ENIGMA CryptoMate v1.0
(LS 2006 / 2007)

Dokumentácia zápočtového programu

Lukáš Kúdela, MFF UK, 1. ročník, stud. odbor: Informatika, krúžok č. 37

Programovanie PRG031
letný semester 2006 / 2007

(cvičiaci: Doc. RNDr. Pavel Töpfer, CSc.)

Užívateľská časť

Stručná charakteristika šifrovacieho prístroja ENIGMA

Prístroj ENIGMA bol šifrovací prístroj používaný na šifrovanie resp. dešifrovanie tajných správ. Presnejšie povedané, meno ENIGMA referuje na celú rodinu navzájom súvisiacich *elektro-mechanických rotorových šifrovacích prístrojov*, pozostávajúcu zo širokého spektra rozličných modelov, využívajúcich *komplexnú formu polyalfabetickej substitučnej šifry*. Hoci šifrovacia procedúra ENIGMY má svoje kryptografické nedostatky, v praxi bolo jej prelomenie spojeneckými kryptoanalytikmi možné iba dôsledkom ich kombinácie s externými faktormi ako napr. chyby operátorov, procedurálne nedostatky, občasne ukoristený prístroj alebo kniha kľúčov (angl. *codebook*).

Stručná história a vývoj šifrovacieho prístroja ENIGMA

Existujú početné modely a varianty patriace do širokej rodiny šifrovacích prístrojov ENIGMA. Rané prístroje boli modely používané v komerčnej sfére od 20. rokov 20. storočia. Počiatkom rokov 1925-26 začínajú používať ENIGMU rôzne divízie nemeckej armády, viac či menej modifikovanú s cieľom zvýšiť úroveň jej bezpečnosti. V priebehu nasledujúcich rokov sa niekoľko ostatných štátov inšpirovalo dizajnom ENIGMY pri vývoji svojich vlastných šifrovacích prístrojov.

ENIGMA v komerčnej sfére

Prístroj ENIGMA bol vynájdený *Arthurom Scherbiusom* (spoločnosť Scherbius & Ritter) a patentovaný 23. februára roku 1918. Okamžite bol ponúknutý nemeckému námorníctvu a ministerstvu zahraničných vecí, ale ani jedna inštitúcia neprejavila záujem. Scherbius a Ritter teda pridelili patent *Gewerkschaft Securitas*, ktorí založili *Chiffriermaschinen Aktien-Gesellschaft* (prekl. Šifrovacie prístroje, a.s.) v júli roku 1923. Scherbius a Ritter sa stali členmi správnej rady novolzaloženej spoločnosti.

Chiffriermaschinen AG začala propagovať rotorový prístroj – **ENIGMA model A** – ktorý bol vystavený na Kongrese Medzinárodnej poštovej únie v rokoch 1923 a 1924. Prístroj, zahŕňajúci i vlastný písací stroj, bol ťažký a objemný; meral 65x45x35 cm a vážil okolo 50 kg. Krátko nato bola predstavená jeho ďalšia verzia, **model B**, s podobým dizajnom. Hoci modely A i B niesli obchodné meno ENIGMA, svojou konštrukciou sa od svojich následovníkov značne líšili veľkosťou i tvarom, ale i kryptograficky, kedže ani jeden neobsahoval reflektor.

Reflektor – nápad Scherbiusovho kolegu *Williho Korna* – bol prvýkrát implementovaný v modeli **ENIGMA C** v roku 1926 a okamžite sa stal kľúčovou komponentou v prístrojoch ENIGMA. Model C bol menší a prenosnejší ako jeho predchodcovia; postrádal písací stroj, spoliehajúc sa na operátorovo odčítavanie z rozsvecujúcich sa žiaroviek. Zakrátko nato, v roku 1927, ho však nahradil nový model - **ENIGMA D**. Táto verzia sa stala veľmi populárnou a jej exempláre putovali do Švédska, Holandska, Anglicka, Japonska, Talianska, Španielska, U.S.A. a Poľska.

ENIGMA vo vojenskej sfére

Námorníctvo bolo prvou divíziou nemeckej armády, ktoré si osvojilo ENIGMU. Táto verzia, pomenovaná **Funkschlüssel C** (*Radio Cipher C*), bola uvedená do výroby v roku 1925 a do služby v roku 1926. Klávesnica a panel so žiarovkami obsahovali 29 písmen (A-Z, Ä, Ö a Ü), ktoré boli usporiadané podľa abecedy, na rozdiel od usporiadania QWERTZ. Rotory mali 28 kontaktov, pričom písmeno X bolo prepojené tak, aby prešlo procesom nezašifrované. Tri rotory mohli byť vybrané zo sady piatich a reflektor mohol byť vložený v jednej zo štyroch rozdielnych pozícií, označených α, β, γ a δ. Tento prístroj bol mierne upravený v roku 1933.

