roku 1933 bola prelomená poľskými analytikmi.

V tejto práci som sa zaoberal analýzou rotorového šifrátora Fialka M-125 a s jeho nadväznosťou na Enigmu. Fialka bola a stále je považovaná za relatívne bezpečnú šifru. Hlavnou silou jej neprelomiteľnosti bolo jej utajenie.

Cieľom tejto práce bolo popísanie vlastností Fialky a zistenie jednotlivých vylepšení oproti Enigme. Na sledovanie činnosti tejto šifry (verzia M-125-xx s prepojením rotorov série 6K) bol vytvorený simulátor, ktorého použitie predstavuje veľmi silný prostriedok pre ochranu dát.

Ďalším cieľom bolo navrhnúť skrátenú verziu Fialky, ktorá umožňuje ľahšie študovanie jej princípu.

Vytvorené aplikácie môžu byť použité aj ako učebné pomôcky. Zverejnené sú na stránke www.bc.fialka.szm.com a budú tiež zlinkované z web stránky predmetu Klasické Šifry.

Použitá literatúra

[1] P. Reuvers, M. Simons: Codename Fialka, 2005
Dostupné elektronicky 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

[9] http://wapedia.mobi/en/Fialka

[10] http://www.pcrevue.sk/buxus_dev/generate_page.php?page_id=2288

Príloha A: Používateľská príručka

Inštalácia a spustenie

Aplikácie na simuláciu šifrátora boli vytvorené v programovacom jazyku Java v prostredí NetBeans IDE 6.1. Na spustenie týchto aplikácii je nutné si nainštalovať Java Run Environment (JRE) v operačnom systéme. Bližšie informácie a inštalačný súbor nájdete na domovskej stránke www.java.sun.com .

Pre spustenie zdrojového kódu je potrebné si nainštalovať vývojové prostredie NetBeans a vývojový nástroj Java Development Kit (JDK). Inštalačný súbor ako aj podrobnejšie informácie sú dostupné z domovskej stránky www.java.sun.com .
Inštalačný súbor NetBeans IDE 6.1 a JDK 6u7 sú tiež dostupné z elektronického média.

Kompatibilitu pre iné prostredie autor nezaručuje.

Ovládanie programu

Simulator umožňuje študovať činnosť Fialky a overovať si rôzne nastavenia.
Ovládanie programu ako aj rôzne nastavenia sú súčasťou video-tutoriálov dostupných na elektronickom médiu, preto spomeniem len hlavné črty:
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.

Pozn.: Skrátená verzia obsahuje len klávesnicu s 6 znakmi a nie je možné si nastaviť textové pole ako vstup.

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.

Príloha B: Obsah elektronického média

Príloha obsahuje súbory rozčlenené do nasledujúcich adresárov:

- dokumentacia – obsahuje tento dokument v elektronickej forme vo formátoch
  - .doc
  - .pdf.

- Java – obsahuje súbory na inštaláciu vývojového prostredia NetBeans
  - JDK-6u7
  - NetBeans-6.1

- program – obsahuje vytvorené programy v dvoch knižniciach:
  1. Antal_Bakalarska_praca – súbory patriace k normálnej verzie
  2. Antal_Bakalarska_praca_part2 – súbory patriace ku skrátenej verzie

  Jednotlivé knižnice obsahujú:
  – build – knižnica obsahujúca skompilované súbory
  - dist - knižnica obsahuje spustiteľný archív programu vo formáte .jar
  Pozn.: samostatne sa tento súbor nespúšťa, lebo sa jedná o applet
  – src – knižnica obsahujúca zdrojové súbory programu
  – nbproject – knižnica obsahujúca projekt

- video_tutorial – obsahuje vytvorené pomocné videá

Príloha C: Webová stránka

Vytvorené učebné pomôcky

- webová aplikácia skrátenej verzie Fialky
- webová aplikácia Fialky M-125-xx
- Video-tutorialy

sú dostupné tiež aj na internetovej adrese: www.bc.fialka.szm.com a budú tiež zlinkované z web stránky predmetu Klasické Šifry.