Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Komunikační rozhraní

Michal Macák

Bakalářská práce

2018

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2017/2018**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michal Macák**
Osobní číslo:	**I15247**
Studijní program:	**B2612 Elektrotechnika a informatika**
Studijní obor:	**Komunikační a mikroprocesorová technika**
Název tématu:	**Komunikační rozhraní**
Zadávající katedra:	**Katedra elektrotechniky**

Zásady pro vypracování:

Cílem práce je návrh modulu k připojení do PC přes standartní port (USB, sériová linka), který bude umožňovat zabezpečenou textovou komunikaci mezi dvěma PC na větší vzdálenosti vzduchem (kilometry) při dodržení platné legislativy.
Teoretická část práce bude obsahovat rozbor dostupných pásem, limity, teoretické dosahy a komunikační rychlosti, dále pak rozbor možnosti zašifrování textových zpráv. Praktická část práce bude obsahovat návrh HW pro připojení k PC a software pro PC s implementací jednoduchého šifrování, závěr bude obsahovat zhodnocení s praktickým testem přenosu.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

[1] VÁŇA, V. Mikrokontroléry ATMEL AVR: popis procesoru a instrukční soubor. Praha: BEN technická literatura, 2003.336 s. ISBN 978-80-7300-083-0.
[2] VÁŇA, V. Mikrokontroléry ATMEL AVR: programování v jazyce C. Praha: BEN technická literatura, 2003. 216 s. ISBN 978-80-7300-102-0.
[3] VLACH, J. Řízení a vizualizace technologických procesů. Praha: BEN technická literatura, 2002. 160 s. ISBN 978-80-86056-66-X.
[4] BRTNÍK, B. Základní elektronické obvody. Praha:BEN technická literatura, 2011. 156s. ISBN 978-80-7300-408-8
[5] RIPKA, P.; TIPEK, A. Master Book of Sensors. Praha : BEN, 2003. ISBN 0-12-752184

Vedoucí bakalářské práce: **Ing. Pavel Rozsíval**
Katedra elektrotechniky

Datum zadání bakalářské práce: **31. října 2017**
Termín odevzdání bakalářské práce: **11. května 2018**

Ing. Zdeněk Němec, Ph.D.
děkan

Univerzita Pardubice Česká republika
L.S.

Ing. Jan Pidanič, Ph.D.
vedoucí katedry

V Pardubicích dne 15. prosince 2017

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 17. 05. 2019

Michal Macák

PODĚKOVÁNÍ

Chtěl bych poděkovat vedoucímu bakalářské práce, Ing. Pavlu Rozsívalovi, za jeho odborné vedení a ochotu a mému bratrovi, Ing. Danielu Macákovi, za cenné rady.

ANOTACE

Cílem této práce je vytvoření programu s jednoduchým šifrováním textu, který bude pomocí komunikačních modulů přenášen na frekvenci 868 MHz mezi dvěma počítači. Teoretická část je věnována přístupným frekvenčním pásmům a možnostem šifrování. Praktická část obsahuje informace o použitém šifrování, zapojení modulu a test přenosu.

KLÍČOVÁ SLOVA

Šifrování textu, kryptologie, kryptografie, Enigma, šifrovací program, komunikační modul, LoRa, bezdrátová komunikace, dostupná frekvenční pásma.

TITLE

Communication Interface

ANNOTATION

The aim of this work is to create a program with a simple text encryption, which will be transmitted by communication modules at frequency 868 MHz between two computers. The theoretical part is devoted to accessible frequency bands and encryption options. The practical part contains informations about used encryption, module connection and transmission test.

KEYWORDS

Text encryption, cryptology, cryptography, Enigma, encryption program, communication module, LoRa, wireless communication, available frequency bands.

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

e.i.r.p.	ekvivaletní izotropický vyzářený výkon
e.r.p.	efektivní vyzářený výkon
NSA	National Security Agency
SRD	Short Range Device
RFID	Radio Frequency Identification
LoRa	Long Range
RLAN	Radio Local Area Network
ČTU	Český Telekomunikační Úřad
ITU	International Telecommunication Union

ÚVOD

V dnešní době čím dál více roste poptávka po spolehlivém zabezpečení komunikace a dat, kterou zapříčinilo riziko související se zneužitím informací, k němuž v dnešním globalizovaném světě internetu tak hojně dochází. Lidé se již ani nemohou spoléhat na sociální sítě, jelikož se z nich stal obrovský byznys založený na prodávání osobních dat korporacím. Celá situace se mnohonásobně vyostřila roku 2013, když Edward Snowden, bývalý zaměstnanec amerických zpravodajských služeb, vynesl na světlo přísně tajné dokumenty o celosvětovém odposlouchávání, shromažďování metadat a zneužívání informací k nežádoucím účelům. Odhalení dobrovolné spolupráce ze strany amerických gigantů s NSA nastolilo otázku, komu lze na internetu a v telekomunikacích tedy věřit, a především, jak se ochránit.

Smyslem této práce je nabídnout alternativní šifrovaný telekomunikační systém, který se nemůže rovnat dnešním sofistikovaným šifrovacím algoritmům, ale svým prozatím nepopulárním způsobem bezdrátového spojení a dosud neprozkoumaným algoritmem může na nějaký čas poskytnout pro uživatele bezpečí.

Práce je rozdělena do dvou částí. Teoretická část poskytuje informace o dostupných frekvenčních pásmech a omezeních s nimi spojenými. Dále se zabývá rozborem jednoduchých šifrovacích metod, jejich slabinami a historickým původem. Praktická část obsahuje rozbor mého šifrovacího programu, fungujícího na podobném principu, jako šifrovací stroj Enigma, a návod, jak ho používat. Mimo to se ještě zabývá komunikačním modulem, který realizuje ono bezdrátové spojení mezi uživateli, i testem jeho teoretických dosahů.

První kapitola obsahuje různá frekvenční pásma přístupná běžnému uživateli s určitými omezeními, možnostmi a přidělenými způsoby využití. Většinou se jedná o nepřekračování maximálních hodnot vyzářeného výkonu a zákaz poupravovat zařízení. Každé omezení má svůj důvod. Musí být zabráněno rušení, a pokud zařízení sdílí některé své kmitočty nebo sousední s jinými pásmy, jsou podmínky striktnější. Bez pravidel by celé frekvenční spektrum byl jeden velké chaos, kde každý by rušil každého, čímž by spousta důležitých aplikací zůstala nevyužita, ba dokonce by mohlo dojít ke škodám na životech.

Ve druhé kapitole jsou rozebrány snad všechny známé šifry používané od řeckoperských válek až po šifrovací stroj Enigma. Trocha místa je věnována i čtyřem algoritmům moderní kryptografie. Rozbor se zabývá vznikem šifry, jejími možnostmi a slabými články v řetězci algoritmů, ze kterých hojně čerpali především nepřátelé. Pozornost je zde upřena především na substituční šifry.

Třetí kapitola je praktickou částí. Její počátek pojednává o návodu, jak správně nastavit klíč a používat šifrovací program, aby nedošlo k nedorozumění. Po návodu je zde popsán i systém toho programu a proveden krátký rozbor osvětlující jeho potenciál a slabé články, které současně mohou posloužit jako varování, jak zbytečně při použití neriskovat. Další částí této kapitoly je popis komunikačního modul „LoPy4“ a ukázka programu do něj vloženého. Na posledním místě kapitoly je stručné ověření funkce a dosahu signálu s předpokladem minimálních ztrát informace.

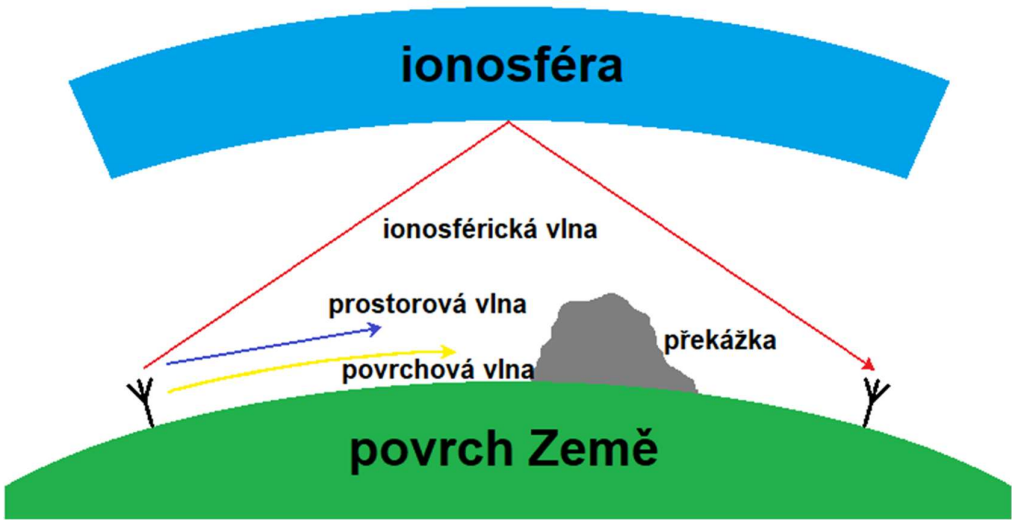
V závěru se nachází zhodnocení provedených testů přenosu.

1 DOSTUPNÁ FREKVENČNÍ PÁSMA

Využívání frekvenčních pásem pro bezdrátový přenos je v dnešní době výrazně okleštěno legislativou České republiky v důsledku čím dále většího využívání kmitočtového spektra. Hlavním motivem je zabránění rušení, které v krajních případech může způsobit i škody na životech a majetku. Proto vznikl Český telekomunikační úřad ČTU a Mezinárodní telekomunikační unie ITU, jejichž úkolem je mimo jiné přidělení frekvenčních pásem pro odlišné technologie a použití, vydávání všeobecných oprávnění, vyhledávání a odstranění rušení. Přesto stále existuje několik dostupných pásem, které lze využívat s drobnými omezeními vztahujícími se především na způsob využití, vyzářený výkon, intenzitu magnetického pole, maximální spektrální hustotu, klíčovací poměr a použitý druhu modulace.

1.1 27 MHz

Toto frekvenční pásmo pohybující se okolo 27 MHz umožňuje dosah na střední až velké vzdálenosti díky odrazům krátkých vln (3-30 MHz) od ionosféry, jež se vytváří díky ultrafialovému záření slunečních paprsků ve dne ve výšce 50 km a v noci 95 km nad povrchem Země. Samotná povrchová (přízemní) vlna dosahuje pouze desítek km.



Obrázek 1: Odraz vlny od ionosféry

Toto pásmo je hojně využíváno uživateli CB stanic, kteří se omezují na povrchovou vlnu, aniž by se na ně vztahovaly registrace nebo poplatky. Použití je podmíněno pravidly všeobecného oprávnění č. VO-R/7/11.2016-12 [1], které nařizuje dodržování stanovených

frekvencí pro kanály, z toho některé z nich jsou přednostně určeny pro konkrétní použití. Například svolávací kanál, který slouží k plánovanému setkání dvou uživatelů, kteří následně přejdou na jiný kanál. Dalšími jsou tísňový kanál, dopravní kanál pro vzájemné šíření informací mezi řidiči, kanály pro opakovače, mezinárodní kanál pro řidiče kamionů a kanál pro přenos dat. Je zakázáno používat jakékoliv zesilovače vysokofrekvenčního výkonu a antény s horizontální polarizací, vysílat pro komerční účely a používat stanice na palubě letadla. Stanice nesmí působit rušení stanicím radiokomunikačních služeb. Běžný dosah stanice se pohybuje od jednotek až po desítky kilometrů. Za ideálních podmínek, jako je vhodné umístění antény a příznivý stav ionosféry, lze dosáhnout i dvojnásobného dosahu.

Zařízení krátkého dosahu (SRD) jsou zařízení, u kterých je pouze malé riziko rušení z důvodu použití nízkého vysílacího výkonu, a proto je lze volně využívat na vzdálenost desítek metrů. Aby toto bylo zachováno, je nutno dodržovat všeobecné oprávnění č. VO-R/10/11.2016-13 [1]. Zařízení nesmí být mechanicky ani elektricky měněna, doplňována vysokofrekvenčními zesilovači ani vybavována jinými anténami než stanovenými výrobcem, působit rušení stanicím radiokomunikačních služeb ani překračovat mezní hodnoty. Obvyklým příkladem použití jsou různé hračky jako auta na dálkové ovládání.

1.2 174-230 MHz

Pásmo se řadí do ultra krátkých vln. Při takových frekvencích již nedochází k odrazu vlny od ionosféry a i povrchová vlna má menší dosah. Teoretický dosah se pohybuje v řádech desítek metrů.

