PŘÍRODOVĚDECKÁ FAKULTA UNIVERZITY PALACKÉHO
KATEDRA INFORMATIKY

BAKALÁŘSKÁ PRÁCE

Simulátor šifrovacího stroje

2013 Zdeněk Fuchs

Anotace

Vytvoření simulátoru šifrovacího stroje Enigma M4. Pomocí softwarové aplikace je demonstrováno jakým způsobem dochází k transformaci šifrovaného znaku v jednotlivých elektrických a mechanických částech šifrovacího stroje. Simulátor je vytvořen pomocí grafického subsystému Microsoft Windows Presentation Foundation, na počítačové platformě Microsoft .NET Framework 4. Výsledná aplikace je určena jako metodická pomůcka pro lektory, případně pro zájemce o obor kryptografie.

Děkuji panu RNDr. Arnoštu Večerkovi za odborné konzultace při vypracování této bakalářské práce a za poskytnutí podkladových materiálů.

Obsah

Seznam obrázků

Seznam tabulek

1. Úvod

Úkolem je sestavit softwarovou aplikaci demonstrující činnost šifrovacího stroje. Šifrovací stroj, vybraný ke zpracování, má typové označení Enigma M4. Tento typ šifrovacího stroje byl používán během 2. světové války na ponorkách německého válečného loďstva (German Kriegsmarine). Poprvé byl nasazen v únoru roku 1942. Většina programově zpracovaných šifrovacích strojů je vytvořena formou "černé skříňky". Jen u málokterých z nich jde vidět, jak k vlastnímu zašifrování znaku dojde. A to buď jen částečně, nebo vůbec. Slouží tedy jen k vlastnímu provedení zašifrování a následnému dešifrování. Cílem je vytvořit aplikaci, pomocí které půjde demonstrovat funkcionalitu uvnitř šifrovacího stroje Enigma M4, aby bylo vidět, jakým způsobem se k zašifrovanému znaku dojde.

2. Základní pojmy

Vysvětlení základních pojmů, které se v šifrovacím stroji Enigma M4 vyskytují.

2.1. Propojovací deska

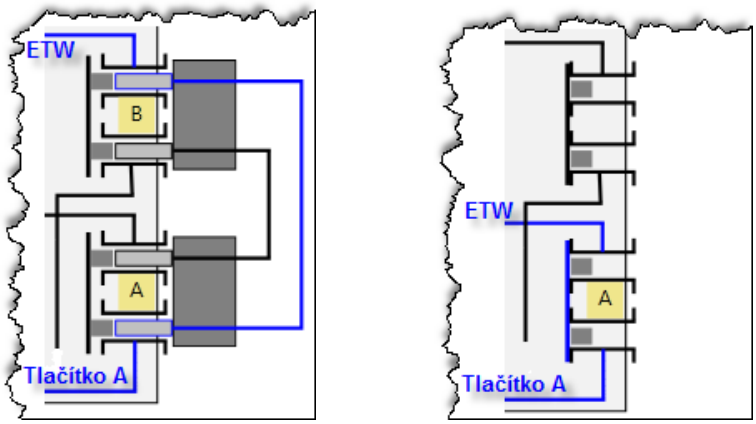
Je umístěna na čelní straně stroje (obr. 1.). Obsahuje 26 konektorů. Každý konektor odpovídá jednomu písmenu A až Z. Jedna zdířka konektoru vede ke stejnému písmenu na tlačítku, druhá zdířka konektoru vede ke stejnému písmenu na vstupním kruhu rotorů tzv. statoru (ETW Entrittswalze).

Obrázek 1. Propojovací deska [1]

Konektory na propojovací desce se propojují pomocí propojovacích kabelů (obr. 2.). Zasunutím propojovacího kabelu se elektrický signál přesměruje na jiné písmeno (obr. 3.,vlevo). Na propojovací desce dochází k první záměně stisknutého znaku za jiný. K záměně znaků na propojovací desce dochází i při návratu elektrického signálu zpět směrem od rotorů.

Obrázek 2. Propojovací kabel [1]

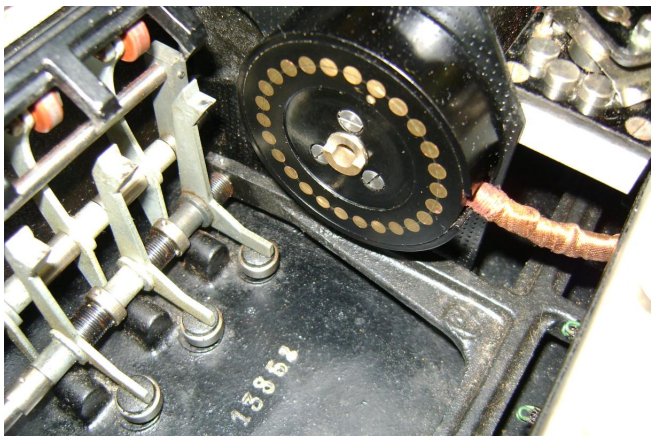
Pokud není propojovací kabel v konektoru zasunutý, signál přes konektor postupuje ze stejného písmene dál (obr. 3. vpravo). Tím že se propojovacím kabelem spojují mezi sebou vždy dvě písmena, lze na propojovací desce najednou zapojit až 13 propojovacích kabelů. V praxi se jich používalo 10.



Obrázek 3. Průběh signálu přes propojovací kabel (vlevo) a bez něj (vpravo)

2.2. Vstupní kruh rotorů (ETW – Entrittswalze)

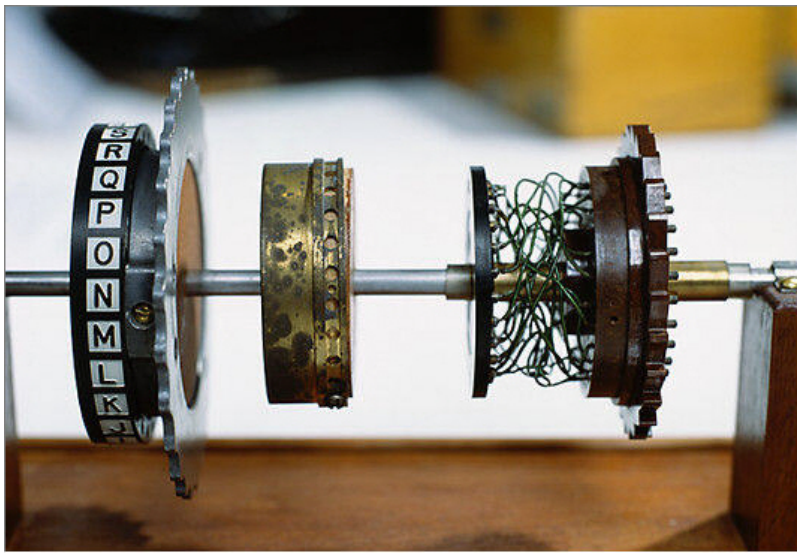
Statický kruhový válec (stator), je umístěný na pravé straně rotorové části (obr. 4.). Stator přenáší signál z propojovací desky na rotory a naopak. Na levé straně má 26 kontaktů. Kontakty statoru se na levé straně dotýkají s kontakty pravého rotoru. Jednotlivé kontakty odpovídají písmenům A až Z. Na druhé straně jsou jednotlivé kontakty statoru spojeny s jednotlivými kontakty na propojovací desce.



Obrázek 4. Pohled na vstupní kruh rotorů [2]

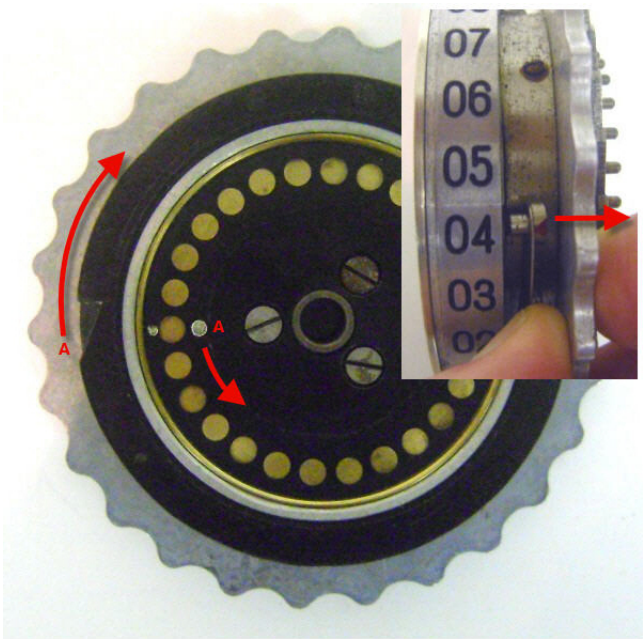
2.3. Rotory

Rotory v šifrovacím stroji slouží k přesměrování elektrického signálu z jednoho písmena na jiné, v závislosti na vnitřním propojení rotoru (obr. 5.). Každý rotor je „válec“, který má po stranách 26 kontaktů. Každý kontakt odpovídá jednomu z písmen A až Z. Uvnitř rotoru je každý kontakt na pravé straně propojen s kontaktem na levé straně. Propojení kontaktů jednotlivých rotorů je uvedeno v tabulce 1. Je-li například u rotoru číslo I. přiveden signál na pravé straně na kontakt A, na levé straně rotoru signál pokračuje z kontaktu E. Tím se změní vstupní písmeno na písmeno jiné.



Obrázek 5. Vnitřní struktura rotoru [1]

Po obvodu rotoru jsou vyznačena písmena A až Z. Prstenec s kontakty (tzv. Ringstellung) se dá vůči písmenům po obvodu otáčet. Jestliže máme kontakt A na prstenci u písmene A na obvodu (obr. 6.), a otočíme prstencem o jednu pozici dopředu, písmeno A na prstenci bude odpovídat písmenu B na obvodu rotoru.



Obrázek 6. Nastavení prstence rotoru [1]

Každý rotor má na sobě jeden nebo dva zářezy (obr. 7.). Pokud jsou rotory v šifrovacím stroji natočeny tak, že západka zapadne do zářezu, dojde k otočení rotoru po jeho levé straně. Toto otáčení platí jen pro druhý a třetí rotor zleva. Pravý rotor se otáčí při každém stisku klávesy.

Obrázek 7. Zářezy na rotoru [1]

Pro typ M4 byla sada osmi rotorů, z nichž do přístroje šli vložit jen tři a sada dvou úzkých rotorů, z nichž do přístroje šel vložit jen jeden. Každý rotor má jiné vnitřní propojení a zářezy pro otáčení (tab. 1.).