15. júla 1928 nemecké pozemné vojsko (*Reichswehr*) predstavilo svoju vlastnú verziu ENIGMY – **ENIGMA G**, upravenú na **ENIGMU I** v júni 1930. ENIGMA I je taktiež známa pod menom **Wehrmacht** a bola používaná nemeckými vojenskými službami a inými vládnymi organizáciami (ako napr. železnice) pred i počas Druhej svetovej vojny. Hlavný rozdiel medzi modelmi ENIGMA I a komerčnou verziou bolo predstavenie tzv. *prepájacieho panelu* na prepojenie párov písmen, čo veľmi zvyšovalo kryptografickú silu prístroja. Ďalšie rozdiely spočívali v používaní fixného reflektora a premiestnení krokovacích zárezov z tela rotora na pohyblivé krúžky z písmenami. Námorníctvo eventuálne nasledovalo a v roku 1934 predstavilo svoju námornú verziu, **Funkschlüssel M** alebo **M3**. Kým pozemné vojsko v tom čase používala iba 3 rotory, námorníctvo, pre vyššiu bezpečnosť, upresnilo výber 3 z 5 možných rotorov.

V decembri 1938 pozemné vojsko predstavilo dva rotory navyše, tak aby tri rotory mohli byť vybrané zo sady piatich. V tom istom roku námorníctvo pridalo ďalšie dva rotory a potom ešte jeden v roku 1939 umožňujúc tak výber troch zo sady ôsmich. V auguste 1935 letectvo taktiež predstavilo Wehrmacht ENIGMU s úmyslom zabezpečiť utajenie svojej komunikácie. Štvor-rotorová ENIGMA, nazvaná **M4**, bola predstavená námorníctvom pre komunikáciu medzi ponorkami U-boat vo Februári 1942. (Táto sieť bola spojencami nazývaná *Triton* alebo *Shark*.) Extra rotor mohol byť vložený vďaka nahradeniu pôvodného (širokého) reflektora kombináciou tenkého reflektora a tenkého štvrtého rotora.

Existoval taktiež veľký, osem-rotorový model s vstavanou tlačiarňou, **ENIGMA II**. Počas roku 1933 poľskí kryptoanalytici zistili, že bol používaný na vysoko-úrovňovú vojenskú komunikáciu, ale že bol čoskoro vyradený z používania z dôvodu nespoľahlivosti a zvýšenej poruchovosti.

Abwehr (nemecká rozviedka) používal model **ENIGMA G** (Abwehr ENIGMA). Tento štvor-rotorový variant postrádal prepájací panel, obsahoval však niekoľko zárezov na obvode rotorov. Navyše bol vybavený počítadlom, ktoré sa zvýšilo po každom stlačení klávesnice, čo ho preslávilo ako **počítadlový prístroj** (nem. **Zählwerk ENIGMA**).

Ostatné krajiny taktiež používali prístroje ENIGMA. Talianska armáda prevzala komerčný model pod menom „Námorná Šifra D“; Španielsko taktiež používalo komerčnú ENIGMU počas občianskej vojny. Britským kryptoanalytikom sa podarilo prelomiť tieto prístroje, keďže postrádali prepájací panel. Švajčiari používali verziu veľmi podobnú komerčnej ENIGME D, ktorá sa volala **model K** alebo **Švajčiarska K** (angl. *Swiss K*) na vojnové či diplomatické účely. Šifra tohto prístroja bola prelomená niekoľkými stranami zahŕňajúc Poľsko, Francúzsko, Britániu a Spojené štáty. Model **ENIGMA T** (s krycím názvom **Tirpitz**) bol vyrobený a používaný v Japonsku.

ENIGMA nebola dokonalá a táto skutočnosť dopomohla spojencom, špeciálne po tom, ako sa jej zmocnili, dekódovať nemecké správy, čo sa neskôr ukázalo ako kľúčový faktor vo *Vojne o Atlantik*. Odborníci odhadujú, že bolo zkonštruovaných až 100,000 prístrojov ENIGMA. Po skončení Druhej svetovej vojny predali spojenci ukoristené prístroje, stále všeobecne pokladané za bezpečné, niekoľkým rozvojovým krajinám.

Substitučné šifry a princíp šifrovacieho prístroja ENIGMA

Šifrovacie systémy

Vo všetkých šifrovacích systémoch odosielateľ správy predpokladá, že správa bola zachytená nepriateľom. Cieľom je teda znemožniť resp. učiniť extrémne časovo náročné rozlúštenie správy. V kryptológií existujú dva diametrálne odlišné myšlienkové prúdy, ako tento cieľ dosiahnúť:

1. **Bezpečnosť cez neznámosť, nezrozumiteľnosť** (angl. *Security through obscurity*)
   Táto kontroverzná kryptologická filozofia vyzdvihuje *utajenie dizajnu či implementácie* šifrovacieho systému na dosiahnutie bezpečnosti. Systém spoliehajúci sa na tento princíp môže mať teoretické i praktické bezpečnostné nedostatky, ale jeho vlastníci či dizajnéri veria, že tieto chyby *nie sú známe* a že je vysoko nepravdepodobné, že nepriateľ systém identifikuje. V prípade, že nepriateľ systém odhalí, stáva sa nepoužiteľným!