Je využíváno bezdrátovými profesionálními mikrofony s maximálním vyzářeným výkonem 100 mW e.r.p. a se zákazem rušení stanic v rozhlasové službě.

Pásmo je využíváno i na frekvenci 174-216 MHz zařízeními krátkého dosahu k bezdrátovému přenosu zvuku s veřejným oprávněním č. VO-R/10 čl. 10 [1]. Dle něj musí být dodržen maximální vyzářený výkon 50 mW e.r.p., protože je pásmo přednostně vyhrazeno pro rozhlasové služby. Nesmí dojít k rušení televizního signálu a zařízení nesmí obsahovat ochranu proti rušení rozhlasovou službou.

1.3 433 MHz

Je určeno pouze pro přenos dat a zákonem omezeno na hodnotu vyzářeného výkonu 10 mW. Teoretický dosah je v řádech od jednotek metrů až po jednotky km. Jde tedy o zařízení krátkého

dosahu, na které se vztahuje všeobecné oprávnění č. VO-R/10/11.2016-13 [1]. Běžné využití pásma spočívá v komunikačních modulech a dálkových ovladačích. Na tomto kmitočtu se lze často setkat s rušením ostatních zařízení.

1.4 446 MHz

Též zvané PMR pásmo, s maximálním povoleným vyzářeným výkonem 500 mW e.r.p. má krátký dosah od desítek metrů až po 10 km v závislosti na terénu. Je využíváno občanskými radiostanicemi s podmínkou dodržování všeobecného oprávnění č. VO-R/3/6.2016-9 [1]. Stanice s digitální modulací smí být používány pouze na frekvenčním úseku 446,1-446,2 MHz, zatímco s analogovou modulací na 446,0-446,2 MHz. Není dovoleno provádět mechanické ani elektrické změny na stanici. Anténa musí být připevněna, aby nebylo možné nahradit ji jinou. Stanice nesmí rušit přednostní radiokomunikační služby.

1.5 470-789 MHz a 832-862 MHz

Pásma jsou využívána k bezdrátovému přenosu zvuku pro zařízení s krátkým dosahem, který se pohybuje v řádech desítek metrů, a vztahuje se na ně tedy všeobecné oprávnění VO-R/10/11.2016-13 [1]. Podmínky jsou podobné jako u pásma 174-230 MHz. Maximální povolený vyzářený výkon je 20 mW e.r.p. Pro mikrofony nošené na těle je povolený vyzářený výkon zvýšen na 50 mW e.r.p. Je zakázáno rušit rozhlasové služby a být chráněn proti rušení touto službou.

1.6 863-865 MHz

Je využíváno mikrofony pro akustické aplikace k bezdrátovému přenosu zvuku pro zařízení s krátkým dosahem s všeobecným oprávněním VO-R/10/11.2016-13 [1]. Maximální povolený vyzářený výkon činí 10 mW e.r.p.

1.7 868-870 MHz

Toto pásmo je určené pro aplikace nespecifikovaných zařízení krátkého dosahu a vztahuje se na něj veřejné oprávnění č. VO-R/10 čl. 3 [1]. Pro frekvence 868-869,2 MHz platí maximální povolený vyzářený výkon 25 mW e.r.p s teoretickým dosahem v řádech jednotek kilometrů.

Pro 869,4-869,65 MHz smí tato dosahovat až 500 mW e.r.p. Pro 869,7-870 MHz pouze 5 mW e.r.p. Příkladem použití mohou být třeba komunikační moduly pro bezdrátový přenos dat.

1.8 870-960 MHz

Pásmo určené pouze pro provoz mobilních telefonů GSM. Pro běžného uživatele jsou dostupné pouze frekvence 880,1-914,9 MHz pro směr od mobilní stanice k základové stanici a 925,1-959,9 MHz pro opačný směr kvůli plně duplexnímu přenosu. Teoretický maximální dosah signálu je 35 km. Okolní frekvence 876-880,1 MHz a 925,1-959,9 MHz jsou využity pro bezdrátové komunikace železniční aplikace GSM-R řadící se mezi nadřazené systémy, které nesmí být rušeny. Komunikační rychlosti se pohybují okolo 13 kbit/s.

1.9 1626,5-1660,5 MHz

Toto pásmo označené jako „L" je využíváno aplikacemi pozemské stanice družicové pohyblivé služby. Užití je podmíněno všeobecným oprávněním č. VO-R/1 [1]. Maximální vyzářený výkon je určen provozovatelem družicové sítě. Dosah signálu musí být minimálně 800 km vertikálním směrem, aby bez problémů bylo možné komunikovat s družicí.

1.10 1785-1805 MHz

Využité pro bezdrátový přenos zvuku pro zařízení s krátkým dosahem s veřejným oprávněním č. VO-R/10/11.2016-13 [1]. Maximální povolený vyzářený výkon je 20 mW e.i.r.p., v případě mikrofonu nošeného na těle až 50 mW e.i.r.p. Předpokládaným dosahem jsou desítky metrů.

1.11 2,4 GHz

Používání RFID, RLAN a zařízení krátkého dosahu je podmíněno veřejnými oprávněními č. VO-R/12/09.2010-12 a VO-R/10/11.2016-13 [1].

Pro RFID je vyhraněno pásmo 2446-2454 MHz. Pro použití uvnitř budov lze vyzářit výkon až 4 W e.i.r.p. Venku je tento výkon omezen pouze na 500 mW e.i.r.p.

RLAN lze používat v pásmu 2400-2483,5 MHz s maximálním vyzářeným výkonem 100 mW e.i.r.p. Předpokládaný rozsah je v řádech desítek metrů.

Nespecifikovaným zařízením krátkého dosahu je přiděleno pásmo 2400-2483,5 MHz s maximálním vyzářeným výkonem 25 mW e.i.r.p.

1.12 10 GHz

Toto pásmo konkrétně zabírá frekvence od 10308 do 10574 MHz a smí být provozováno jen s dodržením všeobecného oprávnění VO-R/2/01.2010 [1]. Je využíváno pouze radiovými systémy bod-bod. Střední výkon přivedený na anténní napaječe smí být maximálně 2 mW. Maximální dosah je 30 km.

1.13 71-76 GHz a 81-86 GHz

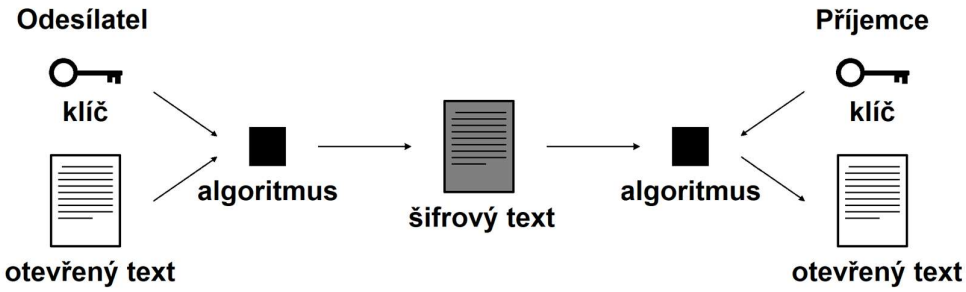
Tato pásma jsou dostupná pro užití spoje typu bod-bod s podmínkou respektování všeobecného oprávnění č. VO-R/23/09.2013-5 [1] a dodržení ohlašovací povinnosti. Uživatel nesmí rušit ostatní služby využívající toto pásmo. Teoretický dosah se předpokládá v desítkách kilometrů.

2 ŠIFROVÁNÍ TEXTOVÝCH ZPRÁV

Kryptologie je věda zabývající se utajováním informací formou přepsání (zašifrování) do takové podoby, ve které bude dávat zcela odlišný nebo dokonce žádný smysl. Motivem je zabránit získání informace třetí stranou, jež je může zneužít ve svůj prospěch. Nejčastějšími důvody, proč je kryptologie neoddělitelnou součástí lidských životů v moderní společnosti, bývají rizika spojená s vojenskými účely, průmyslovou špionáží, citlivostí osobních údajů, soukromou korespondencí i odcizením hesel.

Kryptografie je odvětvím kryptologie, které se zabývá vývojem šifrovacích metod s co možná nejvyšší bezpečností a nejsnadnější možností manipulace pro uživatele. Vyvinout spolehlivé šifrování může být poměrně snadné, ale provést to takovým způsobem, aby bylo možné ho i bez problému s oprávněním dešifrovat, není vždy lehký úkol. Dnes již existuje spousta různých sofistikovaných druhů šifrování velmi znesnadňujících prolomení šifer, avšak ani protivníci nezahálejí a neustále pracují na nových způsobech, jak vyzrát nad kryptografy.

Kryptoanalýza je opakem kryptografie. Toto odvětví si klade za cíl získat z šifry skryté informace bez znalosti klíče a přijít na způsob, jak učinit použitou šifrovací metodu zranitelnou i do budoucna pro opětovné získání informací.



Obrázek 2: Princip šifrování a dešifrování zprávy [2]

Princip celého procesu je patrný z obrázku 2. Odesílatel nejdříve zvolí vhodný šifrovací klíč, podle kterého bude otevřený text algoritmem zašifrován na šifrový text. Následuje předání šifrového textu příjemci, kde bývá občas cestou zachycen třetí stranou. Příjemce po obdržení zprávy použije dešifrovací klíč, který pomocí algoritmu šifrový text dešifruje na otevřený text.

2.1 Základní pojmy

2.1.1 Otevřený text

Je smysluplný text před zašifrováním, který má zůstat před třetí stranou uchráněn. Obvykle bývá, pokud to situace dovoluje, pro přehled zapisován malými písmeny, aby ho bylo možné rozlišit od šifrového textu.

2.1.2 Šifrový text

Je již zašifrovaný text ukrývající informaci před třetí stranou. Pro přehled bývá obvykle zapisován velkými písmeny.

2.1.3 Algoritmus

Algoritmus je metodou neboli šifrovacím systémem, použitým pro zašifrování otevřeného textu. Je vhodné uchovávat i v tajnosti, jaký algoritmus byl použit, protože tím se velice ztíží podmínky pro kryptoanalytiky. V takovém případě nikdo neví, kde začít, což může zabrat spoustu času a stále nemusí dojít k prolomení. Snem každého kryptografa je vyvinout tak sofistikovaný algoritmus, že odradí kryptoanalytika od všech pokusů dříve, než s nimi začne. Bohužel, počet způsobů, jakými lze jedinou metodou zašifrovat zprávu, je konečné číslo dávající třetí straně naději v úspěch. Algoritmus využívá při šifrování dva základní systémy, jež lze i kombinovat. Jsou jimi substituční a transpoziční systém.

Substituční systém zaměňuje jeden znak za jiný. K tomu je zapotřebí otevřené a šifrové abecedy skládající se ze znaků, které jsou spolu zaměněny podle jejich pořadí v abecedách. Obě abecedy obvykle obsahují stejné znaky, avšak mohou se i lišit. Substituce nezaměňuje pouze samotné znaky, ale i slova. Takové šifře se však obvykle neříká šifra, ale kód. Kód bývá obvykle nespolehlivý, protože třetí strana může podle kontextu zprávy odhadnout jeho význam. Proto se v moderní kryptografii používá jen zřídka.

Transpoziční systém funguje na principu změn pozic jednotlivých znaků (písmen) v textu. Ač jde o poměrně jednoduchý systém, počet kombinací roste s délkou textu, což vede k vysokým číslům. Pokud se omezíme pouze na transpoziční systém, počet kombinací je faktoriálem počtu znaků v textu. Typickým příkladem může být případ, kde otevřený text „zpráva“ je zašifrován tak, že znaky jsou rozděleny do dvojic a znak s lichým pořadím se prohodí se znakem se sudým pořadím. Šifrový text následně vypadá takto: „pzárav“. U tak krátkého textu lze obsah otevřeného textu snadno odhadnou, protože jeho délka a počet použitých slov je velmi malý.

2.1.4 Klíč

Je prvek nutný k zašifrování otevřeného textu algoritmem. Bez klíče, tedy s jediným neměnným klíčem, by bylo možné zašifrovat a dešifrovat text pouze jediným způsobem, což by v případě odhalení algoritmu třetí stranou vedlo k okamžitému dešifrování všech zpráv. Proto je nutné, aby algoritmus obsahoval co nejvyšší počet použitelných klíčů, který by při dešifrování neelegantní metodou vyzkoušení všech možností zabral tolik času, aby po konečném získání otevřeného textu byla informace pro třetí stranu již bezcenná.