Rotor	ABCDEFGHIJKLMNOPQRSTUVWXYZ	**Zářez u písmene**
I	EKMFLGDQVZNTOWYHXUSPAIBRCJ	Y
II	AJDKSIRUXBLHWTMCQGZNPYFVOE	M
III	BDFHJLCPRTXVZNYEIWGAKMUSQO	D
IV	ESOVPZJAYQUIRHXLNFTGKDCMWB	R
V	VZBRGITYUPSDNHLXAWMJQOFECK	H
VI	JPGVOUMFYQBENHZRDKASXLICTW	HU
VII	NZJHGRCXMYSWBOUFAIVLPEKQDT	HU
VIII	FKQHTLXOCBJSPDZRAMEWNIUYGV	HU

Tabulka 1. Propojení kontaktů rotorů [2]

2.4. Úzký rotor

Úzký rotor je nazýván první rotor zleva v rotorové části. Od ostatních rotorů se liší tím, že se neotáčí a je užší než rotory na ostatních pozicích. Není tedy možné jej s rotory na ostatních pozicích zaměňovat. Je to způsobeno tím, že se tento čtvrtý rotor vměstnal do přístroje typu M3, který byl koncipován pouze na tři rotory. Tím úzký rotor nemá otáčecí mechanismus, a aby se tam vlezl, musela se zúžit šířka reflektoru zhruba na polovinu. Pro typ M4, byly v sadě dva úzké rotory označené řeckými písmeny Beta a Gama . Z toho důvodu byly také nazývány jako řecké rotory.
Každý z nich má své vnitřní propojení kontaktů (tab. 2.).

Rotor	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Beta	LEYJVCNIXWPBQMDRTAKZGFUHOS
Gama	FSOKANUERHMBTIYCWLQPZXVGJD

Tabulka 2. Propojení kontaktů úzkých rotorů [2]

2.5. Reflektor (UKW – Umkehrwalze)

Reflektor je statický kruhový válec, umístěný v rotorové části úplně vlevo (obr. 8.). Jeho úkolem je vrátit příchozí signál z úzkého rotoru zpátky na něj. Tím se signál vrací zpět na rotory, propojovací desku a přes tlačítka až k žárovce. Reflektor jde v přístroji vyměnit. Konkrétně u typu M4 byly reflektory s označením UKW-B a UKW-C. Signál se vrací přes kontakty reflektoru, které má na své pravé straně. Kontaktů je 26 a odpovídají písmenům A až Z. Každý typ reflektoru má jiné vnitřní propojení (tab. 3.).

Reflektor	ABCDEFGHIJKLMNOPQRSTUVWXYZ
UKW-B	ENKQAUYWJICOPBLMDXZVFTHRGS
UKW-C	RDOBJNTKVEHMLFCWZAXGYIPSUQ

Tabulka 3. Propojení kontaktů reflektorů [2]

Obrázek 8. Reflektor na levé straně [8]

2.6. Tlačítková část

Obdobně jako na psacím stroji obsahuje 26 tlačítek označených písmeny A až Z (obr. 9.). Číslice byly psány celými slovy (eins, zwei, drei, ...). Stisknutím tlačítka se nejprve provede mechanická část a potom teprve elektrická část.

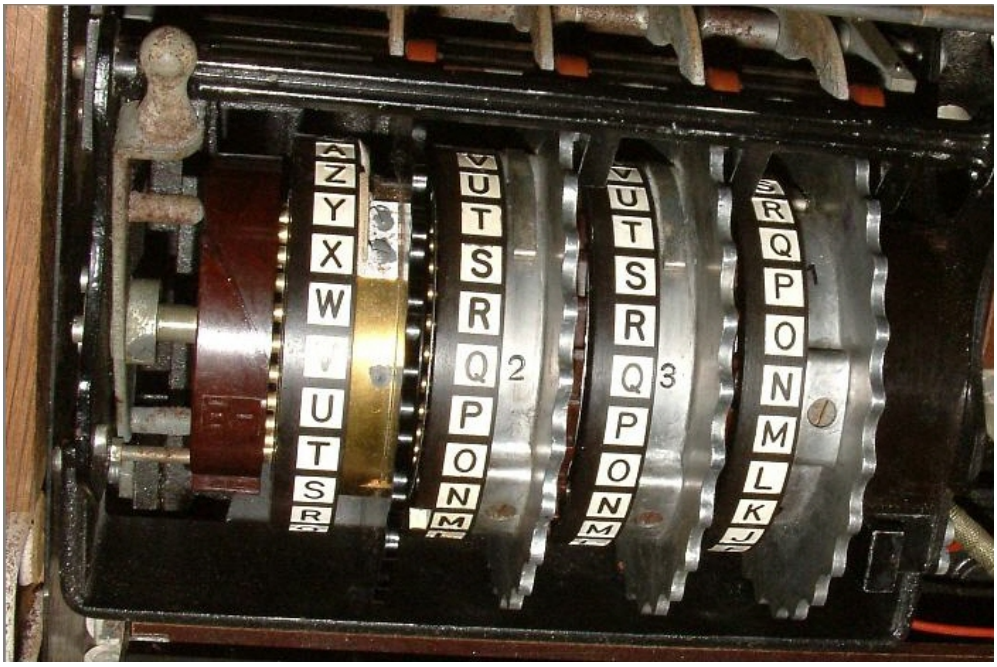
Obrázek 9. Pohled na horní část stroje [1]

2.7. Žárovková část

Rozsvícením žárovky zobrazí výsledný zašifrovaný znak. Obsahuje 26 žárovek. Každá žárovka odpovídá jednomu písmenu A až Z. Žárovky a celý elektrický obvod je napájen buď interní 4V baterií, nebo z externího zdroje.

2.8. Rotorová část

Je složena z otáčecího mechanismu rotorů, vstupního kruhu rotorů, tří širokých rotorů, jednoho úzkého rotoru a reflektoru (obr. 10.).



Obrázek 10. Rotorová část [2]

2.9. Mechanická část

Provádí otáčení rotorů. Rotor na pravé straně se otočí při každém stisku klávesy. Druhý a třetí rotor zleva se otočí, pouze pokud západka zapadne do zářezu v rotoru po jeho pravé straně. Rotory I-V mají na sobě jeden zářez, rotory VI-VIII mají dva zářezy.

2.10. Elektrická část

Tvoří elektrický obvod vedoucí od stisknutého tlačítka, přes propojovací desku, jednotlivé rotory až na reflektor, který signál stejnou cestou vrací zpět až na panel se žárovkami. K záměně (šifrování) stisknutého písmene dochází na propojovací desce, jednotlivých rotorech a to cestou tam i zpátky.

3. Aplikace Simulátor Enigma M4

Úkolem je sestavit softwarovou aplikaci demonstrující činnost šifrovacího stroje Enigma M4. Zaměření aplikace je na probíhající průběh šifrování a ne pouze na výsledek šifrování.

3.1. Cíle aplikace

Vytvořit aplikaci, pomocí které půjde jasně a přehledně demonstrovat:

- z jakých částí se stroj skládá
- znázornění chování stroje během stisknutí tlačítka k zašifrování
- jak se stisknuté písmeno v průběhu šifrování mění
- možnost všech nastavení jaké šly provést na reálném šifrovacím stroji
- uložení a načtení nastavení stroje

Cílovou skupinou uživatelů jsou lektoři, kteří mohou pomocí této aplikace rychle a jednoduše demonstrovat princip činnosti šifrovacího stroje. Další skupinou mohou být studenti nebo obyčejní uživatelé, které princip činnosti šifrovacího stroje Enigma M4 zajímá.

3.2. Použité technologie

Aplikace je vytvořena pomocí grafického subsystému Microsoft Windows Presentation Foundation (WPF) na počítačové platformě Microsoft .NET Framework 4 Client Profile. Naprogramována je v programovacím jazyku Visual C# .NET. Aplikace je určena pro chod na operačních systémech Microsoft Windows. Minimálně Windows XP SP3 s nainstalovaným Microsoft .NET Framework 4. Optimalizována je pro operační systém Windows 7.
Využití grafického subsystému WPF je zvoleno záměrně, vzhledem k nutnosti použít v aplikaci velký počet grafických prvků. Velkou výhodou použití této technologie je možnost využití vektorové grafiky u zobrazení jednotlivých částí šifrovacího stroje. Tím se všechny grafické části dokáží vhodně přizpůsobit a aplikace je použitelná při libovolném rozlišení vyšším jak 1024x768 pixelů.

3.3. Instalátor aplikace

Instalátor aplikace je vytvořen pomocí nástroje na vytváření instalací InstallShield. Projekt je vytvořen jako Basic MSI project.
Instalované položky pomocí instalátoru:

- Microsoft .NET Framework 4 Client Profile – instaluje se pouze v případě že na cílovém počítači ještě není nainstalován
- Složka "Enigma M4" – standardně přednastavená do složky "Program Files"
- Soubor s aplikací "EnigmaM4.exe"
- Konfigurační soubor "enigmaM4.config"
- Zástupce ke spuštění aplikace na ploše
- Složka "Enigma M4" v nabídce start
- Zástupce ke spuštění v nabídce Start složce "Enigma M4"
- Zástupce pro odinstalování aplikace

3.4. Testování aplikace

Aplikace je otestována na operačních systémech Windows 7 Professional a Windows XP SP3 Professional s nainstalovaným Microsoft .NET Framework 4 Client Profile. Kromě základní funkcionality ukládání/načítání nastavení, aktualizace obrazovek během zápisu znaku a prověření vlastního šifrovacího algoritmu, bylo hlavně testováno, aby se na různých operačních systémech správně vykreslovaly signálové čáry. Jejich pozice musí správně odpovídat pozici písmene, kterým má procházet. To bylo problematické hlavně v části Detailu rotorů.

3.5. Ukládání nastavení stroje

Aplikace si do externího konfiguračního souboru ukládá nastavení stroje. Data v něm se aktualizují při každém uložení nastavení. Název konfiguračního souboru je „enigmaM4.config“. Soubor je uložen ve stejné složce jako spustitelný soubor aplikace. Pokud soubor neexistuje nebo obsahuje neplatné údaje, vytvoří se nový se základním nastavením stroje. Aplikace při spuštění načte konfigurační soubor a nastaví podle něj stav stroje.
Konfigurační soubor ukládá data ve formátu XML. Kořenový element má název „MachineSettings“.