2. **Bezpečnosť cez priehľadnosť** (angl. *Security through transparency*)
   Tento prístup v kryptológií predstavuje priamy kontrast predchádzajúcej myšlienke. Dizajnér systému podľa neho predpokladá, že nepriateľ po čase aktívnej kryptoanalýzy odhalí princíp používaného systému. (Toto nutne neznamená, že sa nevyvíja potrebné úsilie na jeho utajenie!) Preto by sa bezpečnosť systému mala spoliehať iba na jeho neveľkú a ľahko vymeniteľnú súčasť, ktorú v kryptológií nazývame *kľúč*. Tento je umožnené a koniec-koncov aj žiadúce meniť tak často, ako je to len prakticky možné. Tento prístup sa v modernej kryptológií teší vyššej popularite ako jeho alternatíva a aj ENIGMA spadá svojou dizajnérskou filozofiou práve do tejto kategórie. Nepriateľovi, ktorý sa zmocnil tohto prístroja zostáva ešte dlhá cesta k prelomeniu jeho šifry.

Každý v praxi používaný šifrovací systém teda musí predpokladať, že napriek úsiliu ho utajiť, ho nepriateľ po čase správne identifikuje. Bezpečnosť správy preto spočíva v znemožnení nepriateľovi zistiť *kľúč*, špecifický detail vypovedajúci o tom, ako presne bol tento systém nakonfigurovaný pred zašifrovaním konkrétnej správy. Je nevyhnutné, aby existoval bezpečný spôsob predania tohto kľúča zamýšľanému adresátovi. Ďalšia nevyhnutná vlastnosť šifrovacieho systému je existencia obrovského počtu rôznych kľúčov, inak povedané rozličných spôsobov, ktorými mohol byt systém nakonfigurovaný pri posielaní konkrétnej správy. Inak by mohol nepriateľ jednoducho vyskúšať všetky tieto kľúče.

Substitučné šifry

Substitučné šifry (ENIGMA je ich sofistikovanou inkarnáciou) zahŕňajú nahrádzanie jedného písmena druhým podľa určitého pravidla. Najjednoduchšia substitúcia je tzv. *Cézarova šifra*, ktorá nahradzuje každé písmeno písmenom vzdialeným o *k* miest doprava v abecede, kde *k* je *kľúč*. Sofistikovanejší systém používa náhodnú permutáciu abecedy, namiesto jej obyčajného posunutia. Obe tieto metódy sú príkladom *monoalfabetickej substitučnej šifry*, keďže sa na šifrovanie celej správy používa iba *jedna* permutácia abecedy.

Šifrovací prístroj ENIGMA

Prístroj bol vynájdený v roku 1918 Arthurom Scherbiusom, ktorého nápadom bolo dosiahnutie efektu substitučnej šifry pomocou elektrických prepojení a tak podstatne skrátiť dobu procesu (de)šifrovania. Prístroj ENIGMA zašifruje správu tak, že na ňu aplikuje niekoľko substitučných šifier za sebou. Povážlivý pokrok oproti triviálnej Cézarovej šifre je posunutie vzájomných prepojení (rotácia rotorov) pri každom stlačení klávesnice, čo spôsobí, že každé písmeno je (de)šifrované *odlišnou* substitúciou, čomu sa v praxi hovorí *polyalfabetická substitučná šifra*.

Jednotlivé substitúcie sú reprezentované valcami (rotormi), nachádzajúcimi sa na spoločnej oske, ktorých podstavy sa navzájom dotýkajú pomocou odpružených kontaktov. Celkovú úroveň zložitosti zdvihol vynálezca Willi Korn pridaním špeciálneho valca – *reflektora*. Namiesto používania výstupu tretieho valca ako zašifrovanie vstupného písmena, je výstup privedený do fixného reflekčného valca, ktorý pozostáva zo vzájomných prepojení párov písmen. Výstup z reflektora je prevedený späť, prechádzajúc všetky rotory v opačnom poradí, na vstupný valec. Takto prístroj vykoná 7 substitúcií za sebou: 3 valce, reflektor a 3 valce v opačnom poradí. Pridanie reflektora však prinieslo aj zjednodušenie systému v určitých aspektoch, konkrétne:

1. Prístroj sa stal *reciprokálnym*, čo znamená, že ak sa pri určitej konfigurácií A zašifruje na Q, potom sa pri tej istej konfigurácií Q zašifruje na A. Táto skutočnosť značne znižuje kryptografickú silu prístroja a je nápomocná nepriateľovi pokúšajúcemu sa prelomiť šifru.

   Reciprokálny šifrovací systém mal jednu výhodu: prístroj sa nemusel prepínať medzi „šifrovacím“ a „dešifrovacím“ režimom, čo značne zjednodušovalo jeho obsluhu. Nemecká armáda však zaplatila vysokú cenu, za túto vymoženosť.