Při symetrickém šifrování odesílatel i příjemce sdílí identické klíče, kterými lze zprávu zašifrovat a následně dešifrovat. Je to jednodušší, avšak zranitelnější varianta. V případě, že je

klíč jednoho uživatele odhalen, je odhalen i klíč druhého, čímž se odkrývá celá korespondence pro třetí stranu. Pokud ten samý klíč mezi sebou používá mnohem více uživatelů, je odhalení hotová katastrofa, jakou bylo například prolomení šifrovacího stroje Enigma.

Asymetrické šifrování využívá odlišných dvou klíčů. Šifrovací tzv. „veřejný“ na straně odesílatele a dešifrovací tzv. „soukromý“ na straně příjemce. Zatímco veřejný klíč znají oba korespondenti a nemusí se jím nijak tajit, protože je pro účel dešifrování naprosto bezcenný, soukromý klíč zná pouze příjemce zprávy. Tím odpadá riziko při distribuci klíčů, do které může zasáhnout třetí strana.

2.1.5 Heslo

Heslo je určitou formou klíče obsahující slova nebo čísla. Pokud je otevřený text delší než heslo, bude se během šifrování pravidelně opakovat, dokud nedosáhne konce.

2.1.6 Klamač

Též zvaný „matoucí znak“ je znak, jež byl vložen během šifrování do textu za účelem ztížení kryptoanalýzy. Při dešifrování se opět odstraňuje. Jde o určitou formu šifrování transpozičním systémem, protože vložením klamače před jiný znak v textu dojde ke změně jeho pořadí. Pokud by byl samotný otevřený text šifrován pouze vložením klamače, člověk by si toho mohl ihned všimnout, avšak v dnešní době, kdy kryptoanalýzu provádějí i stroje, které zkouší všechny možné kombinace klíčů a následně vyhledávají určitá často používaná slova nebo fráze, mohou tato slova přehlédnout.

2.1.7 Třetí strana

Třetí stranou se obvykle v kryptologickém oboru nazývá ten, pro koho zpráva není určena, avšak má snahu se k jejímu obsahu dostat. Je jím například kryptoanalytik.

2.2 Historie

2.2.1 Steganografie

Steganografie je vědou zabývající se fyzickým ukrytím informace tak, aby si třetí strana ani neuvědomila, že před sebou nějakou skrytou informaci má. Název steganografie je odvozen

z řeckých slov steganos (skrytý) a graphein (psát). Nevýhodou je, že jakmile je metoda jednou prozrazena, třetí strana dostane celou zprávu. Proto začala vznikat kryptografie.

První zmínky o použití jsou datovány od 5. století př. n. l., kdy se schylovalo k řeckoperské válce. Perský král měl v úmyslu překvapit Řeky silnou armádou a začal rekrutovat síly. Toho si však všiml Demaratus, řecký vyhnanec, který, ač nedobrovolně, opustil svou vlast a usídlil se v Persii, cítil se být stále Řekem. Rozhodl se tedy, že Řeky varuje, ale hrozilo zde velké nebezpečí, že jeho zpráva bude odhalena. Použil tedy voskové psací destičky, ze kterých odstranil vosk a zapsal zprávu na jejich dřevěnou část. Destičky pak opět zalil voskem, aby informace skryl. Tento trik mu vyšel. Sparta se stačila na Peršany připravit a zvítězila.

Dalším, kdo využil steganografii, byl Histiaios, který chtěl podnítit vzpouru proti perskému králi. Potřeboval vyslat vzkaz vzbouřencům, ale opět zde bylo vysoké riziko prozrazení informace. Proto svému poslu oholil hlavu, napsal zprávu na kůži jeho lebky a počkal, dokud mu opět nenarostly vlasy.

Číňané psali tajné zprávy na kus hedvábí, které zmačkali do kuličky, zalili voskem a nechali posla, aby onu kuličku spolkl. Ač nepříjemná a nebezpečná metoda, slavila poměrně velký úspěch.

Italský vědec Giovanni Porta popsal metodu, při které je vařené vejce popisováno speciálním inkoustem, který pronikne skořápkou a zanechá na ztuhlém bílku stopy po psaní, ale skořápka zůstává netknuta. Příjemce zprávy už jen musí vejce oloupat a vzkaz si přečíst.

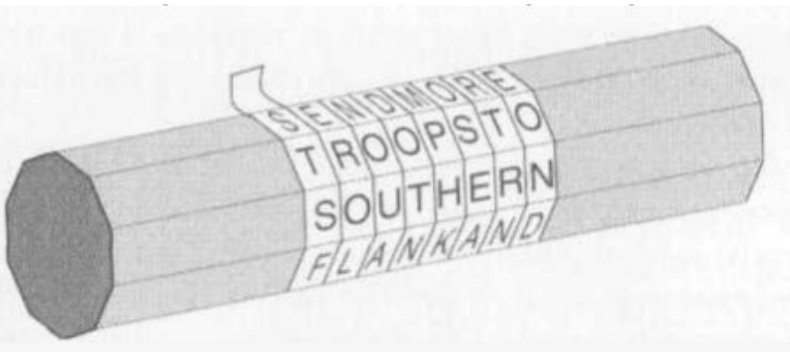
Podobnou metodou je od 1. století našeho letopočtu užívání neviditelného inkoustu z mléka pryšce. Neviditelný inkoust se používá dodnes.

Moderní metodou se stala mikrotečka, kterou hojně využívali němečtí špioni během 2. světové války. Její princip spočívá ve zmenšení textu do velmi malých rozměrů a použití jako tečky. Časem byla tato metoda prozrazena, třetí strana začala kontrolovat korespondenci a hledala odlesk těchto teček na dopisech.

2.2.2 Scytale

Tato kryptografická metoda se řadí mezi transpoziční. Principem je vzít pruh papíru a obmotat ho kolem předmětu ve tvaru válce či hranolu o určitém průměru tak, aby na něj bylo možné psát jako na souvislý kus papíru. Když je otevřený text hotov, je odňat z válce. V případě, že bude vložen kolem válce o jiném průměru, text bude v jiném pořadí než před tím a nebude tedy možné jej přečíst. Metoda je účinná do té doby, než třetí strana zjistí, jak funguje. Pak už stačí jen zkoušet válce o různých průměrech. Scytale tedy obsahuje jednoduchý klíč ve formě

průměru válce a jeho hlavním úkolem pro zachování bezpečí informace je uchování tajemství o použitém algoritmu šifry.



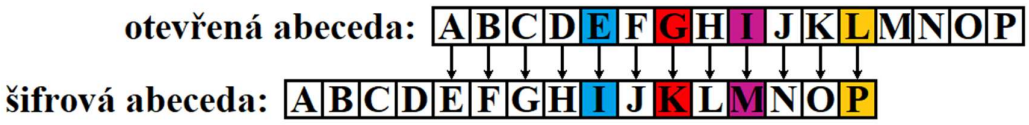
Obrázek 3: Princip šifrování Scytale [1]

V roce 404 př. n. l. této metody využil řecký posel, který ji dokázal zkombinovat se steganografií tím, že zprávu napsal na svůj opasek a celou cestu ho měl okolo pasu, zatímco šifrový text byl uschovaný na vnitřní straně. Díky úspěšnému doručení zprávy byl další perský král poražen.

2.2.3 Monoalfabetická šifra

Tato šifra fungující na substitučním systému obsahuje pouze jednu šifrovou abecedu, z čehož plyne, že všechna jednotlivá písmena otevřené abecedy se budou vždy zaměňovat se svým konkrétním protějškem z šifrové abecedy.

Caesarova šifra je primitivní verzí monalfabetické šifry, která využívá posunu mezi otevřenou a šifrovou abecedou o konkrétní počet míst.

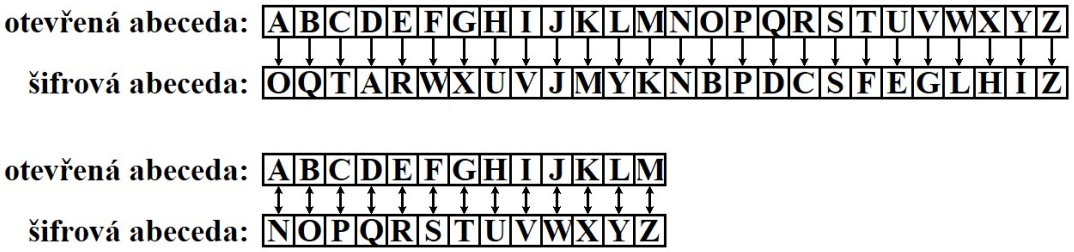


Obrázek 4: Caesarova šifra

Na obrázku 4 je vidět princip této metody. Klíčem je v tomto případě informace o posunutí šifrové abecedy o 4 místa. Pokud budeme chtít zašifrovat slovo „legie“, pak se změní na „PIKMI“. U tak jednoduchých metod je opět nutné uchovat algoritmus v tajnosti, protože počet možných klíčů je s použitím mezinárodní abecedy pouze 26 (25, pokud obě abecedy nesmí být

identické). To znamená, že třetí strana při luštění může dešifrovat text jen během desítek minut pouhým zkoušením všech možností.

Proto se využívá mnohem sofistikovanějších substitučních metod, kde šifrová abeceda je mnohem více promíchána, čímž za použití stejných znaků jako v otevřené abecedě, je možno dosáhnout mnohem většího počtu klíčů (kombinací), který se rovná faktoriálu počtu písmen abecedy.



Obrázek 5: Příklady sofistikovanějších substitučních klíčů

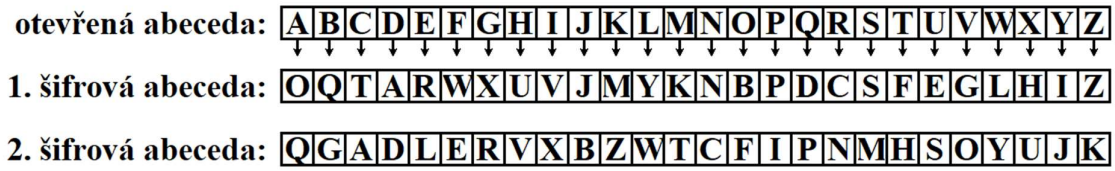
První použití je známé z let 58-50 př. n. l. Juliem Caesarem, jež dal zašifrovanou zprávu doručit do obleženého tábora. Obvykle používal posun o 3 místa. To není jediným systémem, který byl císařem používán, avšak záznamy o jeho sepsaných šifrách se nedochovaly.

Ač sofistikovanější substituční šifra může budit zdání bezpečného systému, je často efektivně napadávána frekvenční analýzou, která se zaměřuje na četnost jednotlivých znaků šifrového textu a porovnává ji s četností znaků vyskytujících se v libovolných otevřených textech psaných stejným jazykem. Poté, co jsou získány podezřelé znaky, tedy znaky, o nichž tušíme, se kterými jsou substituovány, musí se brát v úvahu i znak s četností jim blízký, protože jen substituovat znaky podle četnosti nestačí. Pravděpodobnost této dokonalé shody je příliš malá. Následuje zkoumání okolních znaků v textu, zda se obvykle vyskytují v okolí podezřelých znaků. Aby mohla být frekvenční analýza úspěšná, musí kryptoanalytik luštit dostatečně dlouhou zprávu, protože u krátkých textů jsou četnosti výskytu znaků nesrovnatelné s dlouhým textem.

První zmínky o počátcích frekvenční analýzy pochází z arabského světa z doby 9. století. Teologové, kteří zkoumali slova, se rozhodli zkoumat i samotná písmena a uvědomili si jejich rozdílnou četnost, které náležitě využili v kryptoanalýze.

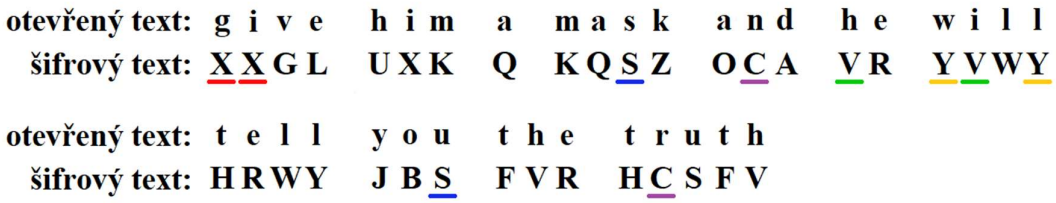
2.2.4 Polyalfabetická šifra

Na rozdíl od šifry monoalfabetické polyalfabetická aplikuje více šifrových abeced, které se mezi sebou prostřídávají. Z této metody plyne, že ze dvou různých písmen otevřené abecedy se může stát jedno a to samé písmeno abecedy šifrové, čímž údaje o četnosti výskytu jednotlivých písmen v šifrovém textu ztrácí na hodnotě a s každou další šifrovou abecedou se pro kryptoanalytiky značně komplikuje frekvenční analýza.