Na první úrovni jsou elementy představující jednotlivé části nastavení:

- RotorPlace – umístění rotorů
- RotorRing – nastavení prstenců
- MachineWindow – natočení rotorů
- PlugBoard – propojovací deska

Na druhé úrovni jsou elementy s hodnotami nastavení:
RotorPlace

- reflector – hodnota 0 až 1
- rotor4 – hodnota 0 až 1
- rotor3 – hodnota 0 až 7
- rotor2 – hodnota 0 až 7
- rotor1 – hodnota 0 až 7

RotorRing

- rotor4 – hodnota 0 až 25
- rotor3 – hodnota 0 až 25
- rotor2 – hodnota 0 až 25
- rotor1 – hodnota 0 až 25

MachineWindow

- rotor4 – hodnota 0 až 25
- rotor3 – hodnota 0 až 25
- rotor2 – hodnota 0 až 25
- rotor1 – hodnota 0 až 25

PlugBoard

- A – hodnota A až Z
- ...
- Z – hodnota A až Z

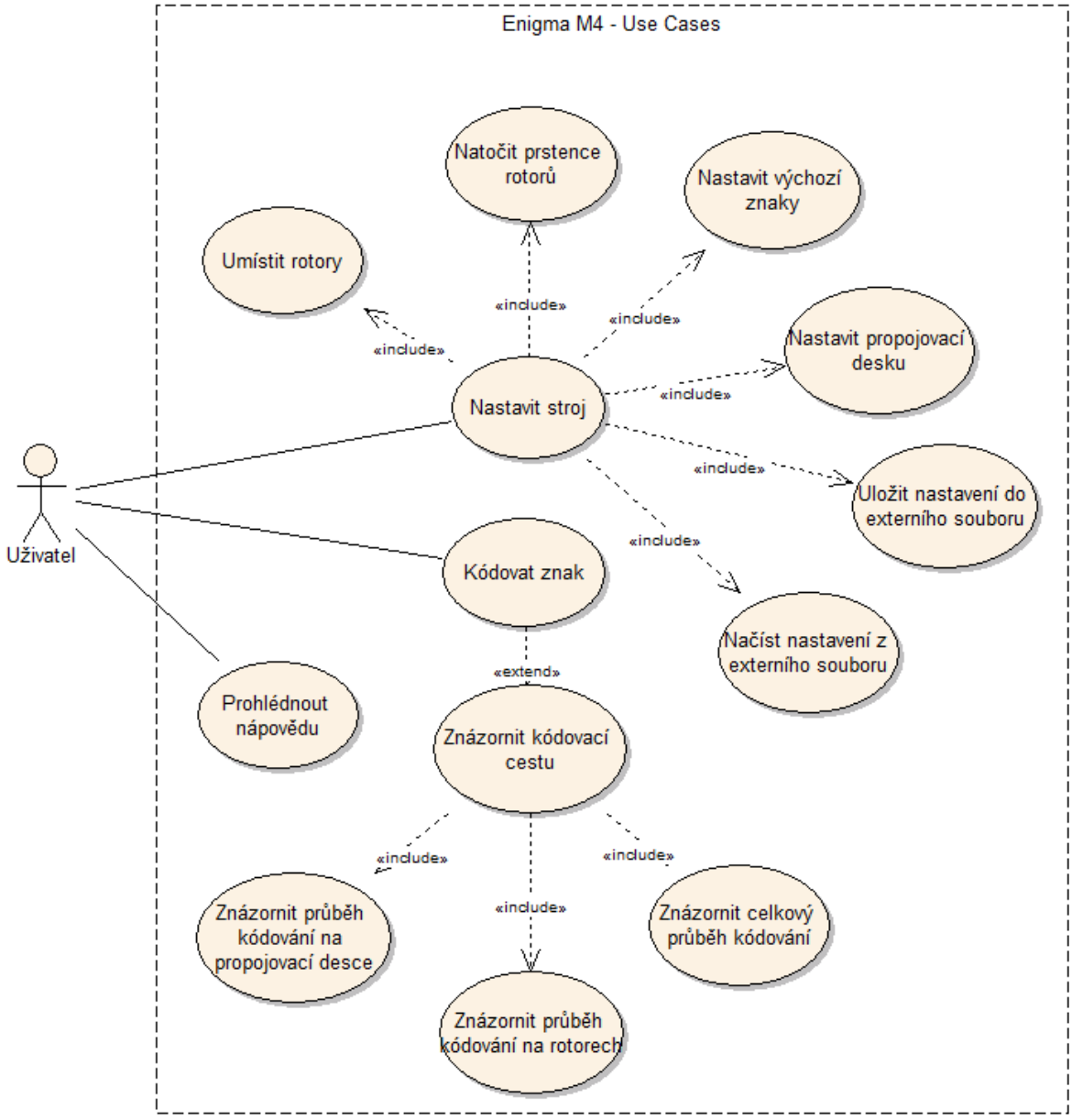
Kompletní vzhled konfiguračního souboru je uveden v příloze B.
Nastavení stroje si lze uložit do vlastního externího souboru. Tyto soubory mají stejnou strukturu jako konfigurační soubor. Příponu mají "*.ecf" (Enigma Configuration File).
XML struktura je zvolena kvůli možnosti rozčlenění na jednotlivé části, obdobně jak je tomu v okně nastavení stroje. Vzhledem k malému množství a jednoduché struktuře dat, není nutné použít ukládání dat do databáze.

3.6. Standardy

Při vytváření WPF aplikací se pro oddělení grafické vrstvy od aplikační nejčastěji používá návrhový vzor MVVM (Model-View-ViewModel, podrobnosti [9]). V aplikaci simulátoru je použit v okně Nastavení stroje a pro zobrazení vstupního a výstupního signálu v okně Propojovací deska. U ostatních oken je použití návrhového vzoru MVVM nevhodné. Pracuje se v nich s velkým množstvím grafických objektů, u kterých se nastavuje jejich pozice, viditelnost a barevnost. Pro všechny tyto atributy každého grafického objektu by bylo nutné vytvořit vlastní třídu a odpovídající atribut, který by ovládal jeho hodnotu. Což by např. v okně Detail rotorů bylo více než 115 atributů třídy. To by popíralo hlavní výhodu návrhového vzoru MVVM, který má činit kód menší a přehlednější. Na těchto ostatních místech je využito standardního rozdělení logické vrstvy a grafického rozhraní pomocí tříd tvořících jádro aplikace a tříd obsluhujících grafické rozhraní. Třídy jádra aplikace jsou od grafického rozhraní zcela nezávislé.

3.7. Případy užití (USE-Case)

Podle vymezených cílů aplikace vznikly tyto případy užití (obr. 11.).



Obrázek 11. Případy užití

1. **Nastavit stroj**
   Uživatel nastaví vlastnosti stroje na počátku šifrování. Nastavení potvrdí stisknutím tlačítka pro uložení.

2. **Umístit rotory**
   Uživatel nastaví, jaká jsou ve stroji na jednotlivých pozicích použita čísla rotorů a reflektorů. V tabulce 4. jsou uvedeny možné hodnoty pro jednotlivé pozice. Hodnoty na pozicích Rotor 1 až Rotor 3 se nesmí opakovat.

Pozice rotoru (počítáno zprava)	**Hodnoty pro výběr**
Rotor 1	I - VIII
Rotor 2	I - VIII
Rotor 3	I - VIII
Rotor 4 (úzký rotor)	Beta, Gama
Reflektor	UKW-B, UKW-C

Tabulka 4. Možné hodnoty nastavení rotorů

3. **Natočit prstence rotorů**
   Uživatel nastaví, jak mají jednotlivé rotory ve stroji nastaveny prstence kontaktů. Pro všechny čtyři rotory se nastavuje hodnota v rozmezí A - Z.

4. **Nastavit výchozí znaky**
   Uživatel pro všechny čtyři rotory nastaví, jaké znaky mají být vidět v horní části přístroje. Pro jednotlivé rotory se nastavuje hodnota v rozmezí A - Z.

5. **Nastavit propojovací desku**
   Uživatel nastaví propojení kabelů na propojovací desce. Propojovací deska obsahuje písmena A - Z. Propojuje se vždy dvojice písmen. Každé písmeno se dá propojit s jiným písmenem pouze jednou. Může tak vzniknout maximálně 13 propojení.

6. **Kódovat znak**
   Uživatel do vstupního pole zadá znak v rozmezí A - Z. Zadaný znak odpovídá znaku stisknutému na klávesnici šifrovacího stroje. Ve vstupním poli se nově zadaný znak zobrazí vždy na poslední pozici. Ve výstupním poli se zobrazí výsledný zašifrovaný znak. Uživatel má k dispozici několik pohledů na průchod šifrovaného signálu strojem.

7. **Znázornit průběh kódování na propojovací desce**
   Uživateli je zobrazen schématický pohled na propojovací desku. Na ní je vidět vzájemné propojení písmen na vstupu propojovací desky a na jejím výstupu. Jakmile uživatel zadá písmeno do vstupního pole, je modře zobrazen signál vstupující na propojovací desku od tlačítek směřující na rotory. Červeně je zobrazen signál přicházející od rotorů na žárovky. Signál zobrazuje celou cestu průchodu propojovací deskou tam i zpátky.

8. **Znázornit průběh kódování rotorové části**
   Uživateli je zobrazen pohled na celou rotorovou část (reflektor a čtyři rotory). Na každém rotoru je znázorněna pozice kontaktů, písmeno zobrazené v horní části stroje, zářezy na rotoru a pozice kde dojde k posunu vedlejšího rotoru. Po zadání znaku do vstupního pole je uživateli zobrazen signál, jak prochází jednotlivými kontakty rotorů. Modře je znázorněn signál vedoucí od propojovací desky až po reflektor. Červeně je znázorněn signál vedoucí od reflektoru přes jednotlivé kontakty rotoru na propojovací desku.

9. **Znázornit celkový průběh kódování**
   Uživateli je zobrazen schématický pohled na jednotlivé části celého stroje:

   - tlačítková část
   - propojovací deska
   - rotorová část
   - žárovková část
   - napájecí část

   Po zadání znaku do vstupního pole je uživateli zobrazen průchod elektrického signálu jednotlivými částmi stroje. V jednotlivých částech je zobrazeno, jak se zadaný znak mění až do výsledného zašifrovaného znaku.

10. **Uložit nastavení do externího souboru**
    Uživatel si může uložit aktuální nastavení stroje do externího souboru. Soubor má příponu ECF (Enigma Configuration File).

11. **Načíst nastavení z externího souboru**
    Uživatel si může načíst nastavení stroje, které si předtím uložil. Jedná se o soubory s příponou ECF. Při načítání se provede kontrola na korektnost načtených dat. V případě poškození nebo neplatných dat, se stroj nastaví do výchozího nastavení.

