

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE  
Fakulta elektrotechniky a informatiky

Študijný program APLIKOVANÁ INFORMATIKA

S T U · ·  
· · · · ·  
· F E I ·  
· · · · ·

**POROVNANIE ROTOROVÝCH ŠIFRÁTOROV  
ENIGMA A FIALKA M-125**

Bakalárska práca

Autor: Eugen Antal

Vedúci bakalárskej práce:  
prof. RNDr. Otokar Grošek, PhD.

Bratislava, máj 2009

**SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE**  
**FAKULTA ELEKTROTECHNIKY A INFORMATIKY**  
**ODBOR APLIKOVANÁ INFORMATIKA**

---

**Z A D A N I E**  
Bakalárska práca

# **ANOTÁCIA**

## **SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE Fakulta elektrotechniky a informatiky**

---

Katedra aplikovanej informatiky a výpočtovej techniky

Študijný program:

**APLIKOVANÁ INFORMATIKA**

Autor:

Eugen Antal

Názov bakalárskej práce:

**POROVNANIE ROTOROVÝCH  
ŠIFRÁTOROV ENIGMA A FIALKA M-125**

Vedúci bakalárskej práce:

prof. RNDr. Otokar Grošek, PhD.

Rok odovzdania:

máj 2009

Fialka M-125 je rotorový šifrátor vytvorený Sovietskou armádou, ktorá sa používala počas studenej vojny. Fialka je založená na princípe rotorového šifrátoru Enigma. Informácie ohľadom šifrátoru boli dlhú dobu utajené, a pre verejnosť nedostupné. Cieľom tejto práce bolo vytvorenie dokumentácie o činnosti tohto stroja.

V tomto dokumente je uvedený stručný prehľad Fialky. Cez jednotlivé kapitoly je popísaný princíp fungovania stroja a rozdiely oproti Enigme. Súčasťou práce je vytvorenie webovej aplikácie na simuláciu, ktorá umožňuje študovať činnosť Fialky a overovať si rôzne nastavenia. Konečným cieľom je vytvorenie skrátenej verzie simulátora, ktorá funguje na princípe Fialky a umožňuje jeho využitie ako učebnej pomôcky.

# **ANNOTATION**

**SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA**  
**Faculty of Electrical Engineering and Information Technology**

---

**Department of Applied Informatics and Information Technology**

<b>Curriculum:</b>	<b>APPLIED INFORMATICS</b>
<b>Author:</b>	Eugen Antal
<b>Title of the diploma thesis:</b>	<b>COMPARE OF ROTOR-CIPHER MACHINES ENIGMA &amp; FIALKA M-125</b>
<b>Supervisor:</b>	prof. RNDr. Otokar Grošek, PhD.
<b>Year of the submission:</b>	May 2009

Fialka M-125 is a rotor-cipher machine created by the Soviet Army, what was used during the Cold-War. Fialka is largely based on the cipher machine named Enigma. Information regarding the machine was kept secret for a long time and unavailable to community. The goal of this work is to create a description of this machine.

In this documentation is referred a brief description of this cipher machine. Through following chapters is described how it works and its differences between Enigma. A part of this work is to create a web application which allows self-study of Fialka and to examine different settings. The final goal is to create a short version of this simulator, which works as Fialka itself, and can be also used as a teaching aid.

# **POUČENIE**

Vychádzajúc z dokumentov

1. „**Zákon o autorskom práve a právach súvisiacich s autorským právom (Autorský zákon) č. 618/2003 Zb. z.“**
2. **Pokyn dekana FEI STU č. 1/2006**

a tiež z faktu, že výsledkom bakalárskej práce môže byť v zmysle vyššie citovaného zákona tzv. "školské dielo", považuje FEI STU za potrebné upozorniť všetkých autorov bakalárskych prác, že v zmysle § 51, odseky (1) a (2)

(1) škola môže uzatvoriť s autorom licenčnú zmluvu o použití školského diela za zvyčajných podmienok; ak autor bez závažného dôvodu odmieta licenčnú zmluvu uzatvoriť, môže sa škola domáhať, aby obsah tejto zmluvy určil súd

(2) ak nie je dohodnuté inak, autor "školského diela" môže použiť svoje dielo alebo poskytnúť licenciu inému, ak to nie je v rozpore s oprávnenými záujmami školy.