Obrázek 6: Klíč polyalfabetická šifry se dvěma šifrovými abecedami

Například dle obrázku 6 jde o aplikaci dvou šifrových abeced, které se budou střídavě používat podle toho, zda právě dochází k šifrování písmena s lichým či sudým pořadím v textu. Pro první písmeno tedy přiřadíme první šifrovou abecedu, pro druhé druhou a pro třetí opět první. Pro názorný postup šifrování celé metody poslouží citát Oscara Wilda: „Give him a mask, and he will tell you the truth."

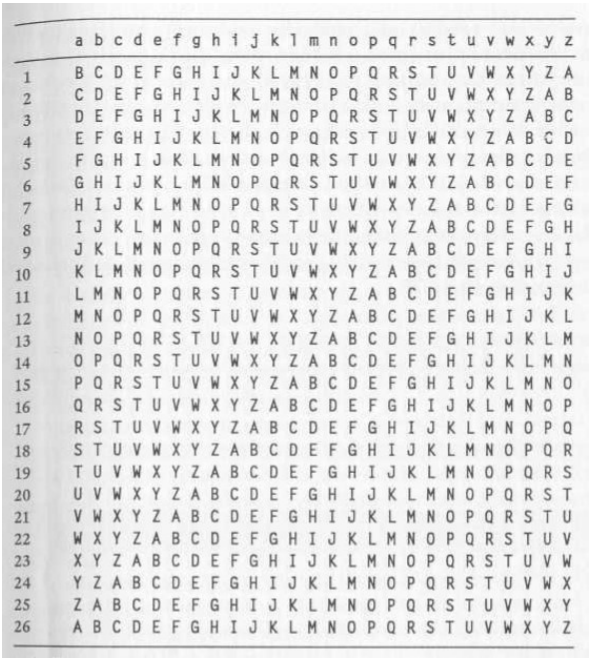


Obrázek 7: Otevřený a šifrový text zašifrovaný dle uvedeného klíče

Obrázek 7 potvrzuje tezi o stejném výsledku z dvou různých nezašifrovaných písmen, a to hned na prvních dvou místech textu, pro názornost červeně podtržených. Z písmen „g" a „i" se stalo „X". Kryptoanalytik teď musí řešit problém, jaká dvě písmena otevřené abecedy lze zaměnit za „X" a jakými dalšími písmeny šifrové abecedy se mohou stát.

S tímto nápadem přišel v 15. století Leon Battista Alberti, avšak jej dostatečně nerozvinul. Až francouzský diplomat Blaise de Vigenère využil jeho potenciál, když vytvořil 26 šifrových abeced, které se liší od každé předchozí tím, že jsou posunuty o jednu pozici. Aplikuje se zde

tedy Caesarova šifra. Sepsáním těchto abeced do tabulky získáváme tzv. „Vigenèrův čtverec“, viz obrázek 8.



	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Obrázek 8: Vigenèrův čtverec [2]

Pro názornou ukázku použití bude zvoleno například heslo „LISSIE“ a otevřený text „praeparet bellum“. Prvním písmenem hesla je „L“, proto přichází na řadu řádek začínající tímto písmenem a tj. řádek č. 11. Prvním písmenem otevřeného textu je „p“, což na řádku č. 11 substituuje písmeno „A“. Jelikož je heslo kratší než text, musí být prodlouženo, aby bylo možné vždy přiřadit řádek, což ve výsledku nabyde podoby „LISSIELISSIELIS“. Opakování tohoto postupu pro druhé písmeno zašifruje „r“ jako „Z“. Šifrový text ve výsledku vypadá „AZSWXECMLTMPWCE“. Postup pro první dvě písmena je předveden na obrázku 9.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1.	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2.	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3.	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4.	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5.	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6.	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7.	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8.	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9.	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10.	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11.	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12.	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13.	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14.	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15.	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16.	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17.	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18.	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19.	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20.	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21.	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22.	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23.	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24.	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25.	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Obrázek 9: Použití Vigenèrova čtverce

2.2.5 Homofonní šifra

Ač se na první pohled zdá býti polyalfabetickou šifrou, jde ve skutečnosti o monoalfabetickou. Použitá písmena otevřeného textu jsou rozepsána do frekvenční tabulky a podle četnosti jejich výskytu v textech v konkrétním jazyce jim je přidělen určitý počet hodnot, kterých mohou v šifrovém nabývat. Například písmeno „a“ v anglických textech zabírá 8 % textu. Bude tedy pro něj v šifrové abecedě vyhrazeno 8 symbolů, které budou libovolně prostřídány. Jeden konkrétní symbol nesmí být použit pro více často objevujících se písmen, protože by jej nešlo dešifrovat. Proto zpravidla by symbol měl být několikamístným číslem, nikoliv písmenem, protože počet použitých symbolů by měl být mnohem vyšší než počet písmen otevřené abecedy, jinak homofonní šifra ztrácí svůj potenciál. Naopak písmeno „q“ zabírá pouze zhruba 0,1 %, což mu přiřazuje maximálně 1 symbol. Samozřejmě je zde možnost každému znaku přiřadit více symbolů, avšak za cenu větší komplikovanosti při šifrování a dešifrování. Příklad otevřené a šifrové abecedy s přiřazenými symboly podle četnosti výskytu v anglických textech lze vidět na obrázku 10.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

Obrázek 10: Klíč homofonní šifry [2]

Jako názorná ukázka poslouží zašifrování textu „assassination“, protože se v něm opakují písmena „a“, „s“, „i“ a „n“. Výsledek může například vypadat takto: „12 11 19 78 36 96 70 71 67 20 88 00 58.“ Tato podoba šifrového textu je velmi uspokojivá, protože se žádný symbol neopakuje, ale u delších textů k tomu dochází, čehož se chápe frekvenční analýza. Opět se zaměřuje na četnost výskytu (tentokráte symbolů), a to nejprve u písmen zřídka se objevujících, jako jsou v anglickém jazyce „q“ a „u“, protože obě mívají přiřazený pouze jeden symbol.

Vigenèrův čtverec je jistě mnohem bezpečnější metodou, ale uživatelé se zabývali i druhou stránkou věci, jakou byla rychlost šifrování kvůli urgentnosti předání zprávy, pohodlnost a bezchybnost. Během šifrování a dešifrování často docházelo k chybám v důsledku přehlédnutí správného výsledku. Proto dávali přednost mnohem pohodlnější homofonní šifře. To se mělo ale brzy změnit.

2.2.6 Bealova šifra

Tato šifra očíslováním počátečních písmen hesla sestaví šifrovou abecedu čísel, kterými je pak otevřený text písmeno po písmeni zašifrován. Nutným předpokladem pro zašifrování všech znaků v otevřeném textu je požadavek na délku hesla, které by mělo na počátečních písmenech minimálně jednou obsahovat každé písmeno v otevřeném textu použité.

Například zašifrování slova „quit“ heslem převzatým z Napoleonova citátu: „Riches do not consist in the possession of treasures, but in the use made of them.“ Očíslování pak probíhá

takto: „[1]Riches [2]do [3]not [4]consist [5]in [6]the [7]possession [8]of [9]treasures, [10]but [11]in [12]the [13]use [14]made [15]of [16]them.“ Z toho vznikne tabulka 1.

Tabulka 1: Klíč Bealovy šifry

1	r	6	t	11	i	16	t
2	d	7	p	12	t		
3	n	8	o	13	u		
4	c	9	t	14	m		
5	i	10	b	15	o		

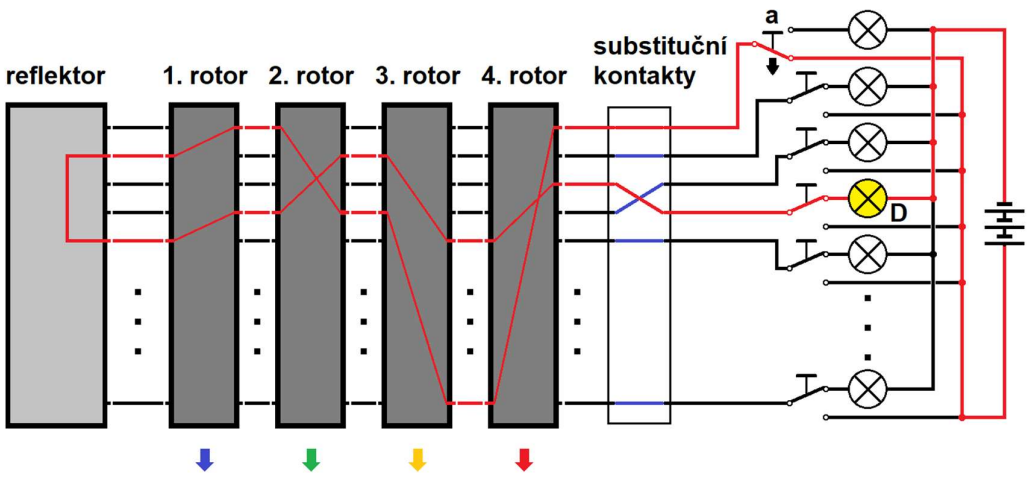
Výsledný šifrový text nabývá podoby „q 13 11 6“. Protože klíč neobsahoval žádné počáteční písmeno, nebylo možné šifrový text řádně zašifrovat.

Původcem šifry byl Thomas J. Beale, který v 1. polovině 19. století trávil čas na divokém západě. Ve státě Virginie se seznámil s majitelem hotelu Robertem Morrisem, a když po dvou letech zjistil, že je čestný muž, rozhodl se uschovat u něj svoji kovovou skřínku s tím, že nevrátí-li se během deseti let, smí ji otevřít a přečíst si zašifrovaný vzkaz, který rozluští klíčem nacházejícím se v příštím dopise. Onen vzkaz měl obsahovat lokaci Bealova pokladu. Beale ani dopis však už nikdy nedorazí. Po deseti letech čekání Morris otevřel skřínku a dal se marně do dešifrování. Ač část dopisu byla později někým jiným rozluštěna a příběh se stal publikací populárním tak, až přilákal hledače pokladů, poklad zůstal nenalezen. Zbytek šifry je dodnes tajemstvím. Jejím přínosem pro vědu však zůstává práce na počítačovém výzkumu, který měl šifru prolomit.

2.2.7 Enigma

Enigma je elektromechanický šifrovací přístroj fungující na substitučním systému. Jeho hlavní potenciál je v používání obvykle tří nebo čtyř šifrovacích rotorů, které uvnitř sebe skrývají spleť vodičů vedoucích zprava doleva. Otevřený text se zadává skrze klávesnici a šifrový se získá rozsvícením jedné z žárovek reprezentujících písmena výstupu přístroje. Stejným způsobem se i dešifruje.

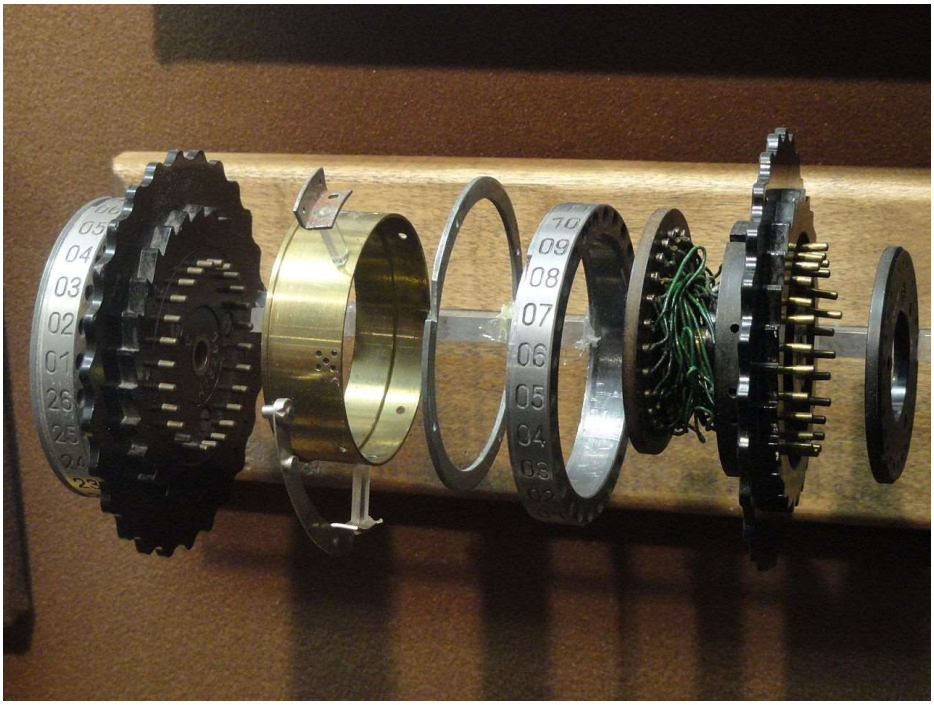
Obrázek 11: Šifrovací stroj Enigma M4 - Převzato z https://www.instructables.com/id/HackerBox-0027-Cypherpunk/