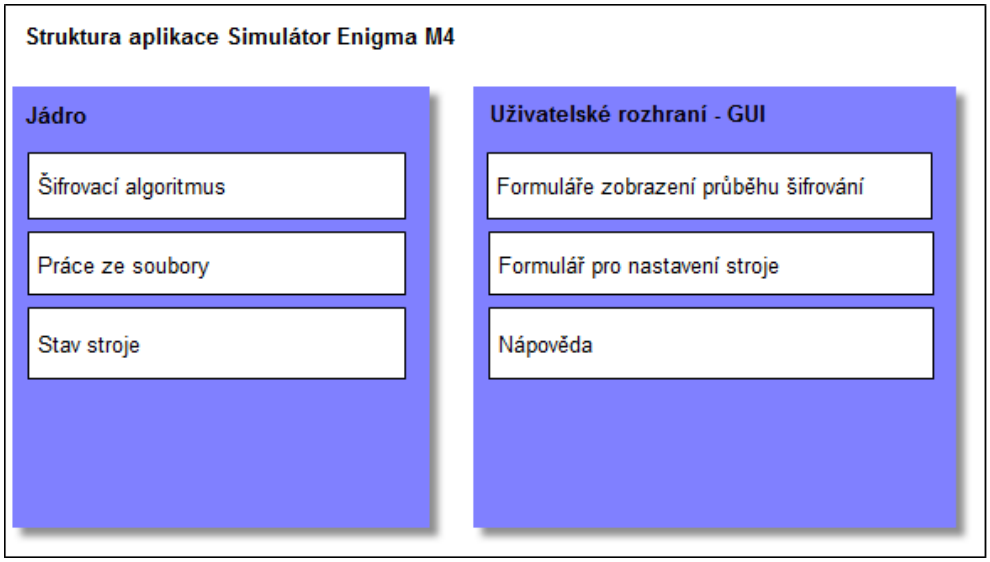
12. **Prohlédnout nápovědu**
    Uživateli se zobrazí obsah nápovědy. Ten je rozdělen na dvě části. První je nápověda k ovládání programu. Druhá část je popis vlastního šifrovacího stroje.

3.8. Struktura aplikace

Základní struktura aplikace rozděluje aplikaci na dvě vrstvy (obr. 12.).

1. **Jádro**
   Logická vrstva oddělená od vrstvy aplikační. Patří do ní šifrovací algoritmus, práce pro uložení, načtení a zpracování nastavení stroje a uchovávání aktuálního stavu stroje, včetně uchovávání historie šifrování.

2. **Uživatelské rozhraní (GUI)**
   Aplikační vrstva zobrazující výstupy a vstupy uživatele.



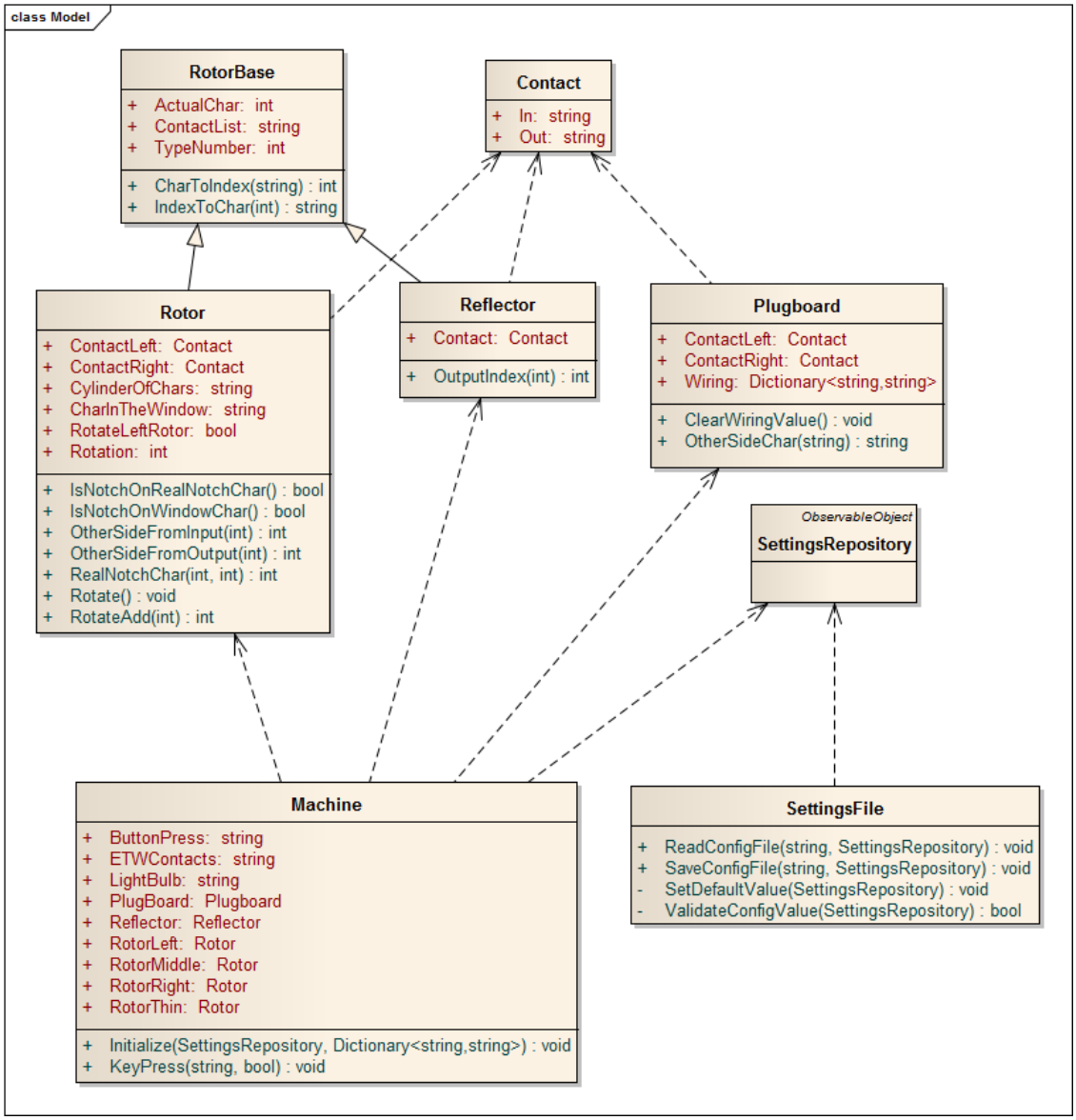
Obrázek 12. Struktura aplikace

3.9. Struktura tříd

Vychází ze základní struktury aplikace.

Základní rozdělení tříd:

- šifrování znaku
- práce s externími soubory
- práce s GUI



Obrázek 13. Struktura tříd jádra

1. **Šifrování znaku**
   Hlavní třídou šifrování znaku je třída „Machine“. Tato třída představuje šifrovací stroj a logiku kódování písmene. Atributy třídy jsou jednotlivé části stroje a položky potřebné pro zobrazení výsledku. Nastavení stroje se z grafické vrstvy do třídy „Machine“ předává pomocí inicializační metody „Initialize“. Kódování písmene je vyvoláno metodou „KeyPress“. Výsledné hodnoty šifrování jsou pak v jednotlivých atributech.

2. **Práce s externími soubory**
   Práci s externími soubory zajišťuje třída „SettingsFile“. Obsahuje metody pro uložení, načtení a verifikaci hodnot sloužících pro nastavení stroje. Externími soubory se rozumí konfigurační soubor a uživatelsky uložené nastavení stroje.

3. **Práce s GUI**
   Třídy „SettingsRepository“ a „PlugBoardRepository“ tvoří rozhraní mezi grafickou vrstvou a aplikační vrstvou v oknech „Nastavení stroje“ a „Propojovací deska“. Jedná se o podpůrnou část návrhového vzoru MVVM. Atributy třídy „PlugBoardRepository“ nastavují pozice vstupního a výstupního signálu po obou stranách. Atributy třídy „SettingsRepository“ se plní a nastavují hodnoty výběrových polí.

4. **Grafická vrstva**
   Patří do ní třídy zajišťující zobrazení hodnot v jednotlivých formulářových oknech (tab. 5.).

ElectricWiring	formulář pro zobrazení Elektrického propojení
HelpView	formulář zobrazující nápovědu
IoFieldsView	pole pro možnost zadání znaku k šifrování a zobrazení zašifrovaného znaku
PlugBoardsSettingsView	mechanismus nastavování propojovací desky v okně Nastavení stroje
PlugBoardView	formulář pro zobrazení pohledu na Propojovací desku
RotorView	formulář pro zobrazení pohledu na Detail rotorů
SettingsView	formulář pro zobrazení a zpracování Nastavení stroje
StartUpView	úvodní obrazovka

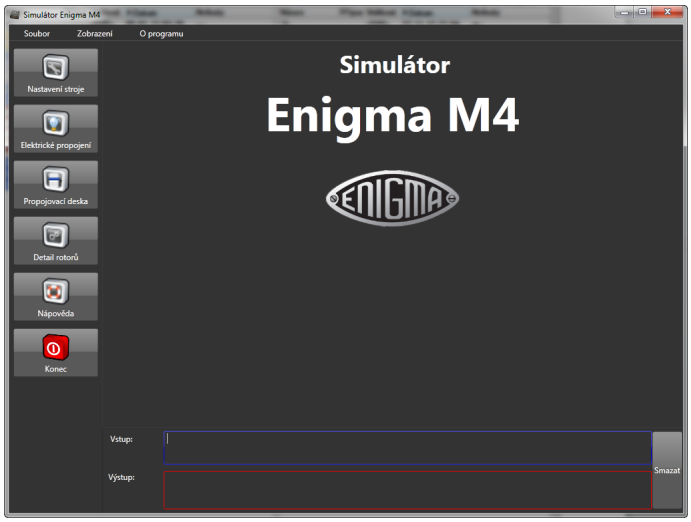
Tabulka 5. Třídy grafické vrstvy

4. Uživatelská část

Popis aplikace pro použití z pohledu uživatele.

4.1. Popis jednotlivých funkcí aplikace

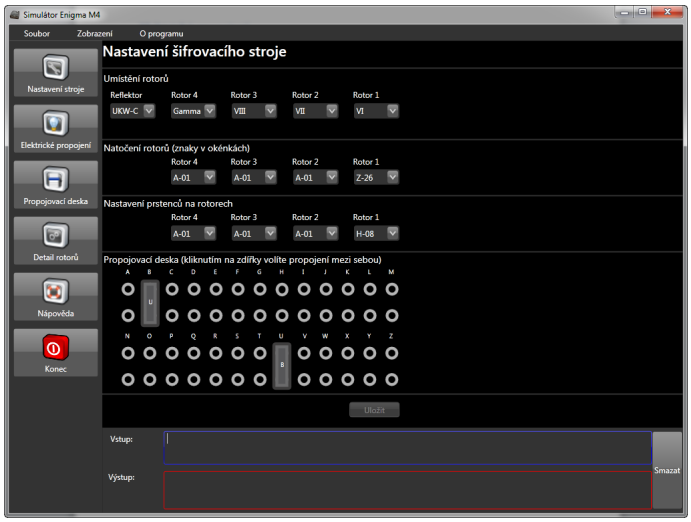
V této části jsou popsány jednotlivé části aplikace a její funkčnost. Veškeré funkce programu se dají vyvolat z menu v hlavním okně. Pomocí velkých tlačítek vlevo na hlavní obrazovce se dají zobrazit hlavní části aplikace.