2. Písmeno sa nemohlo zašifrovať samé na seba, čo je veľký kryptografický nedostatok.

Vyčerpávajúcejší popis doprevádzaný ilustráciami poskytujú použité zdroje č. 1, 2.

Zložitosť šifrovacieho prístroja ENIGMA

Ako bolo povedané v úvode, je rozmuné predpokladať, že nepriateľ má k dispozícií repliku šifrovacieho prístroja ENIGMA. Ochrana pred dešifrovaním teda spočíva v obrovskom počte počiatočných stavov (konfigurácií), ktoré treba všetky odskúšať pri procese kryptoanalýzy.

Základná troj-rotorová ENIGMA má 26 x 26 x 26 (keď opomenieme efekt „dvoj-kroku“) = 17,576 možných stavov rotorov pre každé z možných 6 usporiadaní rotorov, celkovo teda: 6 x 17,576 = 105,456. Pre každú z týchto 105,456 možností sa môže prepájací panel nachádzať v jednom z 150,736,274,937,250 stavov. (Výber 10 párov z 26 prvkov – písmen abecedy.) Celkový počet kombinácií je teda, pre najjednoduchší(!) vojenský model ENIGMY v rádoch 15,000,000,000,000,000,000, čo je ešte skomplikované individuálnou konfiguráciou jednotlivých rotorov (nem. *Ringstellung*). Úloha, ktorej čelí nepriateľ pri pokuse o prelomenie šifry je zistiť, ktorá z týchto pätnástich triliónov možností bola použitá!

Cieľ programu ENIGMA CryptoMate

Program ENIGMA CryptoMate si kladie za cieľ simulovať repliku pôvodného šifrovacieho prístroja ENIGMA, konkrétne jeho nasledujúcich inkarnácií/modelov/verzií: *Wehrmacht/Luftwaffe*, *Kriegsmarine M3* a *Kriegsmarine M4*. Užívateľovi je umožnené vybrať si jeden zo spomínaných modelov a plnohodnotne ho používať na šifrovanie resp. dešifrovanie správ pozostávajúcich z 26 veľkých písmen abecedy v interaktívnom režime, emulujúcom skutočné používanie ENIGMY, ako i v režime neinteraktívnom, ktorý lepšie vyhovuje súčasným požiadavkám pre (de)šifrovanie. Simulátor ENIGMA CryptoMate poskytuje všetky možnosti nastavenia ako i operácie prístroja dostupné na reálnych

historických prístrojoch ENIGMA (v spomínaných verziách) a jeho najvyšším cieľom je spoľahlivo poslúžiť pri dešifrovaní skutočných zachovaných tajných správ z obdobia Druhej svetovej vojny.

Užívateľská interakcia

Užívateľ programu ENIGMA CryptoMate si môže vybrať z troch reálnych modelov šifrovacieho prístroja ENIGMA pomocou ponuky *„Model Enigmy“*

1. **Wehrmacht/Luftwaffe**, poskytujúci nasledujúce šifrovacie komponenty:
   reflektory (nem. *Umkehrwalzen, UKW*): „B“, „C“
   rotory (nem. *Walzen*): „I“, „II“, „III“, „IV“, „V“
2. **Kriegsmarine M3,** poskytujúci nasledujúce šifrovacie komponenty:
   reflektory: „B“, „C“
   rotory: „I“, „II“, „III“, „IV“, „V“, „VI“, „VII“, „VIII“ (teda o 3 rotory naviac oproti W/L)
3. **Kriegsmarine M4,** poskytujúci nasledujúce šifrovacie komponenty:
   reflektory: „B“, „C“, „B Thin“, „C Thin“
   rotory: „I“, „II“, „III“, „IV“, „V“, „VI“, „VII“, „VIII“, „Beta“, „Gamma“ (teda o 2 rotory naviac oproti KM3)

Prepínací panel *„Režim (de)šifrovania“* umožňuje užívateľovi prepínať medzi nasledujúcimi režimami práce:

1. **interaktívny**: Verne simuluje narábanie s prístrojom. Užívateľ ako operátor stláča klávesy zodpovedajúce písmenám pôvodnej správy a prístroj okamžite „rozsvecuje žiarovku“ prislúchajúcu už (de)šifrovanému písmenu. *vstupný text* a *výstupný text* sa zobrazujú zároveň v príslušných editačných oknách. V tomto režime je umožnené meniť nastavenie ENIGMY počas procesu samotného (de)šifrovania.