Obrázek 12: Schéma Enigmy M4

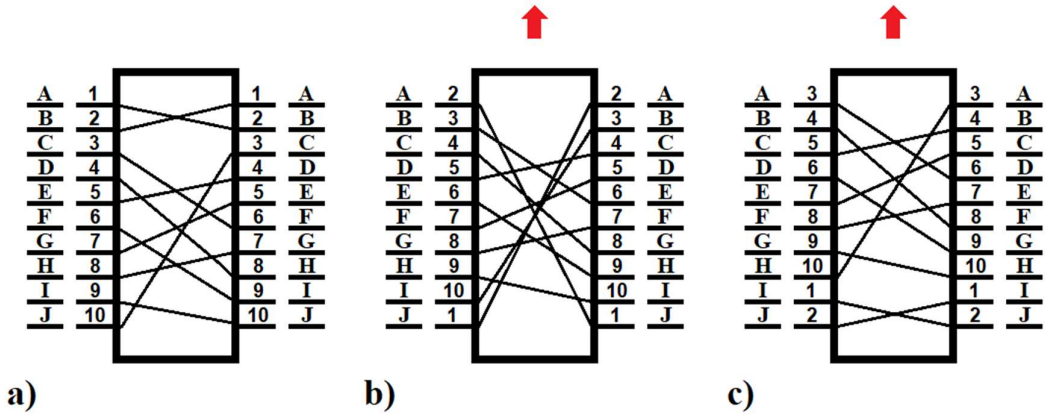
Při každém zmáčknutí klávesnice se 4. rotor pootočí o jednu pozici, čímž se kompletně změní trasa vodivě spojených vodičů, a tedy i elektrického proudu. Díky tomu lze mačkat stejnou klávesu, aniž by se na výstupu objevil znak, který zde byl před tím. Celý princip je patrný z obrázku 12, kde byla stisknuta klávesa „a“, která přepojila obvod ze záporného potenciálu na kladný. V tu chvíli se rotor č. 4 pootočí o jednu pozici a začíná obvodem protékat

elektrický proud, který prochází substitučními kontakty, vodiči, které vzájemně mezi sebou mohou prohazovat dvě písmena. Proud následně protéká 4., 3., 2., 1. rotorem a v reflektoru se v další spleti vodičů navrací nazpět, aby absolvoval cestu 1., 2., 3., 4. rotorem, substitučními kontakty a žárovkou s písmenem „D“, která se rozsvítí. Kdyby uživatel před tím místo klávesy „a“ zmáčkl „d“, stroj by mu odpověděl písmenem „A“. Tím je zaručen princip šifrování i dešifrování při stejném počátečním nastavení klíčů.



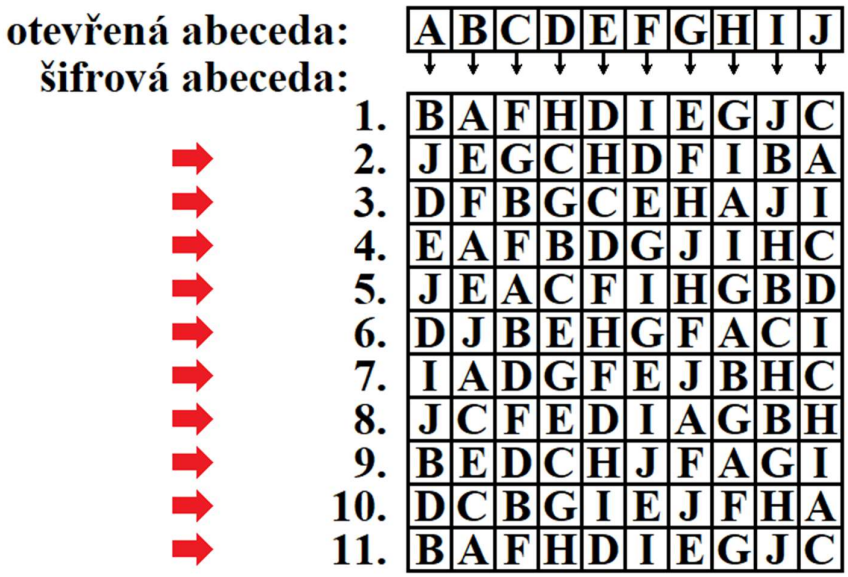
Obrázek 13: Vnitřek šifrovacího rotoru - Převzato z https://de.wikipedia.org/wiki/Enigma-Walzen

Na ukázku funkce rotoru si lze pro zjednodušení představit, že místo 26 kláves, žárovek a kontaktů jich obsahuje pouze 10. Takový rotor by mohl například vypadat stejně jako na obrázku 14.



Obrázek 14: Princip funkce rotoru a) rotor na první pozici, b) rotor na druhé pozici, c) rotor na třetí pozici

Kontakty rotorů byly zde očíslovány, aby bylo zřejmé, odkud kam vedou vodiče a jaký efekt na ně bude mít posunutí o jednu pozici. Na rozdíl od obrázku 12 se zde bude postupovat zleva doprava. V části a) lze konstatovat, že bude-li zadáno písmeno „a“, vstoupí signál do kontaktu č. 1 na levé straně rotoru a vystoupí z kontaktu č. 2 na pravé straně rotoru, kde se z něj na výstupu stává písmeno „B“. V případě pootočení rotoru o jednu pozici jsou posunuty kontakty o jedno číslo výše. V části b) tedy zadání písmena „a“ již vede na kontakt č. 2 a vystupuje na kontaktu č. 1, který v tento moment reprezentuje písmeno „J“. Stejným způsobem se postupuje i v části c). Vodiče tedy vždy vedou stejnou cestou ke stejně očíslovaným kontaktům ve všech případech pootočení. Pouze pozice mezi kontakty označenými písmeny a čísly se mění. Splnění tohoto principu tedy napovídá, že jde o polyalfabetickou šifru, která s každým pootočením přiřazuje k otevřené abecedě jinou šifrovou abecedu, než byla předchozí. Šifrové abecedy tohoto rotoru pro 10 písmen jsou znázorněny na obrázku 15.



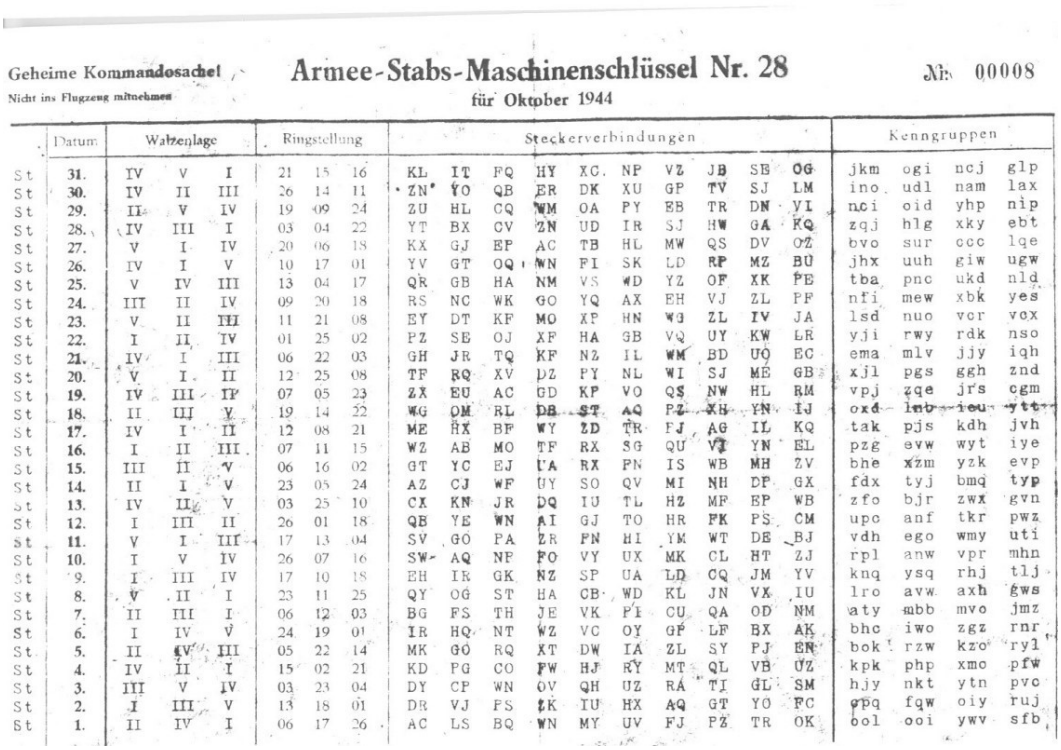
Obrázek 15: Šifrové abecedy uvedeného rotoru pro 10 písmen

Enigma obsahuje čtyři podobné vzájemně vodivě propojené šifrovací rotory. Ve chvíli, kdy rotor dosáhne svým pootočením určité pozice, jež je pro každý rotor odlišně a fixně nastavena výrobcem, dojde k pootočení i sousedního rotoru. To platí i pro zbývající rotory. Šifrové abecedy každého rotoru se tedy postupně střídají a opakují se po otočení o 26 pozic. Aby nedocházelo k opakování stejných tras, pootočením sousedního rotoru se změní i jeho šifrová abeceda. To lze ověřit tím, že uživatel bude zadávat na klávesnici stejné písmeno dvaapadesátkrát. Pokud se na výstupu objeví dvě identické za sebou jdoucí části šifrového textu, znamená to, že nastala chyba, kdy se sousední rotor přestal točit, nebo jeho návrh je nedokonalý. K tomu však u Enigmy nedochází.

Krom polyalfabetické šifry je použita i monoalfabetická, a to konkrétně v reflektoru, ale existují i druhy šifrovacích strojů Enigma, jenž používají rotující reflektor – polyalfabetickou šifru. Monoalfabetické šifrování probíhá i v substitučních kontaktech, též zvaných jako „propojovací panel“. Zde lze nastavením dvě písmena na vstupu i výstupu prohazovat mezi sebou.

Nastavení klíče spočívá ve výběru obvykle tří z pěti typů rotorů, u Enigmy M4 čtyř z osmi s tím, že první rotor se vybírá pouze ze dvou, jménem „Gamma“ a „Beta“. Originálním názvem tohoto procesu je „Walzenlage“. Každý typ rotoru má své pevně nastavené dráhy vodičů. Například typ I se kompletně liší od typu II. Další část klíče, tzv. „Grundstellung“, se nastaví správným pootočením rotoru na konkrétní hodnotu indexu. Tento index se podle druhu Enigmy

označoval písmeny nebo i čísly, a bylo možné tento index přenastavit. Takový malý trik jménem „Ringstellung“ však nebyl pro třetí stranu žádnou velkou překážkou. Posledním nastavením bylo správné zapojení propojovacího panelu (substitučních kontaktů) zvané „Steckerverbindungen“. Příklad klíče z října 1944 je uveden na obrázku 16.