Obrázek 14. Hlavní obrazovka

4.2. Nastavení stroje

Aktivuje se tlačítkem „Nastavení stroje“ z hlavní obrazovky, nebo výběrem položky „Nastavení stroje“ z menu „Zobrazení“ (obr. 15.).
Slouží k nastavení stavu šifrovacího stroje pro možnost šifrování. Každou změnu v nastavení je nutné potvrdit tlačítkem „Uložit“. Pro opuštění okna s nastavením, stačí kliknout na zobrazení některého z pohledů na stroj. Obsahuje všechny možnosti nastavení, jak to umožňuje reálný šifrovací stroj Enigma M4.
Nastavená konfigurace se dá uložit do externího souboru přes menu „Soubor/Uložit nastavení…“ Uloženou konfiguraci lze načíst přes menu „Soubor/Načíst nastavení…“.
Při spuštění aplikace se automaticky nastaví poslední uložené nastavení.



Obrázek 15. Nastavení stroje

4.3. Umístění rotorů

Určuje seřazení a volbu rotorů v šifrovacím stroji. Na jednotlivé pozice lze umístit hodnoty dle tabulky 4. Pro umístění rotorů na pozicích 1 - 3 se vybírá ze sady osmi rotorů. Každé číslo rotoru je v sadě pouze jednou, nelze tedy stejný rotor umístit na více místech ve stroji. Rotory na čtvrté pozici nejsou zaměnitelné s rotory na ostatních pozicích, protože jsou rozměrově užší. V sadě je na výběr ze dvou rotorů, označených řeckými písmeny Beta a Gama.
Reflektory jsou v sadě dva s označením UKW-B a UKW-C.
Při nastavení reflektoru UKW-B a úzkého rotoru Beta, je šifrovací stroj kompatibilní se šifrovacím strojem Enigma M3. Tím je tedy možné kódovat a dekódovat zprávy i s předchozími verzemi stroje až do Enigma M1.
Umístění rotorů se v aplikaci nastavuje zvolením hodnoty z výběrového seznamu na příslušné pozici.

4.4. Natočení rotorů

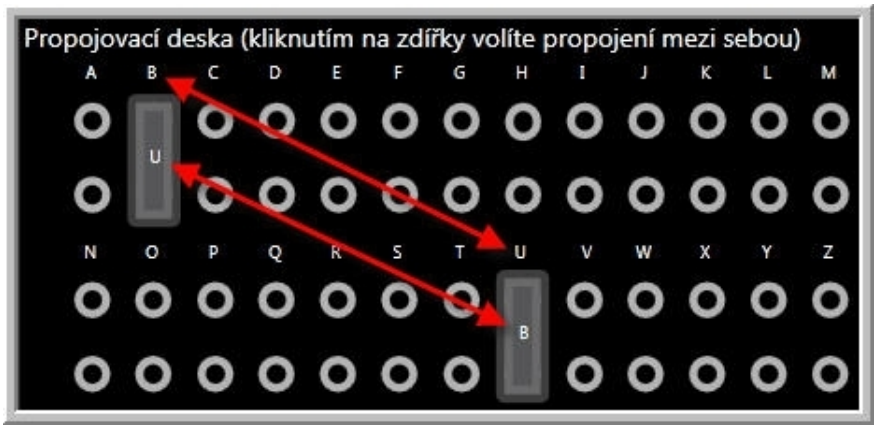
V této části se nastavuje výchozí natočení rotorů na jednotlivých pozicích. Tzn. jaký znak je vidět v horní části stroje. Sady rotorů se vydávaly v provedení s písmeny „A“ až „Z“ po svém obvodu, nebo s čísly 1 až 26. U každého rotoru se dá výběrem ze seznamu zvolit příslušné písmeno. V případě číselného značení číslo 1 odpovídá písmenu „A“ a postupuje abecedně až po písmeno „Z“, které odpovídá číslu 26.

4.5. Nastavení prstenců na rotorech

Nastavení, kterému písmeni po obvodu rotoru odpovídá kontakt „A“ na boku rotoru.
Kontaktů na boku rotoru je 26, stejně jako písmen po obvodu rotoru. Každý kontakt na boku rotoru odpovídá písmenu „A“ až „Z“. Kontakty rotoru, se dají vůči písmenům po obvodu rotoru otáčet. Kontakt písmene „A“ na boku rotoru, pak nemusí odpovídat písmeni „A“ na obvodu rotoru.
Pootočení lze u jednotlivých rotorů nastavit v rozsahu „A“ až „Z“ zvolením hodnoty z výběrového seznamu. Pro nastavení bez pootočení, se nastaví do jednotlivých polí písmeno „A“.

4.6. Propojovací deska

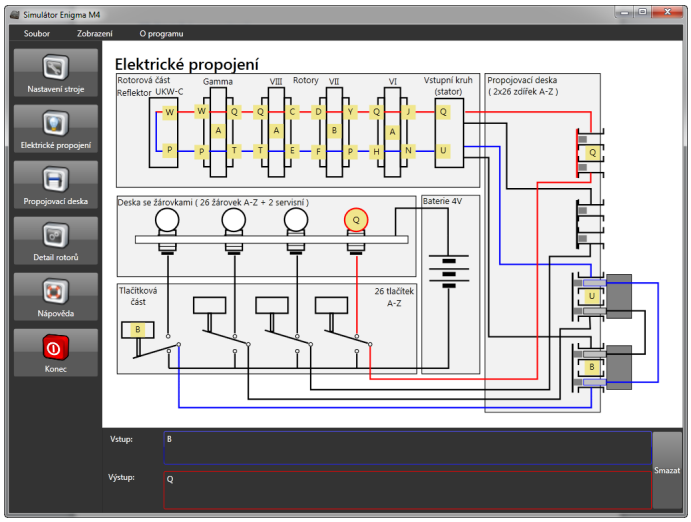
V aplikaci se nastavení propojovací desky provádí kliknutím na zdířku požadovaného písmene. Tím se simultánně provede zasunutí konektoru. Následným kliknutím na zdířku jiného písmene, se provede propojení mezi těmito písmeny. Na konektoru jde vidět s jakým písmenem je daná zdířka propojena. Kliknutím na konektor se propojení z obou písmen zruší.



Obrázek 16. Nastavení propojovací desky

4.7. Elektrické propojení

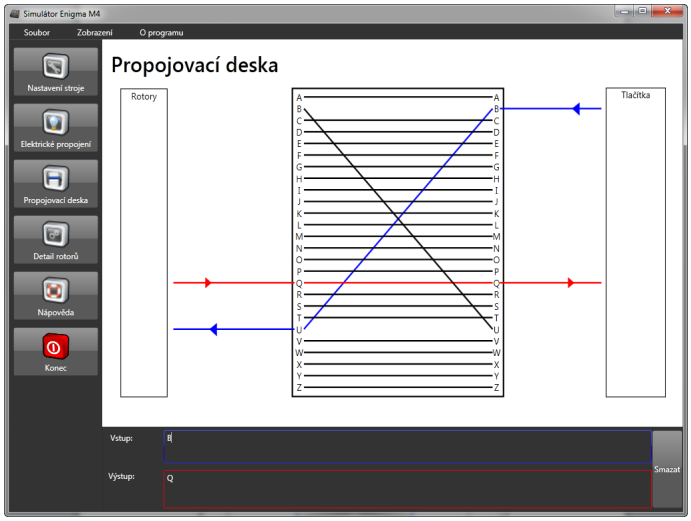
Zobrazuje celkový pohled na jednotlivé části šifrovacího stroje (obr. 17.). Celou cestu signálu od stisknutého tlačítka až po výsledný zašifrovaný znak zobrazený na žárovce. Modrou barvou je označena signálová cesta směrem tam, a červenou barvou signálová cesta ve směru zpátky. Pokud není signálová cesta vidět, stačí zadat do pole vstup libovolný znak „A“ až „Z“ a signálová cesta se zobrazí. Zadáním dalšího znaku v poli Vstup se ihned zobrazí nová cesta signálu pro další znak.



Obrázek 17. Elektrického propojení

4.8. Propojovací deska

Zobrazuje drátové zapojení propojovací desky. Modře je zobrazen vstupní signál vedoucí od tlačítek směrem na rotory. Červeně je zobrazen signál vedoucí od rotorů směrem na tlačítka a žárovky. Pokud signálová cesta není zobrazena, stačí do pole Vstup zadat libovolný znak „A“ až „Z“. Zadáním dalšího znaku v poli Vstup se ihned zobrazí nová cesta signálu pro další znak (obr. 18.).



Obrázek 18. Propojovací deska v simulátoru

4.9. Detail rotorů

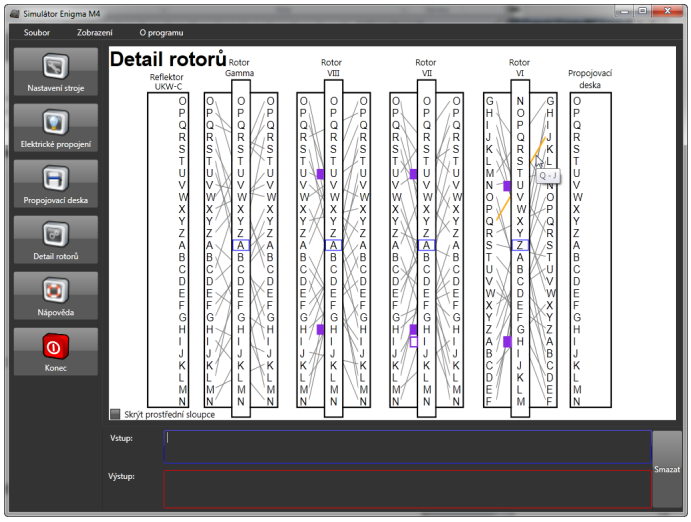
Zobrazuje pohled na jednotlivé rotory. Modré čtverečky uprostřed každého rotoru ukazují znaky, které jsou vidět při pohledu na stroj z venku. Řady znaků po krajích, zobrazují prstence kontaktů na bocích. Kontakty prstenců se dají vůči znakům na obvodu posouvat. Když je prstenec posunut, potom kontakt „A“ na prstenci odpovídá jinému znaku na obvodu. Pokud není posun prstence žádný, kontakty na krajích odpovídají znakům na prostředním sloupci.
Na obrázku 26 je vidět, že prstenec rotoru vpravo je posunut tak, že kontakt „A“ na prstenci, odpovídá znaku „H“ na obvodu rotoru. Tento posun způsobí, že signál přicházející z kontaktu „A“ propojovací desky, vstoupí na kontakt „U“ na prstenci rotoru (obr. 19.).