Potvrdzujem vlastnoručným podpisom, že som zobraľ na vedomie vyššie citované informácie zo zákona č. 618/2003 Zb. z..

.....  
Eugen Antal

V Bratislave, dňa .....

Poznámka:

Úplné znenie zákona č. 618/2003 Zb.z. môžete nájsť na adrese [www.zbierka.sk](http://www.zbierka.sk).

## Pod'akovanie

Týmto by som sa chcel pod'akovať prof. RNDr. Otokarovi Grošekovi, PhD. za jeho rady a organizačné vedenie pri vypracovaní tejto práce. Ďalej by som sa chcel pod'akovať svojej priateľke, rodine a kamarátom za poskytnutú pomoc a morálnu podporu.

## Čestné prehlásenie

Prehlasujem, že som bakalársku prácu, vrátane príloh, som vypracoval samostatne na základe mojich vedomostí a použitej literatúry.

.....  
Eugen Antal

V Bratislave, dňa .....

## Zoznam obrázkov

Obr. 1. Čelný pohľad na Fialku.....	12
Obr. 2. Pohľad zhora po odstránení držiaku rukopisu (copy holder).....	14
Obr. 3. Ľavá strana Fialky.....	15
Obr. 4. Pravá strana Fialky.....	15
Obr. 5. Vnútro Fialky.....	16
Obr. 6. Klávesnica Fialky M-125-xx.....	17
Obr. 7. Klávesnica Fialky M-125-3xx .....	17
Obr. 8. Sada rotorov Fialky.....	18
Obr. 9. Rotor z Fialky.....	21
Obr. 10. Označené rotory a smer otáčania rotorov.....	23
Obr. 11. Ručná páka.....	25
Obr. 12. Súprava rotorov.....	26
Obr. 13. Revízny zoznam.....	27
Obr. 14. Blokový diagram Fialky M-125-xx.....	28
Obr. 15. Blokový diagram Fialky M-125-3xx.....	30
Obr. 16. Schéma šifrátoru Fialka M-125-xx.....	31
Obr. 17. Schéma fungovanie Fialky.....	33
Obr. 18. Zvolené rotory pre skrátenú verziu.....	34
Obr. 19. Zvolené rotory so šiestimi kontaktmi.....	35
Obr. 20. Blokový diagram skrátenej verzie.....	36
Obr. 21. Blokový diagram Enigmy.....	41

## Zoznam tabuľiek

Tab. 1. Cyrilská abeceda.....	18
Tab. 2. Prepojenie kontaktov na Test reflektore.....	20
Tab. 3. Prepojenie rotorov Fialky M-125 série 3K.....	22
Tab. 4. Prepojenie rotorov Fialky M-125 série 6K.....	22
Tab. 5. Prepojenie rotorov Fialky M-125 série 4K – neznáme.....	22
Tab. 6. Substitúcia z klávesnice na čítačku kariet.....	29
Tab. 7. Substitúcia z čítačky kariet na vstupný disk.....	29
Tab. 8. Substitúcia na reflektore.....	29
Tab. 9. Substitúcie na reflektore .....	31
Tab. 10. Substitúcie na reflektore .....	31
Tab. 11. Použitá abeceda a jeho označenie.....	35
Tab. 12. Prepojenie klávesnice.....	35
Tab. 13. Prepojenie vstupného disku.....	35
Tab. 14. Prepojenie na reflektore.....	35
Tab. 15. Prepojenie rotorov.....	36
Tab. 16. Rozloženie blokovacích pinov .....	36
Tab. 17. Postupnosť pri zašifrovaní znakov „abd“.....	39
Tab. 18. Postupnosť pri dešifrovaní znakov „abd“.....	40
Tab. 19. Zhrnutie rozdielov medzi Fialkou a Enigmou.....	42