Geheime Kommandosache!
Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28
für Oktober 1944

№ 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SB	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	VI	nci	oid	yhp	nip
St	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	KQ	zqj	hlg	xky	ebt
St	27.	V	I	IV	20	06	18	KX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	ccc	lqe
St	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	FI	SK	LD	RP	MZ	BU	jhx	uuh	giw	ugw
St	25.	V	IV	III	13	04	17	QR	GB	HA	NM	VS	WD	YZ	OF	XK	PE	tba	pnc	ukd	nld
St	24.	III	II	IV	09	20	18	RS	NC	WK	GO	YQ	AX	EH	VJ	ZL	PF	nfi	mew	xbk	yes
St	23.	V	II	III	11	21	08	EY	DT	KF	MO	XP	HN	WG	ZL	IV	JA	lsd	nuo	vor	vox
St	22.	I	II	IV	01	25	02	PZ	SE	OJ	XF	HA	GB	VQ	UY	KW	LR	yji	rwy	rdk	nso
St	21.	IV	I	III	06	22	03	GH	JR	TQ	KF	NZ	IL	WM	BD	UQ	EC	ema	mlv	jjy	iqh
St	20.	V	I	II	12	25	08	TF	RQ	XV	DZ	PY	NL	WI	SJ	ME	GB	xjl	pgs	ggh	znd
St	19.	IV	III	II	07	05	23	ZX	EU	AC	GD	KP	VO	QS	NW	HL	BM	vpj	zqe	jrs	cgm
St	18.	II	III	V	19	14	22	WG	OM	RL	DB	ST	AQ	PZ	XH	YN	IJ	oxd	lnb	icu	ytt
St	17.	IV	I	II	12	08	21	ME	HX	BF	WY	ZD	TR	FJ	AG	IL	KQ	tak	pjs	kdh	jvh
St	16.	I	II	III	07	11	15	WZ	AB	MO	TF	RX	SG	QU	VJ	YN	EL	pzg	evw	wyt	iye
St	15.	III	II	V	06	16	02	GT	YC	EJ	UA	RX	PN	IS	WB	MH	ZV	bhe	xzm	yzk	evp
St	14.	II	I	V	23	05	24	AZ	CJ	WF	UY	SO	QV	MI	NH	DP	GX	fdx	tyj	bmq	typ
St	13.	IV	II	V	03	25	10	CX	KN	JR	DQ	IU	TL	HZ	MF	EP	WB	zfo	bjr	zwx	gvn
St	12.	I	III	II	26	01	18	QB	YE	WN	AI	GJ	TO	HR	FK	PS	CM	upo	anf	tkr	pwz
St	11.	V	I	III	17	13	04	SV	GO	PA	ZR	FN	HI	YM	WT	DE	BJ	vdh	ego	wmy	uti
St	10.	I	V	IV	26	07	16	SW	AQ	NP	FO	VY	UX	MK	CL	HT	ZJ	rpl	anw	vpr	mhn
St	9.	I	III	IV	17	10	18	EH	IR	GK	NZ	SP	UA	LD	CQ	JM	YV	knq	ysq	rhj	tlj
St	8.	V	II	I	23	11	25	QY	OG	ST	HA	CB	WD	KL	JN	VX	IU	lro	avw	axh	gws
St	7.	II	III	I	06	12	03	BG	FS	TH	JE	VK	PI	CU	QA	OD	NM	aty	mbb	mvo	jmz
St	6.	I	IV	V	24	19	01	IR	HQ	NT	WZ	VC	OY	GP	LF	BX	AK	bhc	iwo	zgz	rnr
St	5.	II	IV	III	05	22	14	MK	GO	RQ	XT	DW	IA	ZL	SY	PJ	EN	bok	rzw	kzo	ryl
St	4.	IV	II	I	15	02	21	KD	PG	CO	FW	HJ	RY	MT	QL	VB	UZ	kpk	php	xmo	pfw
St	3.	III	V	IV	03	23	04	DY	CP	WN	OV	QH	UZ	RA	TI	GL	SM	hjy	nkt	ytn	pvo
St	2.	I	III	V	13	18	01	DR	VJ	PS	LK	IU	HX	AQ	GT	YO	FC	qpq	fqw	oiy	ruj
St	1.	II	IV	I	06	17	26	AC	LS	BQ	WN	MY	UV	FJ	PZ	TR	OK	ool	ooi	ywv	sfb

Obrázek 16: Šifrovací tabulky k armádní Enigmě z října - Převzato z http://users.telenet.be/d.rijmenants/en/enigmaproc.htm

S dostupnými informacemi lze spočítat počet možných nastavení klíče, které se liší podle použitého druhu Enigmy. Podle klíče na obrázku 16 lze použít vzorec 1.

$$r * (r-1) * (r-2) * p * p * p * \frac{p!}{(p-2*v)! * v! * 2^v} \tag{1}$$

kde,

r… počet typů rotorů

p… počet písmen otevřené (a šifrové) abecedy

v… počet použitelných vodičů propojovacího panelu.

Celkový výsledek je 158 962 555 826 360 000 možných kombinací nastavení. V případě, že by uživatel chtěl vyměnit i reflektor nebo použil námořní Enigmu se čtyřmi rotory, celý počet kombinací by se mohl zdvojnásobit i ztrojnásobit nebo v případě Enigmy používané Abwehrem zšestadvacetinásobit díky pozičně nastavitelnému reflektoru.

Dlouho před koncem první světové války si německý elektroinženýr Arthur Scherbius uvědomil, že v éře mechanizované války je stará metoda šifrování tajných zpráv pomocí tužky a papíru beznadějně zastaralá. [3]Nejprve nabízel Enigmu s deseti rotory, ale kvůli nepříznivé situaci a naivitě armády i vlády, která věřila v bezpečnost svých zastaralých šifrovacích metod, se objevil zájem až ve dvacátých letech poté, co se mocnosti Trojdohody chvástaly, s jakou lehkostí během války četly zašifrované zprávy svého nepřítele. Německá armáda začala nakupovat šifrovací stroje, avšak trvala na několika úpravách. Jednou z nich bylo zavedení propojovacího panelu. Později se připojilo i německé námořnictvo, které však trvalo na používání čtyř rotorů namísto tří. V roce 1935 Hitler roztrhal Versailleskou smlouvu a spustil masivní expanzi německých ozbrojených sil. Brzy po strojích Enigma vypukla obrovská poptávka ve všech odvětvích armády, a to i v bezpečnostních složkách. [3] Vzniklo několik různých druhů Enigem, které šifrovaly text s naprosto odlišným výsledkem. Zašifrované zprávy byly běžně posílány přes radiové vysílání. To byla skvělá příležitost pro okolní státy zprávy zachytit, avšak aniž by je dokázaly rozluštit. Němci spoléhali na obrovský počet kombinací a každodenní změnu šifrovacích klíčů. Kdyby se třetí strana rozhodla dešifrovat zprávy hrubou metodou zkoušením všech kombinací jedné po druhé, zabralo by jí to tolik času, že by informace již ztratila svou hodnotu nehledě na to, že zpočátku netušila ani, s jakým algoritmem má tu čest. Důvěra Němců v neprolomitelnost Enigmy se však ukázala osudovou chybou.

Hans-Thilo Schmidt, zaměstnanec šifrovacího oddělení německého ministerstva obrany a bratr vysoce postaveného důstojníka Rudolfa Schmidta, se hnán touhou po penězích rozhodl roku 1931 nabídnout informace o Enigmě některé z Evropských zemí. Francie, znepokojena nárůstem vlivu nacistů, se zdála vhodnou volbou. Došlo k setkání a předání kompletní dokumentace Enigmy Francouzům. Ač šlo o velmi cennou informaci, samotná ke každodennímu prolamování nestačila, ale byl to skutečný počátek velké bitvy mezi kryptografy a kryptoanalytiky. Z důvodu nedostatku francouzských kryptoanalytiků bylo nutné najít jinou zemi, která by byla ochotna a připravena s takovou výzvou pomoci. Polsko, země v soukolí dvou agresivních mocností, se právoplatně cítilo ohroženo a nabídku přijalo. Tento nelehký úkol připadl do rukou Mariana Rejewskeho.

Obrázek 17: Marian Rejewski – Převzato z zdroj https://www.nsa.gov/About-Us/Current-Leadership/Article-View/Article/1621548/marian-rejewski/

Ten podrobil Enigmu matematické analýze a hledal v šifrovém textu údaje o opakujícím se klíči původně zapsaném do otevřeného textu. Z těchto informací dokázal vyloučit některé kombinace klíčů. S každou další zprávou se mu hromadily informace, dokud nebyl schopen přiřadit otevřeným abecedám šifrové abecedy. Z nich byly údaje svisle uspořádány do řetězců. Tím, že se dostal k řešení zabývajícím se rotory, mohl zanedbat vliv propojovacího panelu, a tedy i počet všech možných kombinací s ním souvisejících. Tím velmi klesl počet prohledávaných kombinací na hodnotu 105 456, které nakonec kryptoanalytici museli vyzkoušet na replice Enigmy a vytvořit katalog vztahů z řetězců. Když byl klíč rotorů nalezen a na Enigmě nastaven, přišel čas na propojovací panel. Bez zapojení vodičů do panelu byl do kláves vkládán šifrový text, který sice nebyl moc čitelný, ale byly na něm obvykle patrné "obrysy" slov. Podle písmen, která do těchto slov moc nepasovala, se dalo předpokládat, že mají být propojena vodiči. Pak byl klíč kompletní. Rejewski si velmi zjednodušil úkol nalézt denní klíč tím, že oddělil problém nastavení scramblerů (rotorů) od problému nastavení propojovací desky (panelu). [2] Později Rejewski vytvořil dešifrovací stroj, jménem „Bomba", zkoušející všechna možná nastavení klíčů. Šlo o neuvěřitelný úspěch.

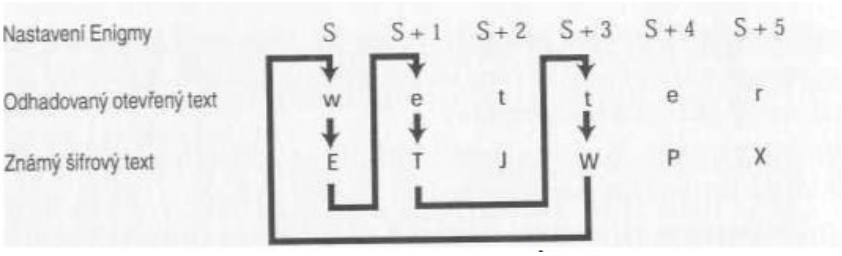
S blížící se válkou se Němci rozhodli zdokonalit zabezpečení svých šifer tím, že zvýšili počet typů rotorů ze tří na pět. To znamenalo desetinásobný počet kombinací vložení rotor, a tedy desetinásobný čas pro hledání klíče, který se dal snížit pouze výrobou dalších Bomb. K tomu byl zvýšen počet vodičů pro propojovací panel z šesti na deset. Najít obrysy slov již bylo mnohem těžší a jejich špion Schmidt přerušil kontakt. Rejewski s takovým stupněm ochrany už nedokázal držet krok. Ještě stihl v srpnu 1939 svým britským a francouzským

kolegům nabídnout plány Bomb a repliky Enigem, kteří tento dar s velkým překvapením přijali. Stalo se to jen několik dní před napadením Polska Německem.

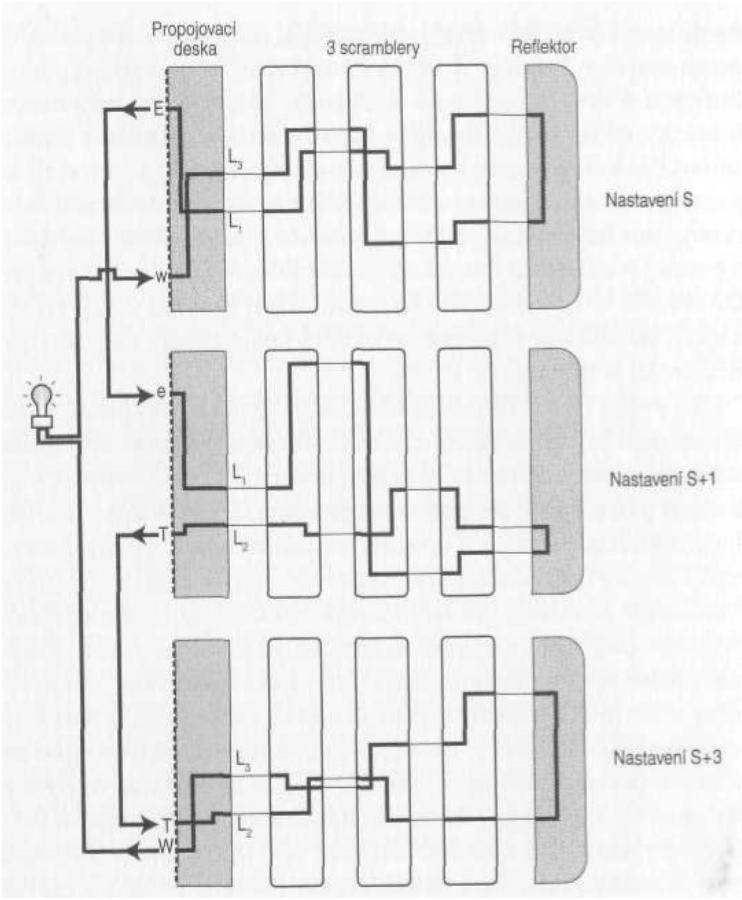
Tyto nové informace přinutily Brity a Francouze přehodnotit pohled na jejich kryptoanalytický přístup. V Anglii v Bletchley Parku začalo vznikat sídlo MI6 a Vládní telekomunikační ústředí s cílem, mimo jiné, zachytávat nepřátelské zprávy a luštit je. Díky velkému množství specializovaných zaměstnanců a cenných údajů od Poláků se jim to pomalu začalo dařit. Následovaly pokusy najít zprávy s klíči, které se při každém vysílání opakovaly. Krom toho dne neměnného klíče, daném šifrovacími tabulkami, si dle předpisů měl operátor Enigmy zvolit i klíč vlastní, který by se při každém vysílání opakoval. Údaj o klíči byl následně zašifrován podle šifrovacích tabulek a vložen na začátek zprávy. Zbytek zprávy byl zašifrován i klíčem operátora. Pohodlnost a spěch operátorů však vedl k ignorování předpisů, a tedy k nevědomému poskytnutí cenného vodítka třetí straně. Operátoři volili klíče, které se daly snadno zapamatovat nebo představovaly nějaké slovo, ke kterému měli osobní vztah. Britští kryptoanalytici tedy zkoušeli používat tyto opakující se klíče, a to jim začalo přinášet kýžený úspěch. Další chybou Němců byla jejich snaha ještě více zabezpečit klíče tím, že do šifrovacích tabulek vybírali pořadí rotorů tak, aby se určitý typ rotoru na konkrétním místě se nemohl na témže místě objevit po další dva dny. Myšlenkou bylo zaručení, aby se klíče neopakovaly a zabránit tím dlouhodobému dešifrování v případě získání klíče. Následkem ale bylo, že kryptoanalytikové mohli velmi výrazně vyřadit množství možných klíčů. Jiným vodítkem bylo pravidlo, že na propojovacím panelu se některá písmena nesměla propojit s jinými konkrétními. Tím se opět daly vyřadit některé kombinace.