2. **neinteraktívny**: Lepšie zodpovedá súčasným požiadavkám na rýchle (de)šifrovanie. Užívateľ najprv napíše (prípadne otvorí textový súbor, resp. prilepí text z ClipBoard-u pomocou *Lokálnej ponuky* dostupnej cez pravo-klik na editačnom okne či tlačítka *„Možnosti“* nad ním), zvolí *rýchlosť (de)šifrovania* pomocou posuvníka a následne spustí proces (de)šifrovania pomocou tlačítka *„Šifruj/Dešifruj“*. Počas procesu šifrovania nie je, na rozdiel od interaktívneho režimu umožnené meniť nastavenia ENIGMY, ale je povolené znižovať resp. zvyšovať rýchlosť šifrovania, ktorá môže nadobúdať hodnoty v rozsahu: *2 znak /s* až *CPU výkon*.

Stav procesu (de)šifrovania v neinteraktívnom režime je indikovaný *ProgressBar-om*, ktorý sa nachádza nad editačným oknom vstupného textu.

Pre dosiahnutie efektu vyššej historickej vieruhodnosti bol simulátor ENIGMA CryptoMate obohatený o dve komponenty, ktoré prispievajú k jeho funkcionalite len mimimálne, no neodmysliteľne patrili k reálnym modelom šifrovacieho prístroja ENIGMA. Sú to:

1. *Panel s klávesnicou*, ktorý poskytuje alternatívny spôsob zadávania vstupného textu v oboch režimoch, interaktívnom i neinteraktívnom.

2. *Panel so „žiarovkami“* (RadioButton-y) „podsvecujúcimi“ jednotlivé písmená Výstupného textu, ktorý funguje v oboch režimoch, okrem situácie, kedy je v neinteraktívnom režime zvolená najvyššia rýchlosť (de)šifrovania. Vtedy by „rozsvecovanie žiaroviek“ nemalo pre operátora (užívateľa) reálny zmysel a navyše by spomaľovalo proces (de)šifrovania.

Pod panelom s klávesnicou sa nachádza dôležité tlačítko *„Reset“*, ktoré okamžite po stlačení uvedie program ENIGMA CryptoMate do pôvodného stavu, v ktorom sa nachádzal po spustení.

Definícia kľúča a nastavenie ENIGMY

Kľúč ENIGMY je postupnosť znakov dodržiavajúca nasledujúci špeciálny formát:

B(T)-(B|G)-I-II-III; 01-01-01; A-A-A(-A); na-na-na-na-na-na-na-na-na-na

Táto postupnosť znakov sa zobrazuje v editačnom poli *„Kľúč“*, a pozostáva z nasledujúcich častí:

1. **B(T)-(B|G)-I-II-III;** 01-01-01; A-A-A(-A); na-na-na-na-na-na-na-na-na-na

   Výber a poradie rotorov (nem. *Walzenlage*) je možné ovplyvniť ComboBox-ami uvedenými popiskom *„Walzenlage“*. Určuje výber a poradie jednotlivých šifrovacích valcov oddelených znakom „-“: reflektor, „extra“ rotor (Iba model Kriegsmarine M4!), ľavý rotor, prostredný rotor, pravý rotor.

   Príklad: „**CT-G-VIII-II-IV“** naznačuje, že model použitej ENIGMY je „Kriegsmarine M4“ **(tenký reflektor** („C Thin“) **+ 4 rotory** (1 „extra“ rotor „Gamma“ + 3 rotory: „VIII“, „II“, „IV“ v tomto poradí)).

2. B(T)-(B|G)-I-II-III**; 01-01-01**; A-A-A(-A); na-na-na-na-na-na-na-na-na-na

   Natočenie rotorových krúžkov (nem. *Ringstellung*) je možné ovplyvniť ComboBox-ami uvedenými popiskom *„Ringstellung“* v rozsahu: 01 – 26. Technicky ide o relatívne natočenie popisného kovového krúžku s číslami (reprezentujúcimi 26 písmen abecedy) vzhľadom k internému drôteniu – jadru rotora. (presnejšie: Každý valec je vlastne reprezentácia permutácie abecedy, ktorá však pre zvýšenie možností nie je daná jednoznačne, ale je možné ju „posunúť“ do ľubovoľnej z 26 pozícii, napr. dve rôzne pozície abecedy sú: „ABC..XYZ“ a „BCD..YZA“).

   Príklad: „**14-01-09“** znamená, že ľavý rotor je určený permutáciou „posunutou“ o 13 doľava, prostredný svojím pôvodným nastavením a pravý „posunutý“ o 8 doľava.

3. B(T)-(B|G)-I-II-III**;** 01-01-01; **A-A-A(-A)**; na-na-na-na-na-na-na-na-na-na

   Počiatočnú pozíciu jednotlivých rotorov (nem. *Grundstellung*) je možné nastaviť ComboBox-ami uvedenými popiskom *„Grundstellung“* na ľubovoľnú počiatočnú pozíciu determinovanú písmenom, ktoré sa momentálne zobrazuje v „okienku“ a v každom okamihu jednoznačne určuje aktuálnu pozíciu rotoru.

   Príklad: „**B-X-C-I“** signalizuje, že „extra“ rotor je v pozícií „B“, ľavý rotor v pozícií „X“, prostredný v pozícií „C“ a pravý v pozícií „I“.