Obrázek 19. Detail rotorů

Fialový prázdný rámeček na levé straně každého z rotorů ukazuje, kam dopadají západky starající se o otáčení rotorů po stisku klávesy. Plný fialový čtvereček ukazuje zářezy na rotoru. Jakmile se zářez na rotoru dostane do pozice kam dopadají západky, dojde k posunu rotoru po jeho levé straně. To platí pro druhý a třetí rotor. Pravý rotor se otáčí při každém kroku a úzký rotor (první zleva) se neotáčí vůbec.
Modře je zobrazen vstupní signál vedoucí od propojovací desky. Červeně je zobrazen zpětný signál vedoucí od reflektoru směrem na propojovací desku. Pokud signálová cesta není zobrazena, zadejte do pole „Vstup“ nějaký znak „A“ až „Z“. Zadáním dalšího znaku v poli „Vstup“ se ihned zobrazí nová cesta signálu pro zadaný znak.
Zapnutím přepínače „Skrýt prostřední sloupce“ se skryjí prostřední seznamy znaků (obr. 20.). Lépe je tak vidět signálová cesta. Vypnutím přepínače se prostřední seznamy znaků zase zobrazí.

Obrázek 20. Detail rotorů bez prostředních sloupců

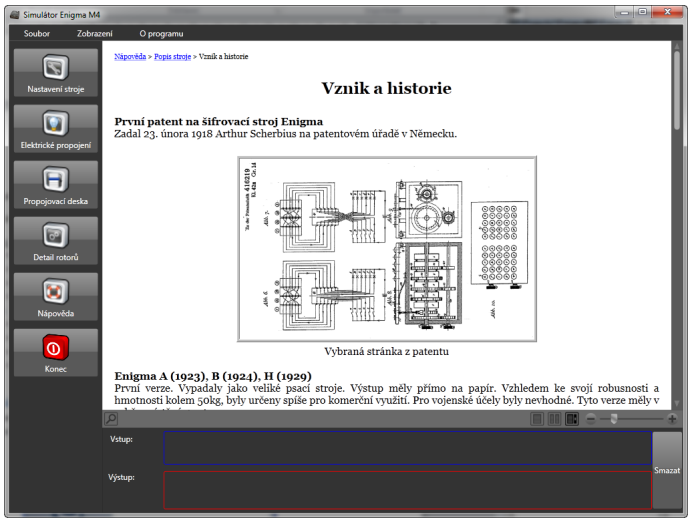
Šedými čarami na pozadí rotorů, je znázorněno vnitřní propojení kontaktů rotorů. Každý kontakt na pravé straně je propojen s kontaktem na levé straně. Najetím myši na šedou čáru se propojení zvýrazní a v tooltiptextu zobrazí znaky propojení (obr. 21.).



Obrázek 21. Zvýraznění propojení při najetí myši

4.10. Nápověda

Nápověda je rozdělena do dvou základních částí. Jedna popisuje šifrovací stroj Enigma M4 a druhá popisuje aplikaci simulátoru (obr. 22.).



Obrázek 22. Zobrazení nápovědy

Mapa nápovědy:
Popis stroje

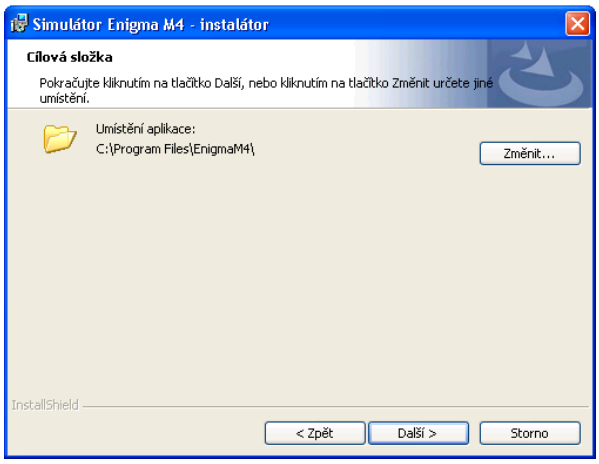
- Vznik a historie
- Složení stroje
- Rotory ve stroji
- Propojovací deska

Popis programu

- Nastavení stroje
- Elektrické propojení
- Propojovací deska
- Detail rotorů

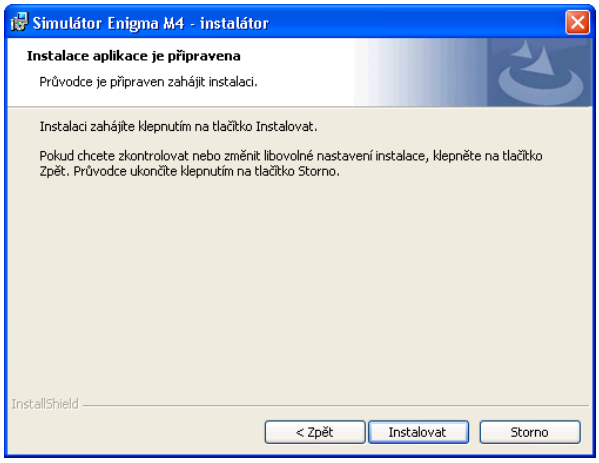
4.11. Postup instalace aplikace

Instalátor aplikace Simulátor EnigmaM4 se spustí souborem „EnigmaM4_setup.exe“. Tento soubor se nachází ve složce „BIN“. Po spuštění instalátoru se zobrazí úvodní obrazovka. Pokračujeme kliknutím na tlačítko „Další“. Zobrazí se obrazovka s výběrem cesty kam se má aplikace nainstalovat (obr. 23.). Kliknutím na tlačítko „Změnit…“ můžeme zvolit jiné umístění kam se má aplikace nainstalovat.



Obrázek 23. Výběr cílové složky pro instalaci

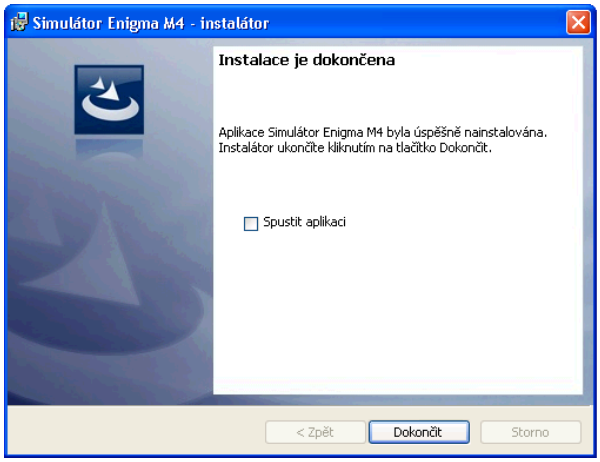
Následně tlačítkem „Další“ přejdeme na okno pro zahájení instalace (obr. 24.).



Obrázek 24. Připraveno k instalaci

Stiskneme tlačítko „Instalovat“. Zobrazí se okno s průběhem instalace a aplikace se nainstaluje do zvoleného umístění. Na plochu se vytvoří zástupce ke spuštění. Do nabídky se Start vytvoří zástupce ke spuštění a k odinstalování.

Jestliže na cílovém počítači není nainstalován Microsoft .NET Framework 4 Client Profile, nainstaluje se nejprve Microsoft .NET Framework 4 Client Profile a potom vlastní aplikace.
Po dokončení instalace si lze zaškrtnutím přepínače „Spustit aplikaci“ zvolit jestli se má aplikace po zavření instalátoru hned spustit. Tlačítkem „Dokončit“ instalátor ukončíme (obr. 25.).



Obrázek 25. Dokončení instalace

4.12. Spuštění aplikace

Aplikace se spouští souborem „EnigmaM4.exe“. Tento soubor se nachází ve složce „EnigmaM4“, v místě kde byla aplikace nainstalována. Dalším způsobem je spuštění přes zástupce „Simulátor Enigma M4“ na ploše, nebo z nabídky „Start“, volbou položky „Všechny programy/Enigma M4/Simulátor Enigma M4“.

4.13. Odinstalování aplikace

Aplikaci Simulátor Enigma M4 lze odinstalovat dvěma způsoby:

- Volbou „Odinstalovat“ z nabídky „Start/Všechny programy/EnigmaM4“
- Z okna „Odebrat nebo změnit program“, do kterého se lze dostat přes nabídku „Start/Ovládací panely/Programy/Programy a funkce“ (platí pro Win7).

4.14. Ověření funkcionality aplikace

Ověření funkcionality lze provést otestováním jednotlivých částí šifrovacího stroje.

Nejdůležitější jsou části, kde probíhá záměna znaku:

- Propojovací deska
- Otáčení rotorů
- Průchod signálu rotory
- Pootočení prstence rotoru
- Reflektor

Pro ověření funkcionality jednotlivých částí nastavíme stroj do základního nastavení (tab. 6.).

	Reflektor	Rotor 4	Rotor 3	Rotor 2	Rotor 1
Umístění rotorů:	UKW-B	Beta	III	II	I
Natočení rotorů:		A	A	A	A
Nastavení prstenců:		A	A	A	A
Propojovací deska:	Bez propojení.				

Tabulka 6. Základní nastavení stroje

4.14.1. Propojovací deska

Ověření funkcionality propojovací desky v jednotlivých zobrazeních, které aplikace umožňuje.

Výchozí nastavení stroje:

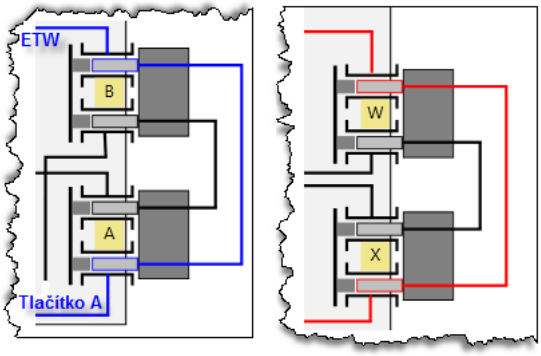
- Nastavíme stroj do základního nastavení (tab. 6.)
- Nastavíme propojovací desku:
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
  BADCFEHGJILKNMPORQTSVUXWZY

Provedení testu:

- Do pole „Vstup“ zadáme znak „A“.
- V jednotlivých zobrazeních aplikace je v částech propojovací desky vidět u vstupního signálu záměnu písmene „A“ na písmeno „B“ a u výstupního signálu záměnu písmene „W“ na písmeno „X“.