Obrázek 18: Alan Turing - Převzato z https://www.nsa.gov/About-Us/Current-Leadership/Article-View/Article/1621551/alan-turing/

S pokrokovou myšlenkou přišel Alan Turing, geniální matematik pozvaný do Bletchley Parku. Ten si povšiml, že některá slova se v otevřeném textu opakují a některá bývají i na stejných místech zprávy. Například každý den po šesté hodině ranní rozesílali Němci zprávu obsahující předpověď počasí na daný den. To znamenalo, že zcela jistě na počátku zprávy bylo německé slovo „wetter – počasí. V případě, že lze takto propojit část šifrového textu s otevřeným bez klíče, jde o tzv. „tahák“. Turing využil postupu Rejevského a řešil rotory a propojovací panel zvlášť s pomocí řetězců obsahujících smyčky – viz Obrázek 19.



Obrázek 19: Cyklus řetězce [2]



Obrázek 20: Hledání cyklu [2]

Nakonec přišel na metodu, která procházela každou možnou pozici rotorů, dokud nedošlo k nalezení cyklu. To ale bylo možné jen v případě, že byl každý z rotorů na správném místě. Proto bylo nutné vyrobit více dešifrovacích strojů konajících toto hledání s rozdílně seřazenými rotory. Těchto možností seřazení bylo u Enigmy M3 celkem 60. Na obrázku 20 jsou tři Enigmy, jež hledají cyklus. Druhá Enigma s nastavením S+1 má na rozdíl od první levý rotor pootočený o jednu pozici, aby výstup první Enigmy mohl být okamžitě připojen. To samé následuje pro

třetí Enigmu s nastavením s+3, tedy pootočené o dvě pozice napřed oproti druhé. Pokud je celý cyklus z obrázku 19 nalezen, žárovka se rozsvítí. Pokud ne, je třeba vybrat jinou kombinaci typů rotorů. Následně přichází na řadu propojovací deska. Pokud kryptoanalytik na výstupu Enigmy získá otevřený text, který není oním odhadovaným slovem, avšak obsahuje zpřeházená písmena, která by v něm měla být obsažena, provede zapojením vodičů substituci mezi těmito písmeny. Z tohoto konceptu Turing dal roku 1940 vyrobit svou vlastní Bombu, avšak tento prototyp pojmenoval „Victory" a nedosahoval takových rychlostí, jak se od něj očekávalo. Najít klíč trvalo i týden. Za takovou dobu drtivá většina šifrovaných zpráv už ztratila svou hodnotu. Bylo navrženo pár modifikací. V srpnu 1940 konečně dorazil poupravený stroj jménem „Agnes" a kýžený výsledek na sebe nenechal dlouho čekat. Obvykle stroj získal klíč během jedné hodiny. K vyhledání byl především určen jeden z taháků, ale občas se stávalo, že kryptoanalytik netušil, kde konkrétně v textu se nachází. Musel využít další slabiny Enigmy, kterou byl fakt, že písmeno otevřeného textu se nemohlo ve stejném pořadí objevit v šifrovém textu. Respektive písmeno nelze zašifrovat tak, aby se stalo samo sebou. Pokud uživatel zmáčkne klávesu „a", nikdy se nerozsvítí žárovka „A". Proto se obvykle odhadovaný šifrový text napsal na papír a posouval se horizontálně pod šifrovým textem. Pokud jedno z písmen odhadovaného otevřeného textu bylo na stejné pozici jako písmeno šifrového textu, bylo jasné, že na tomto místě se nenachází. Jakmile bylo nalezeno místo, kde se všechna písmena ve vertikálním směru liší, mohlo být zahájeno vyhledávání Bombou.

Zatímco Britové sklízeli plody své práce dešifrováním většiny německé komunikace, trnem v jejich oku zůstávalo stále německé námořnictvo – „Kriegsmarine". To používalo sofistikovanější Enigmu M4 se čtyřmi vloženými rotory z osmi celkových. Proto se muselo zorganizovat několik přepadů německých lodí a ponorek pro odcizení šifrovacích tabulek a Enigem. Spojenci si museli počínat opatrně, protože jakýkoliv náznak, že jim do rukou padly seznamy s několikaměsíčními platnými klíči, by vedl k velké změně způsobu šifrování a kryptoanalytici z Bletchley Parku by museli začít opět od nuly. Proto byla zahájena klamavá hra s cílem uchlácholit Němce, že je jejich komunikace zcela v bezpečí. I když Britové získali informace o záměrech a pozicích nepřítele, nemohli je plně využít. Místo toho na základě výpočtů pravděpodobností museli zvážit, co vše si mohou dovolit, aniž by nepřítel pojal podezření. V případě, že německé ponorky vysílačkou nahlásily velitelství své pozice, museli Britové nejdříve poslat k onu místu své průzkumné letadlo, aby měli záminku, jakým náhodným způsobem se jim podařilo nepřítele lokalizovat. Až pak mohli vyslat torpédoborce, ať ponorky zničí. S postupem času se začala celá válka nejen o Atlantik pro Němce ve zlé obracet.

2.3 Moderní šifrování

Postupem času se z kryptologie stala především matematická záležitost z důvodu nastolení počítačového věku. Rychlost a logika strojů mohly využít složitých početních operací, které by člověku zabraly příliš mnoho času, a eliminovaly chyby způsobené lidským faktorem.

2.3.1 DES

Data Encryption Standard byl jeden z prvních algoritmů používající symetrické blokové šifrování, který na rozdíl od proudového pracoval s textem jako s bloky o stejné délce, kdežto proudové šifrování probíhá znak po znaku. DES používal klíč o délce 64 bitů, z toho bylo 8 bitů kontrolních a 56 bitů efektivních.

Rozšířenou verzí bylo 3DES, též zvané jako TDES. Výhodou byla trojnásobná délka klíče 168 bitů.

Tento standard byl později prolomen a nastal čas se poohlédnout po bezpečnějším standardu.

2.3.2 IDEA

International Data Encryption Algorithm je blokový šifrovací algoritmus, který měl být alternativou pro DES. Používá bloky o velikosti 64 bitů a klíč o délce 128 bitů. Jeho nevýhodou byla existence slabých klíčů, ale protože jich nebylo mnoho, nepřikládala se jim větší pozornost.

2.3.3 AES

Advanced Encryption Standard je další symetrický blokový šifrovací algoritmus, který se nakonec stal nástupcem DESu. Velikost jeho bloků je 128 bitů a klíč dosahuje délek 128, 192 nebo 256 bitů. Šifra AES údajně nebyla ještě žádným elegantním způsobem prolomena.

2.3.4 RSA

V roce 1976 pánové Whitfield Diffie a Martin Hellman uvedli na svět kryptografii s veřejnými klíči, jednalo se o zlomový bod v kryptografii. [4] Název algoritmu je odvozen od iniciála autorů Rivesta, Shamira a Adlemana. Výhodou nesymetrické kryptografie byla délka klíčů, avšak šifrování bylo pomalejší. V praxi nejvyužívanější a nejvýhodnější způsob použití spočívá v kombinaci obou principů (symetrická/asymetrická kryptografie). Na data se použije rychlá

symetrická šifra a na přenos symetrického klíče se použije asymetrická šifra za pomoci privátních/veřejných klíčů. [4] Používaná délka klíče bývá 1024 bitů, avšak začíná se přecházet i na 2048 bitů.

3 PRAKTICKÁ ČÁST

3.1 Šifrovací program

Základní myšlenka programu vychází z algoritmu šifrovacího stroje Enigma. Cílem bylo princip zdokonalit i lépe ochránit proti opětovnému prolomení. Algoritmus byl realizován v jazyce C# ve vývojovém prostředí Microsoft Visual Studio 2017.

Jednou z inovací je zvýšení počtu použitelných znaků abeced z 26 na 60. Tím rapidně stoupá počet možných klíčů a výsledků. Další výhodou, ale i Achillovou patou, je komfort uživatele, který již má tu možnost používat i čísla, symboly, tečky, čárky a především mezerník. Nebezpečí spočívá v tom, obsahuje-li otevřený text tyto znaky, dostává kryptoanalytik spoustu užitečných taháků, které může využít při vyhledávání slov ukrytých v otevřeném textu. Například různé spojky ohraničené mezerníky nebo tři číslice vedle sebe, které téměř jistě budou mít nějaký význam podle velmi nízké pravděpodobnosti tak hojného výskytu vedle sebe. V dnešní době má již spoustu možností vytvořit rychlý program, který vyzkouší všechna možná nastavení klíčů, dokud hledané výrazy nenalezne.

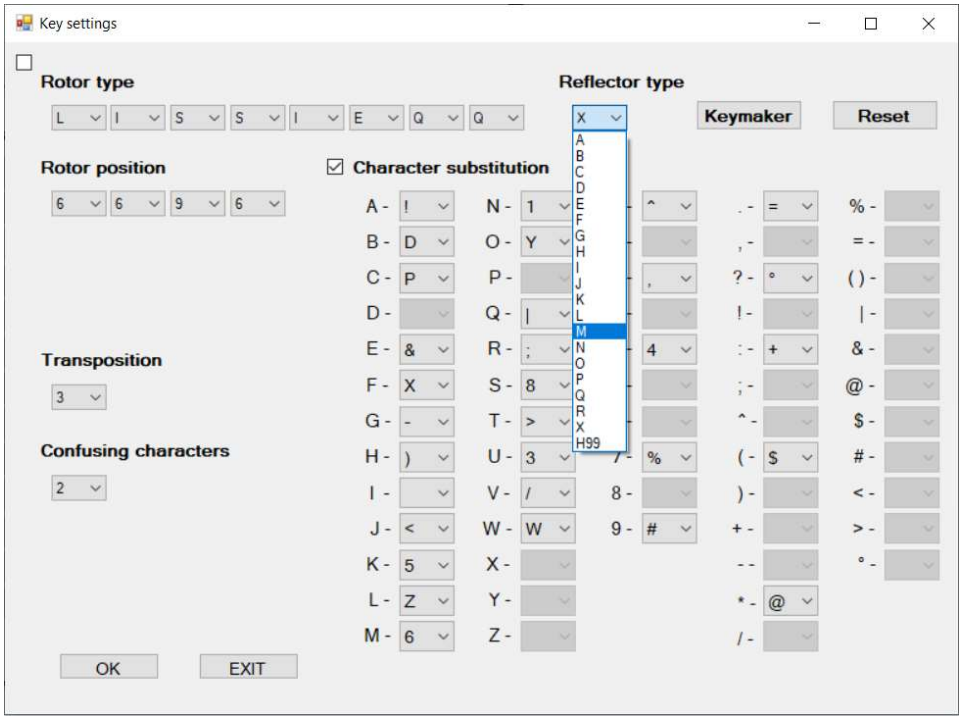
3.1.1 Obsluha programu

Program na některých místech může být těžký na pochopení, a proto by uživatel měl dbát těchto pokynů.

Nejprve je po spuštění programu prvním oknem dotázán na výběr ze tří jazyků.