# **Obsah**

Zoznam obrázkov.....	8
Zoznam tabuliek .....	9
Obsah.....	10
1    Úvod.....	11
2    Fialka M-125 .....	12
2.1    História Fialky .....	12
2.2    Charakteristika Fialky.....	13
2.3    Vonkajší popis zariadenia .....	14
2.4    Rozdiel medzi verziami M-125-xx a M-125-3xx .....	17
2.5    Rotory .....	18
2.5.1    Test reflektor .....	20
2.5.2    Prepájanie rotorov.....	21
2.5.3    Krokovanie rotorov.....	23
2.6    Príslušenstvo .....	25
2.7    Technické detaily a blokové diagramy Fialky .....	28
2.7.1    Základná schéma Fialky .....	31
2.7.2    Postupnosť udalostí pri fungovaní Fialky .....	32
2.8    Vytváranie kľúčov - nastavenie Fialky .....	33
2.9    Skrátená verzia Fialky .....	34
2.9.1    Volba počtu rotorov a znakov .....	34
2.9.2    Volba prepojení .....	35
2.9.3    Výsledný blokový diagram .....	36
2.9.4    Šifrovanie a dešifrovanie.....	37
3    Enigma .....	41
3.1    Technické detaily a blokové diagramy Enigmy .....	41
4    Zhrnutie rozdielov medzi Fialkou a Enigmou.....	42
5    Záver.....	43

# 1 Úvod

Spochybnená bezpečnosť šifier s malou periódou opakovaných znakov viedla k využitiu kľúčov, meniacich sa pri šifrovaní každého znaku. Tak došlo k návrhu nových typov šifier. Do tejto skupiny patria aj rotorové šifrátory ( V týchto šifrátoroch sa k i-temu znaku  $x_i$  otvoreného textu priraduje znak  $y_i$  pomocou permutácie  $\pi$  a kľúčov  $k_i, \lambda_i$  v tvare  $y_i = \pi(x_i + k_i) - \lambda_i$ ). Výpočet sa realizuje na elektromechanickom princípe.

Myšlienkou rotorového šifrátora sa zaoberali aj mnohí konštruktéri, ako napríklad Američan Edward Hebern a Holandčan Hugo Alexander Koch. Patent nakoniec odkúpil nemecký inžinier Scherbius, a v roku 1924 predstavil svoj vlastný fungujúci stroj, ktorý nazval Enigma.

Enigma zohrala významnú úlohu počas druhej svetovej vojny, kde bola používaná Nemeckou armádou.

Okolo roku 1965 Sovietska armáda uviedla nový šifrovací stroj menom Fialka. Dizajn a fungovanie tohto nového stroja boli založené na podobnom princípe ako je Enigma, ale pri jej tvorbe sa pokúsili napraviť chyby Enigmy.

Odlišné verzie Fialky sa objavili v bývalom Československu, na území východného Nemecka a v Poľsku. Po páde Sovietskeho zväzu vydali príkaz na pozbieranie a zničenie vydaných strojov, čo bolo súčasťou zmluvy, ktorá hovorila len o zápožičke. Zachránilo sa len málo kusov. Z toho dôvodu je skúmanie Fialky v dnešnej dobe veľmi náročné.

Popis tejto práce bol vytvorený pomocou na konci uvedenej použitej literatúry. Vytvorené aplikácie sú vlastné.

## 2 Fialka M-125

Fialka je ruské slovo, ktoré v preklade znamená fialovú farbu alebo kvet. Fialka bola využívaná Sovietskou armádou počas studenej vojny. Existujú dva verzie šifrátoru: M-125-xx a M-125-3xx. Šifrovací stroj sa nazýva M-125, kým Fialka je meno šifrovacej procedúry. Dizajn a fungovanie Fialky sú založené na princípe šifrátoru Enigma, ktorú používala Nemecká armáda počas druhej svetovej vojny.



**Obr. 1.** Čelný pohľad na Fialku (prevzaté z [8] )

### 2.1 História Fialky

Fialka bola prvý krát uvedená okolo roku 1965. Dlhú dobu sa predpokladalo, že Sovietska armáda nemá detailné informácie o Enigme. Z nápadnej podobnosti Fialky a Enigmy sa ale narodila myšlienka, že Sovietsi mali podrobňší popis Enigmy. Pri tvorbe Fialky brali do úvahy aj nedostatky Enigmy a pokúsili sa o napravenie jej chýb.