Zobrazení elektrického propojení:

- Vstupní signál vede od tlačítka „A“ na zdířku „A“ propojovací desky. Zdířka „A“ je na propojovací desce spojena se zdířkou „B“ (obr. 26. vlevo). Signál z propojovací desky pokračuje od písmene „B“.
- Zpětný signál přichází na zdířku „W“. Ta je podle nastavení propojena se zdířkou „X“, proto signál odchází ze zdířky „X“ (obr. 26. vpravo).



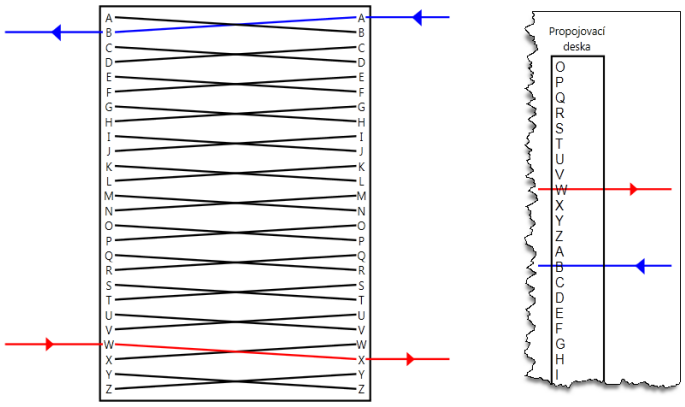
Obrázek 26. Výsledný průběh signálu přes propojovací kabel

Zobrazení propojovací desky:

- Podle výchozího nastavení stroje je vidět, že všechny písmena jsou propojeny do kříže se sousedním písmenem (obr. 27. vlevo).
- Vstupní signál přichází na písmeno „A“ a přes propojení odchází z písmene „B“.
- Výstupní signál přichází z opačné strany na písmeno „W“ a odchází z písmene „X“.

Zobrazení detailu rotorů:

- V tomto pohledu jde vidět, že vstupní signál přichází na rotory z písmene „B“ a výstupní signál z písmene „W“ (obr. 27. vpravo).



Obrázek 27. Výsledný signál testu propojovací desky

4.14.2. Otáčení rotorů

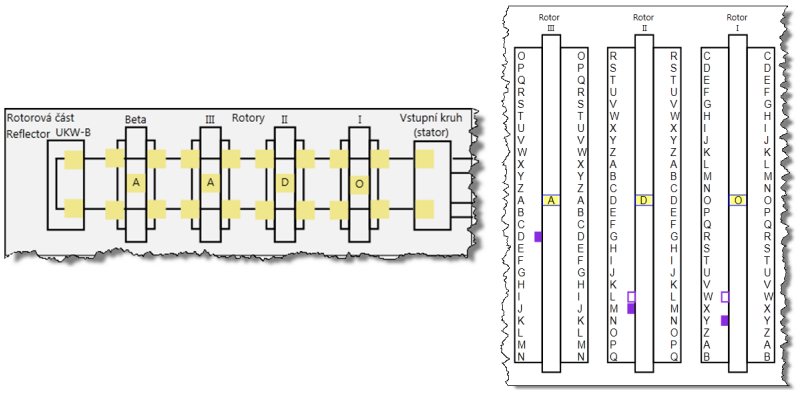
Postup ověření funkcionality otáčení jednotlivých rotorů. Otáčení rotorů se dá v aplikaci kontrolovat na dvou místech. Jedno je při zobrazení elektrického propojení a druhé při zobrazení detailu rotorů. Pro obě zobrazení platí stejný postup ověření.

Zobrazení elektrického propojení:

- Pohyb rotorů je indikován změnou písmen uprostřed jednotlivých rotorů (obr. 28. vlevo).

Zobrazení detailu rotorů:

- Pohyb rotorů je indikován změnou písmen v modrých čtverečcích uprostřed jednotlivých rotorů. Zároveň se posouvají i řady kontaktů na bocích rotorů (obr. 28. vpravo).



Obrázek 28. Znaky představující otáčení rotorů

Výchozí nastavení stroje:

- Nastavíme stroj do základního nastavení (tab. 6.)
- Nastavíme písmena rotorů:

	Rotor 4	**Rotor 3**	**Rotor 2**	**Rotor 1**
Natočení rotorů:	A	A	D	O

Provedení testu:

- Do pole „Vstup“ zapíšeme libovolný znak A-Z.
- Posune se Rotor 1.
  Aktuální stav rotorů:

Rotor 4	**Rotor 3**	**Rotor 2**	**Rotor 1**
A	A	D	**P**

- Do pole „Vstup“ zapíšeme další libovolný znak A-Z.
- Posune se Rotor 1.
- V pohledu detailu rotorů vidíme, že se u Rotoru 1 dostal zářez na rotoru (plný fialový rámeček) na pozici kam dopadají západky posouvající rotory. To znamená, že se v dalším kroku se posune i Rotor 2.
  Aktuální stav rotorů:

Rotor 4	**Rotor 3**	**Rotor 2**	**Rotor 1**
A	A	D	**Q**

- Do pole „Vstup“ zapíšeme libovolný znak A-Z.
- Posune se Rotor 1 a Rotor 2.

- V pohledu detailu rotorů vidíme, že se u Rotoru 2 dostal zářez na rotoru (plný fialový rámeček) na pozici kam dopadají západky posouvající rotory. To znamená, že se v dalším kroku posune i Rotor 3. Zároveň se musí posunout i Rotor 2, protože jinak by do jeho zářezu stále zapadala západka a stále posouvala Rotorem 3. Tomuto dvojímu posunutí se říká „double step“ [3].
  Aktuální stav rotorů:

Rotor 4	**Rotor 3**	**Rotor 2**	**Rotor 1**
A	A	**E**	**R**

- Do pole „Vstup“ zapíšeme libovolný znak A-Z.
- Posune se Rotor 1, Rotor 2 a Rotor 3.
- Tímto krokem se dle výše uvedeného popisu posunuly všechny tři rotory.
  Aktuální stav rotorů:

Rotor 4	**Rotor 3**	**Rotor 2**	**Rotor 1**
A	**B**	**F**	**S**

- V dalším kroku se posune jen Rotor 1, protože všechny zářezy rotorů jsou mimo západky.
- Do pole „Vstup“ zapíšeme libovolný znak A-Z.
- Posune se Rotor 1.
  Aktuální stav rotorů:

Rotor 4	**Rotor 3**	**Rotor 2**	**Rotor 1**
A	B	F	**T**

- Zadáním dalších vstupních znaků se bude posouvat jen Rotor 1 až do doby než znovu dosáhne písmena „Q“. Rotor 4 se při psaní neotáčí. Šifrovací stroj Enigma M4 nemá v sobě implementován mechanismus pro otáčení čtvrtým rotorem.

4.14.3. Průchod signálu rotory

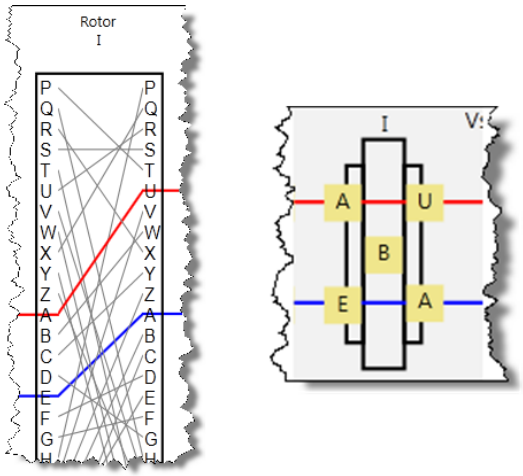
Každý rotor, který jde do přístroje vložit má jiné propojení kontaktů (tab. 1., tab. 2.). Otestování m se prověří, zda je signál u jednotlivých rotorů správně převáděn z pravé strany kontaktů na levou a naopak.

Výchozí nastavení stroje:

- Nastavíme stroj do základního nastavení (tab. 6.).

Provedení testu:

- Do pole „Vstup“ napíšeme písmeno „Z“.
- Zvolíme zobrazení Detail rotorů.
- Vidíme, že signál u prvního rotoru přichází na kontakt „A“ (obr. 29.).
- Na první pozici zprava je umístěn rotor číslo „I“.
- Kontakt „A“ je podle tabulky propojení (tab. 1.) u rotoru číslo „I“ spojen s kontaktem „E“.
- Na pravé straně Rotoru 1 je vstupní signál na kontaktu „A“ a pokračuje na levé straně kontaktem „E“.
- Zpětný signál přichází u Rotoru 1 na písmeno „A“ (obr. 29.).
- Kontakt „A“ na levé straně rotoru číslo „I“ je podle tabulky propojení (tab. 1.) spojen s kontaktem „U“ (Protože se jedná o opačný směr, musíme se v tabulce propojení dívat zdola nahoru).
- Na levé straně Rotoru 1 je výstupní signál na kontaktu „A“ a pokračuje na pravé straně kontaktem „U“.
- To samé vidíme i při zobrazení Elektrického propojení (obr. 29.vpravo).



Obrázek 29. Výsledek testu průchodu signálu rotory

- Postupným zadáváním dalších písmen „Z“ do pole vstup, můžeme výše uvedeným postupem otestovat správnost propojení všech kontaktů A až Z.
- Záměnou rotoru na první pozici lze tak prověřit propojení pro všechny rotory I-VIII.
- U rotorů na ostatních pozicích postupujeme obdobně. Porovnáme, zda kontakt kde signál vstupuje na jedné straně a vystupuje na druhé straně odpovídá propojovací tabulce 1. U vstupního signálu čteme propojovací tabulku shora dolů a u výstupního signálu zdola nahoru. Už se nedá postupovat systematicky od A do Z, ale velkým počtem zadaných znaků, projde signál většinou kontaktů. Takto se dají otestovat i úzké rotory Beta a Gama, které se vkládají na čtvrtou pozici. Propojení úzkých rotorů je uvedeno v tabulce 2.