4. B(T)-(B|G)-I-II-III**;** 01-01-01; A-A-A(-A); **na-na-na-na-na-na-na-na-na-na**

   Párovanie písmen na prepájacom paneli (nem. *Steckerverbindungen*) je možné ovplyvniť ComboBox-ami v dolnej časti formulára, pričom platí pravidlo, že prepojenie sa dá aktivovať/deaktivovať iba vtedy, keď je aktívne/neaktívne prepojenie bezprostredne pred/za ním. Jedno prepojenie symbolizuje jednu transpozíciu, ktorá sa uplatní na písmeno pri procese (de)šifrovania ako prvý a zároveň posledný (de)šifrovací mechanizmus.

Príklad: „**AB-FI-YZ-NM-RQ-na-na-na-na**“ znamená, že su aktívne prepojenia medzi nasledujúcimi dvojicami písmen: A a B, F a I, Y a Z, N a M, R a Q. Štyri zvyšné prepojenia su neaktívne.

Nakonfigurovaný kľúč sa dá uložiť vo formáte „ENIGMA CryptoMate Key“ (prípona „eck“) pre opätovné použitie pomocou tlačítka „Uložiť“. Rovnako je možné takto uložený kľúč otvoriť a načítať pomocou tlačítka „Otvoriť“. Pri jeho načítaní sa ENIGMA CryptoMax automaticky nakonfiguruje.

Tlačítko *„Generátor kľúčov“* spustí vstavaný nástroj na generovanie náhodných kľúčov.

Generátor náhodných kľúčov

Tlačítko *„Nájdi“* umožňuje zvoliť cieľový adresár, kam budú kľúče uložené. Táto cesta sa zobrazí v editačnom riadku s titulkom *„Cieľ“*. V editačnom okienku *„Počet kľúčov“* je možné nastaviť počet kľúčov v rozsahu 1 – 999, ktoré sa naraz vygenerujú. Po stlačení tlačítka *„Generuj kľúče“* sa začnú generovať náhodné kľúče a priebeh tohto procesu je užívateľovi zobrazený pomocou ProgressBar-u priamo pod tlačítkom. Naposledy vygenerovaný kľúč sa zároveň zobrazí v editačnom riadku v spodnej časti formulára. Ten je možné okamžite použiť v simulátore stlačením tlačítka *„Použi kľúč“*. Prípadne prerušenie procesu generovania náhodných kľúčov a pôvodné nastavenia generátora sa vyvolajú stalčením tlačítka *„Reset“* v spodnej časti formulára.

Tlačítko s popiskom *„?“* otvorí informačný formulár, obsahujúci rôzne informácie o programe ENIGMA CryptoMate, znenie Všeobecenej verejnej licencie (angl. *General Public Licence*, *GPL*) a v neposlednom rade kompletné znenie užívateľskej nápovedy.

Krok-za-krokom demonštrácia posielania (a príjmania) šifrovaných správ

Aby správa mohla byť korektne zašifrovaná odosielateľom či dešifrovaná príjemcom, obidve strany musia musia nastaviť svoju ENIGMU do rovnakého počiatočného stavu, tj. 1. výber rotorov a ich poradie, 2. individuálne natočenie rotorových krúžkov, 3. pozícia rotorov a 4. párovanie písmen na prepájacom paneli musia byť identické. Všetky tieto nastavenia (nazývané *kľúč*) museli byť dohodnuté vopred a distribuované všetkým stranám v knihách kľúčov (angl. *codebooks*).

Počiatočné štádium ENIGMY, tzv. *kryptografický kľúč*, má niekoľko aspektov, ktoré je nutné nastaviť v tomto poradí:

1. *Výber a poradie rotorov* (nem. *Walzenlage*, angl. *Wheel order*) zahŕňa nasledovné komponenty (zľava):
   a) *Reflektor* (nem. *Umkerwalze*, angl. *Reflector*) je možné vybrať z dvoch modelov: „B“ a „C“ pre modely Wehrmacht/Luftwaffe a Kriegsmarine M3 a z modelov „B Thin“ a „C Thin“ pre model Kriegsmarine M4.
   b) Extra rotor je potrebné zaradiť iba v prípade, že používaný model je Kriegsmarine M4, voľbou medzi rotorom „B“ („Beta“) a „G“ („Gamma“).
   c) Ľavý rotor je možné zvoliť zo sady piatich rotorov („I“, „II“, „III“, „IV“, „V“) pre model Wehrmacht/Luftwaffe a zo sady ôsmich rotorov („I“, „II“, „III“, „IV“, „V“, „VI“, „VII“, „VIII“) pre modely Kriegsmarine M3 a Kriegsmarine M4.
   d) Prostredný rotor detto.
   e) Pravý rotor detto.
   Poznámka: Každý rotor je možné použiť iba na jednej pozícií.