Táto myšlienka bola podložená príbehom, čo zverejnili v roku 1999. Príbeh odhalil študenta, Ruského špióna Johna Cairncrossa, ktorý pracoval na projektoch zlomenia nemeckých šifier v Bletchley Parku v Anglicku.

Podrobnejšie informácie o Fialke boli neúplné až do roku 2005, kedy Paul Reuvers a Marc Simons vydali prvý manuál s podrobným popisom.

## 2.2 Charakteristika Fialky

Na zakódovanie písmen napísaných na klávesnici používa Fialka, podobne ako Enigma niekoľko rotorov. Pri každom stlačení klávesy sa rotory nastavia na novú pozíciu, čím efektívne menia substitúciu pre každý znak napísaný na klávesnici. Stlačením klávesy sa zakódovaný znak tlačí priamo na diernu pásku. V tom istom čase sa znak môže objaviť aj vo forme 5-bitového digitálneho kódu a to spôsobom dierkovania (razenia).

Stroj obsahuje aj vysielač diernej pásky, ktorý je možné použiť na zaslanie alebo kopírovanie správy.

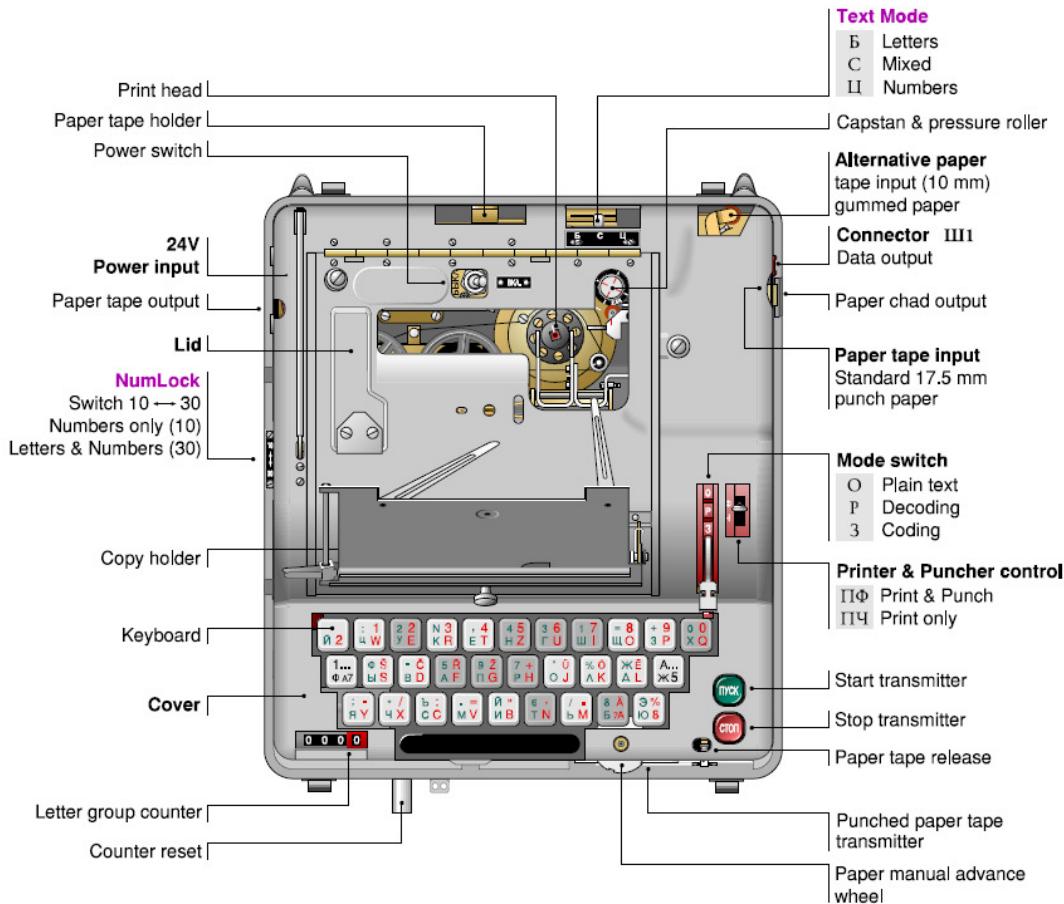
Pri tvorbe Fialky sa poučili z chýb Enigmy, a zrealizovali nasledovné vylepšenia:

- 10 rotorov oproti 3-4 v Enigme, čo značne zvýšilo maximálny počet permutácií
- častejšie pretáčanie rotora
- príahlé rotory sa pohybujú v opačnom smere
- používanie čítačky kariet oproti plug board Enigmy, čo redukuje počet chýb pri nastavení
- sebazakódovateľnosť znaku
- využíva 30 znakov, kým Enigma len 26

Ďalšie vlastnosti Fialky:

- môže byť nastavená na používanie písmen, čísel, alebo oboch na raz
- môže kopírovať diernu pásku
- môže byť použitá ako štandardný písací stroj
- používa cyrilské ako aj latinské písmo

## 2.3 Vonkajší popis zariadenia



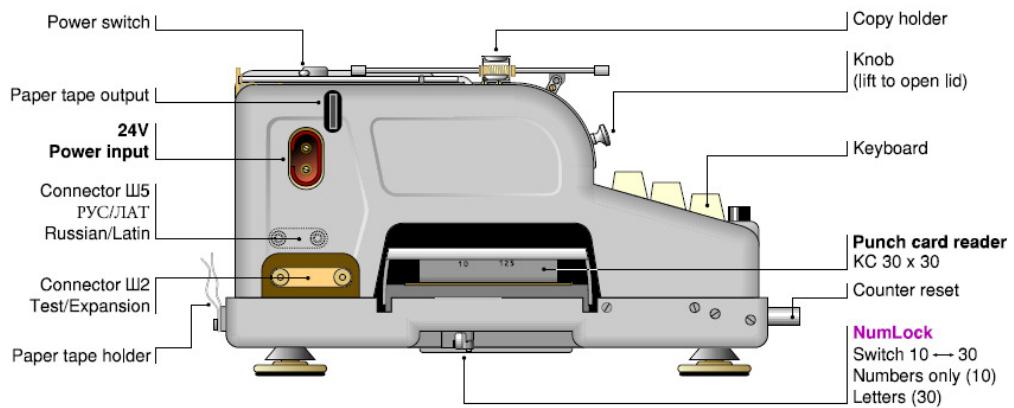
Obr. 2. Pohľad zhora po odstránení držiaku rukopisu (copy holder) (prevzaté z [1] )

Prepínač módov (Mode Switch) – slúži na nastavenie šifrátoru na jednu z 3 možností:

- О** – čistý text, režim „písací stroj“ – bez šifrovania
- Р** – Decoding - režim rozšifrovania správy
- З** – Coding - režim zašifrovania správy.

Vpravo od prepínača módov sa nachádza ďalší prepínač (Printer & Puncher control) na ovládanie papiera - dierovač a /alebo tlač.

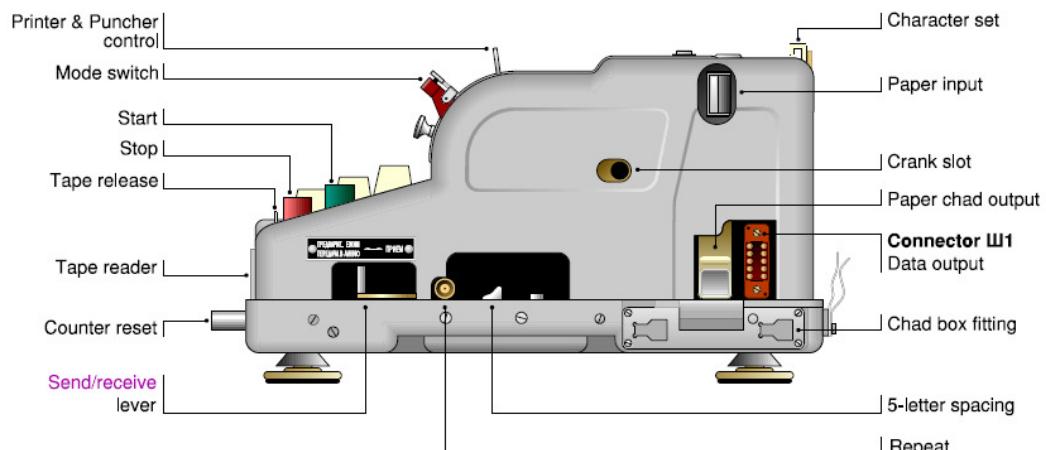
Na dolnej časti sú tlačidlá (Start, Stop) na ovládanie čítania diernej pásky. Tlačidlá sa používajú na priame odoslanie správy z diernej pásky.