4.14.4. Pootočení prstence rotoru

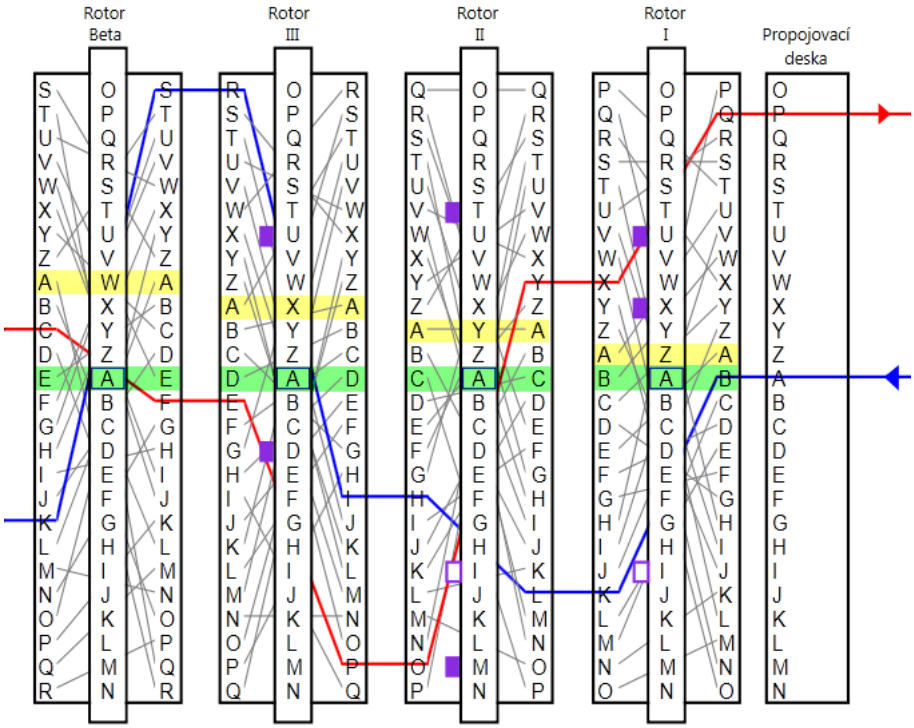
Výchozí nastavení stroje:

	Reflektor	**Rotor 4**	**Rotor 3**	**Rotor 2**	**Rotor 1**
Umístění rotorů:	UKW-B	Beta	III	II	I
Natočení rotorů:		A	A	A	Z
Nastavení prstenců:		W	X	Y	Z
Propojovací deska:	Bez propojení.				

Tabulka 7. Nastavení stroje pro test pootočení prstenců

Provedení testu:

- Zobrazíme Detail rotorů.
- Do pole „Vstup“ zadáme písmeno „A“.
- U každého rotoru vidíme, že písmeno „A“ na bocích rotoru odpovídá písmenu, které bylo zadáno v „Nastavení prstenců“ (obr. 30., označené žlutým pruhem).



Obrázek 30. Pohled na pootočené prstence rotorů

- Z propojovací desky přišel signál z písmene „A“, v okénku prvního rotoru je písmeno „A“, ale kvůli posunutí prstence o jedno písmeno dopředu, se signál dostal na kontakt „B“. Kóduje se tedy jako „B“.
- Stejná situace je i u ostatních rotorů. I když je u všech rotorů z vnějšku vidět písmeno „A“, tak jemu odpovídající kontakt na boku je u rotoru 2 kontakt „C“, rotoru 3 kontakt „D“ a rotoru 4 kontakt „E“ (obr. 30., označené zeleným pruhem).

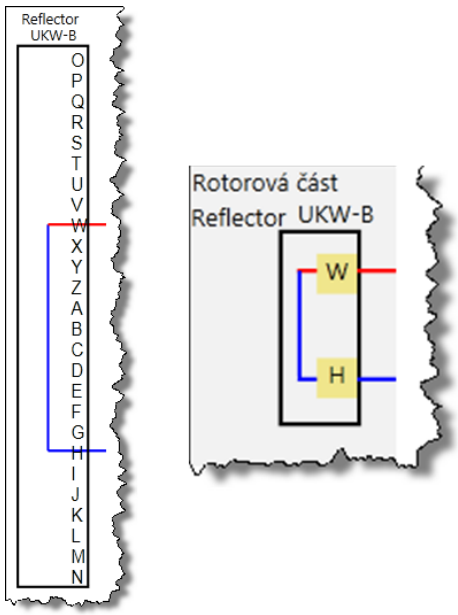
4.14.5. Reflektor

Výchozí nastavení stroje:

- Nastavíme stroj do základního nastavení (tab. 6.)

Provedení testu:

- Zobrazíme Detail rotorů.
- Do pole „Vstup“ zadáme písmeno „Z“.
- Signál vstupuje na kontakt „H“.
- Podle tabulky propojení kontaktů reflektoru UKW-B (tab. 3.) je kontakt „H“ spojen s kontaktem „W“.
- Výstupní signál vychází z kontaktu „W“ (obr. 31.).
- Tento výsledek se dá zároveň zkontrolovat i v zobrazení Elektrického propojení.



Obrázek 31. Výsledný signál testu reflektoru

- Zadáním dalších znaků do pole „Vstup“ můžeme výše uvedeným způsobem vyzkoušet i další kontakty, na které vstupní signál přijde. Vždy v porovnání s tabulkou propojení kontaktů reflektorů. Záměnou reflektoru UKW-B za UKW-C můžeme ověřit správnost zobrazování i u tohoto druhého reflektoru.

Závěr

Práce je orientována na realizaci simulátoru šifrovacího stroje Enigma M4. K tomuto účelu byl nastudován princip funkcionality mechanických i elektrických částí stroje a následně provedena analýza k přípravě aplikace.
Výstupem analýzy je diagram případů užití (USE-Case), návrh modulárního rozdělení a diagram tříd jádra aplikace. Součástí je i grafická podoba, která umožňuje detailní pohled na propojovací desku, celkové elektrické propojení a rotorovou část stroje. Kladen byl důraz na přehledné a jasné zobrazení všech částí, s možností se mezi nimi během šifrování zadaného znaku přepínat. Tato funkcionalita u obdobných programů schází.
K realizaci byla použita technologie Microsoft Windows Presentation Foundation (WPF), na počítačové platformě Microsoft .NET Framework 4. V části nastavení stroje a propojovací desky bylo pro oddělení grafické vrstvy od logické využito návrhového vzoru MVVM. Pro zobrazení jednotlivých částí stroje je využito vektorové grafiky. Tím dokáže všechny grafické části přizpůsobit libovolnému rozlišení vyššímu než 1024x768 pixelů.
Mezi další náměty na vylepšení simulátoru by mohlo být doplnění 3D modelů znázorňujících mechanické otáčení rotorů, případně vytvoření dalších jazykových mutací.

Reference

[1] Reuvers, Paul *Crypto Museum Enigma Cipher Machine* [online], http://www.cryptomuseum.com/.

[2] Rijmenants, Dirk *Technical Details of the Enigma Machine* [online], http://users.telenet.be/d.rijmenants/en/enigmatech.htm.

[3] David H. Hamer *Enigma: Actions involved in the „Double stepping“ of the middle rotor*, Bedminster, NJ 07921-1083, U.S.A.

[4] Deavours A., Kruh Louis. *Machine Cryptography and Modern Cryptoanalysis.*, Norwood MA: Artech House, 1985.

[5] Deavours A., Kruh Louis. *The Commercial Enigma: Beginnings of Machine Cryptography*, 2002.

[6] Copeland, Jack. *Enigma*, University of Canterbury, 2006.

[7] Churchouse, Robert. *Codes and Ciphers*, Cambridge University Press, 2001.

[8] Wikipedia.org, *Enigma-M4* [online], http://de.wikipedia.org/wiki/Enigma-M4

[9] Dajbych, Václav. *MVVM: Model-View-ViewModel*[online], http://dajbych.net/model-view-viewmodel

A. Copyright obrázků z CryptoMuseum.com

Copyright question

Zdeněk Fuchs <zfuchs@centrum.cz> 21. července 2012 14:35
Komu: info@cryptomuseum.com

Hi,
I do bachelor's thesis on Enigma M4.
Could I use some Enigma images from your site in my school work?
I'll write your sites as source.

Thanks for the answer.
Best regards,
Zdenek Fuchs

Paul Reuvers <info@cryptomuseum.com> 21. července 2012 16:33
Komu: Zdeněk Fuchs <zfuchs@centrum.cz>

Dear Zdenek,

You are welcome to use the pictures for your school work, if you give reference to the site as your source.
Good luck with your thesis!

Best regards,

Paul Reuvers
Crypto Museum
The Netherlands
[Citovaný text byl skryt]
Paul Reuvers
Crypto Museum
info@cryptomuseum.com

B. Vzhled konfiguračního souboru

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<MachineSettings>
    <RotorPlace>
        <reflector>0</reflector>
        <rotor4>0</rotor4>
        <rotor3>2</rotor3>
        <rotor2>1</rotor2>
        <rotor1>0</rotor1>
    </RotorPlace>
    <RotorRing>
        <rotor4>0</rotor4>
        <rotor3>0</rotor3>
        <rotor2>0</rotor2>
        <rotor1>0</rotor1>
    </RotorRing>
    <MachineWindow>
        <rotor4>0</rotor4>
        <rotor3>0</rotor3>
        <rotor2>0</rotor2>
        <rotor1>0</rotor1>
    </MachineWindow>
    <PlugBoard>
        <A></A>
        <B></B>
        <C></C>
        <D></D>
        <E></E>
        <F></F>
        <G></G>
        <H></H>
        <I></I>
        <J></J>
        <K></K>
        <L></L>
        <M></M>
        <N></N>
        <O></O>
        <P></P>
        <Q></Q>
        <R></R>
        <S></S>
```

```
        <T></T>
        <U></U>
        <V></V>
        <W></W>
        <X></X>
        <Y></Y>
        <Z></Z>
    </PlugBoard>
</MachineSettings>
```

C. Obsah přiloženého CD

Stručný popis obsahu přiloženého CD.

`bin/`
: **EnigmaM4_setup.exe** – instalátor aplikace Simulátor Enigma M4.
EnigmaM4 – složka s aplikací Simulátor Enigma M4 přímo ve spustitelné podobě. Kvůli zápisům do svého konfiguračního souboru nelze spouštět a používat přímo z CD.

`doc/`
: **bp_zf_enigmaM4.pdf** – dokumentace ve formátu PDF
bp_zf_enigmaM4_tex.zip – dokumentace formátu TEX, včetně příloh

`src/`
: **EnigmaM4_src.zip** – kompletní zdrojové texty

`data/`
: **double_step.ecf** – ukázkové nastavení stroje

`install/`
: **dotNetFx40_Full_x86_x64.exe** – instalace Microsoft .NET Framework 4.0 Client Profile

`readme.txt`
: Instrukce pro instalaci a spuštění aplikace, včetně požadavků pro jeho provoz.