2. *Natočenie rotorových krúžkov* (nem. *Ringstellung*, angl. *Ring settings*) je možné nastaviť pre každý z rotorov (ľavý, prostredný a pravý) individuálne v rozmedzí od 01 do 26, čo odzrkadľuje

počet písmen v abecede a vyjadruje relatívne natočenie rotorového jadra (angl. *wiring*) vzhľadom k popisnému abecednému krúžku.

3. *Pozícia rotorov* (nem. *Grundstellung*, angl. *Initial position of the rotors*) je počiatočná pozícia jednotlivých rotorov, ktorú je možné nastaviť pre každý z 3 (Wehrmacht/Luftwaffe a Kriegsmarine M3) resp. 4 (Kriegsmarine M4) rotorov individuálne a odzrkadľuje momentálnu pozíciu rotora, inak povedané, ktoré písmeno na obvode rotora sa zobrazuje v indikačnom okienku.

4. *Spárovanie písmen* (nem. *Steckerverbindungen*, angl. *Plugboard connections*) je možné nastaviť v rozsahu od 0 do 10 prepojení. Prepojenie sa aktivuje zaškrtnutím zaškrtávacieho políčka vedľa páru ComboBox-ov, v ktorých užívateľ následne zvolí písmená, ktoré budú navzájom prepojené. Poznámka: Po použití písmena v páre (prepojení) už nie je možné toto písmeno použiť v ďalšom páre.

Následne užívateľ začne písať správu do editačného okna „Vstupný text“ a jej zašifrovaná verzia zároveň vzniká v editačnom okne „Výstupný text“. Táto sa odošle adresátovi.

Keďže šifrovací systém ENIGMA je reciprokálny, príjemca správy nemusí prepínať svoju ENIGMU do špeciálneho dešifrovacieho režimu. Jednoducho nastaví svoju ENIGMU identicky s odosielateľom (podľa vopred dohodnutého kľúča) a postupuje ako pri šifrovaní: Zašifrovanú správu píše do editačného okna „Vstupný text“ a súbežne sa mu v editačnom okne „Výstupný text“ zobrazuje dešifrovaná správa.

ENIGMA bola navrhnutá tak, aby bola zabezpečená i v prípade, že anatómia rotorov je nepriateľovi známa, hoci v praxi bolo vyvinuté považlivé úsilie udržať ju v tajnosti. Ak je drôtenie v rotorových jadrách neznáme, celkový počet možných konfigurácií bol vyčíslený na okolo 10^{114} (približne 380 bitov); so známym drôtením a inými operačnými obmedzeniami okolo 10^{23} (76 bitov). Užívatelia ENIGMY boli uistení jej bezpečnosťou práve obrovským počtom možností; v tej dobe nebolo pre nepriateľa ani len pomyslitelné začať skúšať všetky možné konfigurácie *hrubou silou*.

Programátorská časť

Algoritmická charakterizácia

Substitúcia za každé písmeno môže byť vyjadrená matematicky ako *súčin permutácií*. Uvažujme troj-rotorovú Wehrmacht/Luftwaffe ENIGMU, nech P označuje transformácie prepájacieho panelu, U značí reflektor a L, M, R označujú činnosť ľavého, prostredného respektíve pravého rotora. Potom sa šifrovanie E dá vyjadriť ako $E = PRMLUL^{-1}R^{-1}P^{-1}$

Po každom stlačení klávesy valce rotujú, meniac tak transformáciu. Napríklad, ak sa pravý rotor otočí o i pozícií, transformácia sa stane nasledovnou $\rho^{i}R\,\rho^{-i}$, kde ρ je tzv. cyklická permutácia mapujúca A na B, B na C atď. Nápodobne môžu byť reprezentované ostatné rotory (prostredný a ľavý) ako j a k rotácií permutácií M a L. Šifrovacia funkcia potom vyzerá nasledovne: $E = P(\rho^{i}R\rho^{-i})(\rho^{j}M\rho^{-j})(\rho^{k}L\rho^{-k})U\,(\rho^{k}L^{-1}\rho^{-k})(\rho^{j}M^{-1}\rho^{-j})(\rho^{i}R^{-1}\rho^{-i})P^{-1}$.

Programová realizácia

Program ENIGMA CryptoMate pozostáva z hlavného programového modulu „Enigma“ a troch formulárových modulov: „Enigma_“, „Generator_“ a „About_“. Kľúčové procedúry / funkcie jednotlivých modulov sú v prehľade zvýraznené **hrubým písmom**, vedľajšie sú spomenuté *kurzívou*.