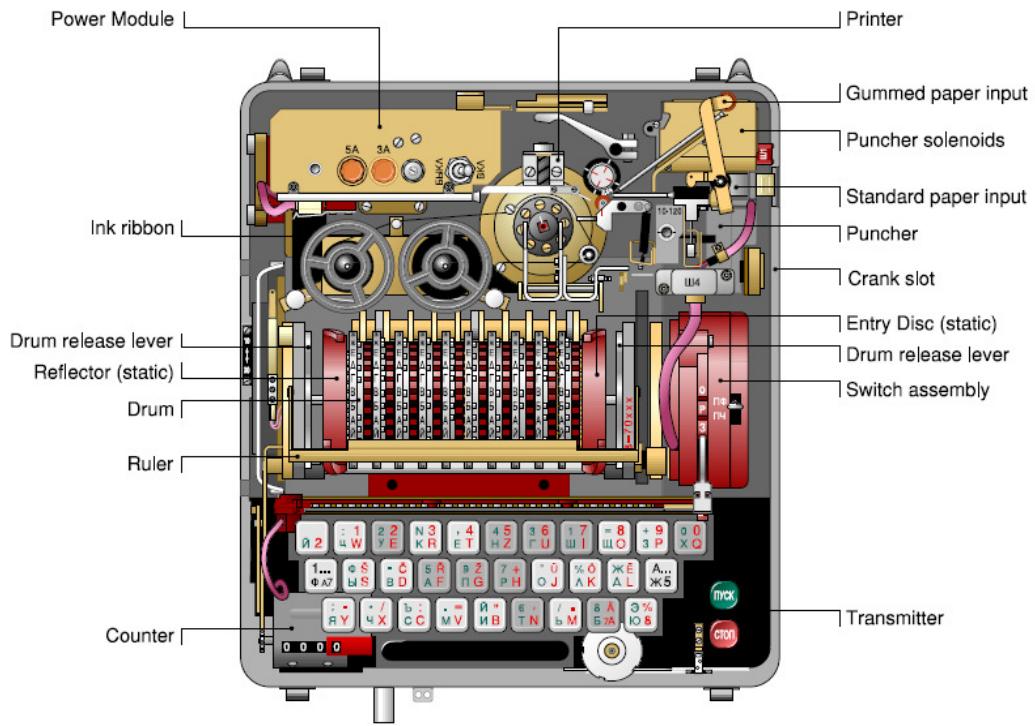
Obr. 3. Ľavá strana Fialky (prevzaté z [1] )

Na ľavej strane stroja sa nachádza čítačka diernej pásky a zásuvka na zapájanie.

Pod čítačkou sa nachádza prepínač (NumLock), na prepínanie medzi písaním písmenom a číslom.



Obr. 4. Pravá strana Fialky (prevzaté z [1] )



**Obr. 5.** Vnútro Fialky (prevzaté z [1] )

Kovová schránka vľavo hore obsahuje zásuvku, poistky a hlavný vypínač, ktoré sú priamo pripojené na motor a dodávajú energiu zvyšku zariadenia. Vpravo sa nachádza tlačové zariadenie. Atramentová pánska (ink ribbon) je okolo tlačovej hlavy. Text sa tlačí priamo na diernu pásku, do ktorej je možné zároveň naraziť informáciu pomocou dierkovača napravo. V strede sa nachádza kódovacie zariadenie, obsahujúce sadu desiatich rotorov. Rotory sa pohybujú pri každom stlačení klávesy. Pomocou dvoch veľkých bakelitových diskov sa pripájajú oba konca sady rotorov k ďalšej časti stroja. Disk na pravej strane sa nazýva vstupný disk (entry disk), disk na ľavej strane sa nazýva reflektor.