1. **Enigma_**: kľúčový modul obsahujúci kľúčovú funkciu **DeSifruj**, ktorá ako parameter dostane písmeno vstupného textu a zašifrované ho vracia ako svoju výstupnú hodnotu. Jednotlivé rotory sú reprezentované reťazcom 26 znakov, usporiadaných podľa permutácie, ktorú uplatňujú. Podľa počtu používaných rotorov je zopakovaný proces vyhľadania miesta (poradia) v abecede pre písmeno, upravenie tohto miesta (poradie) podľa relatívneho natočenia dvoch rotorov medzi ktorými prechod práve uvažujeme a napokon určenie substitúcie za dané písmeno na základe už spočítaného poradia v reťazci.
   Príklad: šifrovanie písmena **L**:
   0. spočíta sa poradie písmena v abecede: **12** (iba pred vstupom do prvého rotora!)
   1. toto poradie sa upraví podľa pozície prvého rotora, ak je natočený na písmene **D** (4) je potrebné to zohľadniť a upraviť poradie na: 12 + 4 – 1 = **15**
   2. v reťazci, ktorý reprezentuje prvý rotor, ‚`EKMFLGDQVZNTOWYHXUSPAIBRCJ`‘ vyberieme 15. písmeno, čo je substitúcia za naše L: **Y**
   3. spočíta sa poradie tohoto písmena (Y) v abecede: **25**
   4. toto poradie sa opäť upraví podľa pozície prvého rotora: 25 – 4 + 1 = **22**
   5. toto číslo sa pošle ďalej ako vstup do ďalšieho rotora, kde sa zopakujú kroky 1 – 5.

   Modul ďalej obsahuje procedúry *Registruj* (rutina na registráciu konfigurácie šifrovacieho prístroja pred spustením (de)šifrovania), *UpDate_kluc1* a *UpDate_kluc2* (rutiny na obnovenie časti kľúča po akejkoľvek zmene v nastavení šifrovacieho prístroja), *Rotuj* (rutina, ktorá uskutoční korektnú rotáciu príslušných rotorov, emulujúca aj efekt „dvoj-kroku“ prostredného rotora) a triviálna procedúrka *Rozsviet_ziarovku*, ktorá, ako už jej názov napovedá, zaškrtne korektný RadioButton podľa (de)šifrovaného písmena.

2. **Generator_**: obsahuje kľúčovú procedúru, vyvolanú pri stlačení tlačítka „Generuj kľúče“ **TForm2.Button1Click**, ktorá sa stará o vygenerovanie požadovaného počtu náhodných kľúčov. Je navrhnutá precízne, aby všetky kľúče boli rovnako prevdepodobné, snáď až na konfiguráciu prepájacieho panelu, kde konfigurácie s malým počtom prepojení majú štatisticky väčšie zastúpenie, ako v množine *všetkých* možných kľúčov. Kľúč s jedným prepojením je teda rovnako pravdepodobný ako kľúč s desiatimi prepojeniami, hoci kľúčov s desiatimi prepojeniami je v skutočnosti oveľa viac ako kľúčov s jedným prepojením.

3. **About_**: obsahuje iba *triviálne procedúrky* na obsluhu stlačenia niektorého z niekoľkých tlačítiek: „O Programe“, „Licencia“ či „Pomoc“.

Známe nedostatky programu ENIGMA CryptoMate

1. V neinteraktívnom režime práce nie je užívateľovi umožnené **prerušenie procesu (de)šifrovania**, rekonfigurácia šifrovacieho prístroja a jeho opätovné spustenie od bodu prerušenia. Program je jedine možné reštartovať tlačítkom „Reset“.

2. **Editovanie vstupného textu** pomocou panelu s klávesnicou a práca v interaktívnom režime (s či bez panelu s klávesnicou) je problematická, keďže kurzor editácie nie je automaticky presúvaný na koniec vloženého textu. Užívateľ tak musí sám meniť polohu kurzora pri kombinácií viacerých druhov editácie: vstup z klávesnice, prilepenie textu z ClipBoard-u, či otvorenie a načítanie súboru.

3. Stabilita programu nie je zaručená v prípade, že užívateľ úmyselne edituje súbor s uloženým kľúčom, zmení jeho formát a následne sa ho pokúsi otvoriť a nakonfigurovať podľa neho šifrovací prístroj. **Kľúč ma striktne stanovený formát**, ktorého nedodržanie nie je rozumne ustrážiteľné a detekovateľné ale najmä v programe nedoriešené počas jeho analýzy pri otváraní.

   Je teda odporúčané otvárať iba kľúče vygenerované vstavaným *Generátorom náhodných kľčov* alebo uložené priamo pomocou tlačítka *„Uložiť“*, kedy je zaručená ich kompatibilita s predpísaným formátom.

4. Nie je umožnené použitie špeciálneho programovateľného rotora **„D“**, predstaveného a uvedeného do praxe v neskorej fáze Druhej svetovej vojny.

O programe ENIGMA CryptoMate

Program ENIGMA CryptoMate je napísaný v jazyku Object Pascal a navrhnutý v integrovanom vývojovom prostredí Borland(R) Turbo Delphi(R) for Microsoft(R) Windows™. Program vznikol v auguste roku 2007. Autorom je Lukáš Kúdela.

Použité zdroje

1. http://en.wikipedia.org/wiki/Enigma_machine - Enigma machine Wikipedia entry
2. http://www.codesandciphers.org.uk/Enigma/index.htm - Tony Sale’s Codes and Ciphers