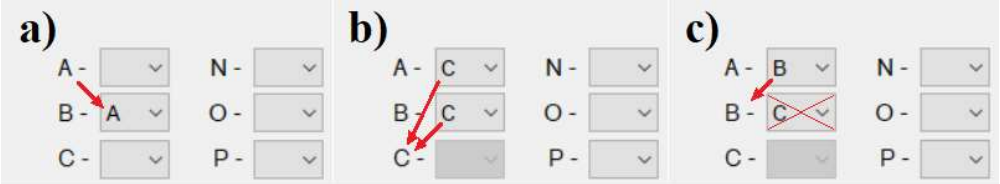
Následuje druhé okno, kde je potřeba si zvolit, zda se jedná o šifrování nebo dešifrování. Tato volba bude mít vliv na některé texty labelů a na proces šifrování či dešifrování, ale pouze v případě, že při volbě klíče byla vybrána možnost použití transpozice a klamače. Dále je zde možnost nastavit si, která použitá data budou uložena do textových souborů.

Třetí okno je nejdůležitějším a možná i nejtěžším, co se manipulace týče, viz obrázek 21.



Obrázek 21: Nastavení klíče

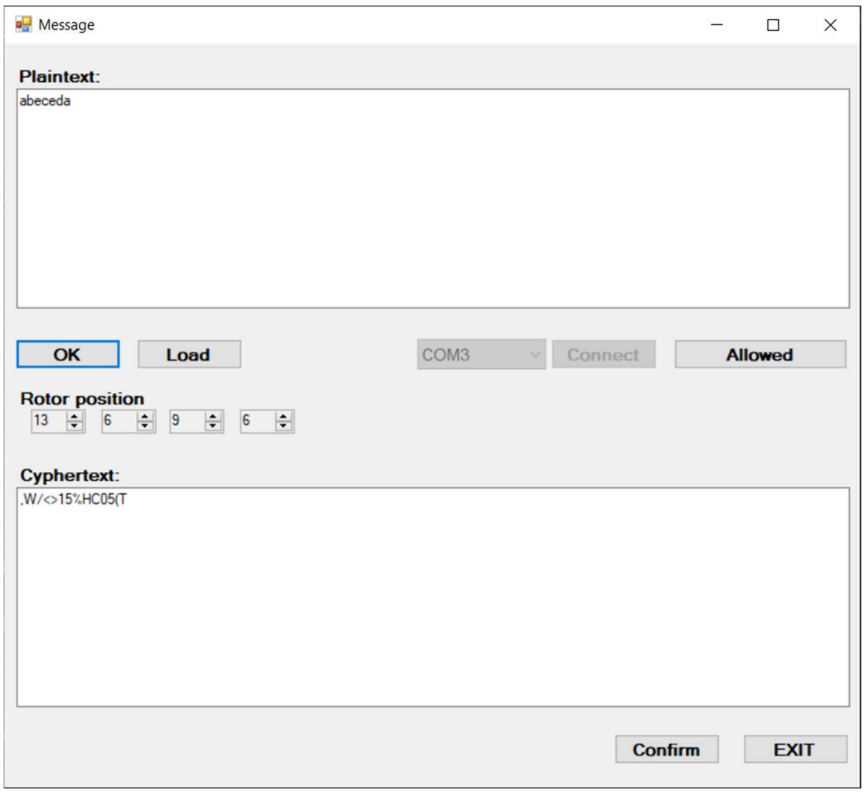
Nejprve je potřeba si vysvětlit, nač se zde nachází dva checkboxy. Levý checkbox má vliv na nastavení rotorů, reflektoru, pozic rotorů, volbu transpozice a klamače. Prostřední naopak může ovlivnit monoalfabetickou substituční šifru. V moment, kdy je stisknuto tlačítko s nápisem „Keymaker“, začne se generovat klíč těch částí, jejichž checkbox byl zaškrtnut. To znamená, že zadané hodnoty budou ztraceny a nahrazeny jinými náhodnými. Dalším tlačítkem, majícím vliv, je „Reset“. Stisknutí vede také ke ztrátě zadaných hodnot, ale i k nastavení původních továrních hodnot. Význam checkboxů tedy spočívá v tom, že když uživatel bude chtít anulovat své původní rozhodnutí, nemusí nutně vše ručně přenastavit nebo měnit celý klíč. Nastavení monoalfabetické substituce může být poměrně obtížné a nedostatečně ošetřené. Uživatel by měl nastavovat jeden combobox po druhém. V případě nedodržení pravidel by mohl špatně nastavit klíč substituce, čímž by riskoval zakázané stavy – viz obrázek 22. Nikdy by nemělo dojít k tomu, že k labelu o určitém znaku bude comboboxem přiřazen znak jemu pozičně nadřazený. Například lze ke znaku „A“ přiřadit „B“, avšak nelze k „B“ přiřadit „A“, viz část a). Ani by nemělo docházet k situaci, kdy dva comboboxy přiřadí dvěma různým labelům jednu identickou hodnotu, viz část b). Případ přiřazení znaku comboboxem k již zadanému labelu také nelze tolerovat, viz část c).



Obrázek 22: Zakázané stavy

Pokud je pro uživatele nastavení příliš složité, měl by dát přednost generátoru klíčů a nový klíč si uložit.

Ve čtvrtém okně se již nachází textová pole pro zadání otevřeného a šifrového textu, viz obrázek 23.



Obrázek 23: Okno pro otevřený text, šifrový text a vysílání zpráv

Zadáním textu do vrchního pole a stisknutím tlačítka „OK“ lze text ihned zašifrovat/dešifrovat. Tlačítko „Load“ slouží k načtení již předpřipravenému textu ze souboru „message.txt“. V případě, že hodlá uživatel použít komunikační modul, musí modul přes USB připojit a opět spustit program. Pak vybere jednu z možností v comboboxu a klikne na tlačítko „Connect“. Po tomto stisknutí musí uživatel počítat s tím, že může od druhé nebo i třetí strany obdržet zprávu, která se zobrazí ve vrchním textovém poli. Tento šifrovací program byl vytvořen pro konečný

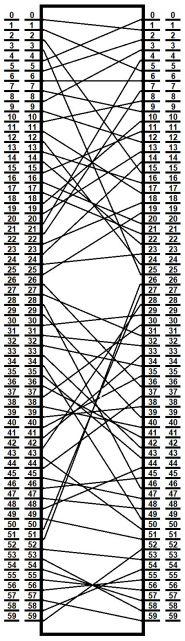
počet znaků. Proto by se měl uživatel seznámit s tlačítkem „Allowed characters“. Pokud chce odeslat přes modul zprávu, která se nachází v dolním textovém poli, musí kliknout na tlačítko „Confirm“. Ve čtvrtém okně jsou obsažena i čtyři numericUpDown okna, která umožňují opětovné přenastavení pozic šifrovacích rotorů.

3.1.2 Použité šifrování

Monoalfabetická šifra použitá propojovací deskou (substitučními kontakty) Enigmy se používá i zde. Jediným rozdílem je skutečnost, že používá místo 26 písmen 60 znaků a umožňuje propojit až 30 znakových párů. Enigma směla propojit pouze 10 párů, zatímco 3 páry zůstaly netknuté. Tímto se zde počet možných kombinací velmi zvyšuje, viz rovnice 2.

$$\frac{p!}{(p-2*v)!*v!*2^v} = \frac{60!}{(60-2*30)!*30!*2^{30}} = 29*10^{39} \quad (2)$$

Polyalfabetická šifra realizovaná rotory zde funguje také v principu stejně jako u německé Enigmy.



Obrázek 24: Rotor typu „A“

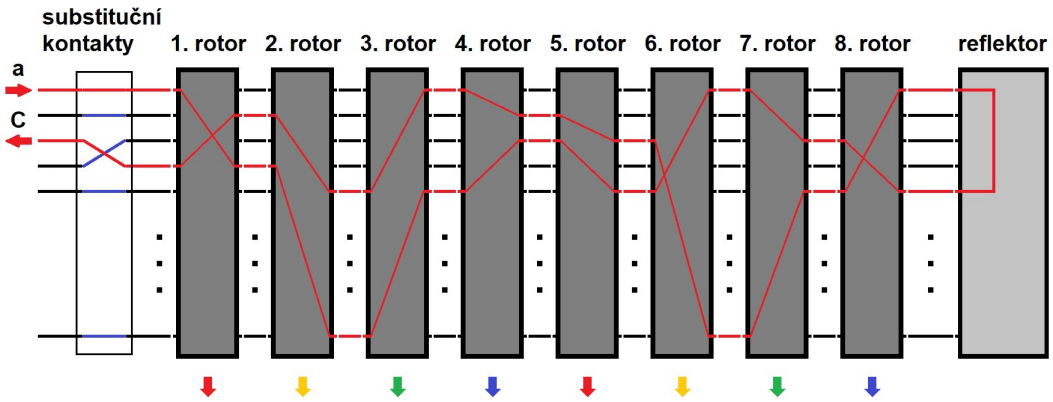
Rotor na obrázku 24 lze popsat částmi zdrojového kódu 1 použitého v programu, kde je možné vidět souvislost mezi čísly konstant rotorů a indexy kontaktů.

```
case "A":
     rotorConstants = new int[] { 4, 0, 5, 8, 20, 1, 6, 21, 10, 7, 18, 15,
         9, 19, 23, 2, 13, 11, 22, 25, 16, 17, 14, 24, 12, 3, 51, 50, 42, 30,
         37, 27, 31, 41, 32, 40, 26, 44, 39, 29, 38, 36, 33, 35, 48, 46, 28,
         45, 47, 34, 43, 49, 59, 52, 58, 56, 55, 54, 53, 57 };
     break;

case "A":
     rotorConstants = new int[] { 1, 5, 15, 25, 0, 2, 6, 9, 3, 12, 8, 17, 24,
         16, 22, 11, 20, 21, 10, 13, 4, 7, 18, 14, 23, 19, 36, 31, 46, 39,
         29, 32, 34, 42, 49, 43, 41, 30, 40, 38, 35, 33, 28, 50, 37, 47, 45,
         48, 44, 51, 27, 26, 53, 58, 57, 56, 55, 59, 54, 52 };
     break;

static int[] ROTOR(int[] array1, int k, int[] constants)
{
     int a = 0, b = 0;
     const int N = 60;

     int[] array2 = new int[N];

     for (int i = 0; i < N; i++)
     {
         a = k + i; b = k + constants[i];
         if (a > (N - 1)) { a = a - N; }
         if (b > (N - 1)) { b = b - N; }
         array2[a] = array1[b];
     }
     return array2;
}
```

Zde je k dispozici 19 typů rotorů s 60 pozicemi, z nichž se jich 8 vloží do programu, a 19 reflektorů, plus jeden testovací jménem „H99“. Reflektoru „H99“ by se měl uživatel vyvarovat, pokud mu záleží na soukromí, protože naprosto vyruší veškeré šifrování fungující na stejném principu jako Enigma. I jeden rotor je testovací a to konkrétně „H“. Jeho označení písmenem naprosto vystihuje schéma propojení vodičů, jelikož u rotoru typu „H“ jsou všechny vodiče vodorovně propojeny se svým protějším kontaktem. Takové rotory fungují tedy tak, jako by vůbec nebyly přítomny a šifrovací program by místo osmi používal nižší počet rotorů. Celkový počet možných nastavení rotorů je znázorněn na rovnici 3.

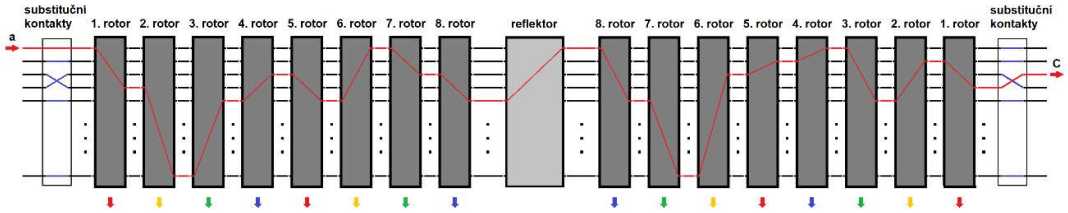
$$r^8 * p^4 = 19^8 * 60^4 = 22 * 10^{16} \quad (3)$$

S rotory tentokráte počítáme tak, jako by se ty samé typy mohly vícekrát objevit v jednom a tom samém nastavení. Když se výsledky rovnice 2 a 3 vynásobí mezi sebou, dostáváme číslo $64*10^{56}$. To už je velmi vysoké číslo, avšak i to lze ještě zvýšit, když vezmeme v úvahu oněch 19 vyměnitelných typů reflektorů a vynásobíme. Konečným výsledkem pro tento vylepšený systém je $12*10^{58}$ možných nastavení. Celý systém vylepšené Enigmy je na obrázku 25.



Obrázek 25: Principiální schéma Enigmy použité v programu

Toto schéma díky programové realizaci bylo možné překreslit i podrobněji pro pochopení funkce, viz obrázek 26.

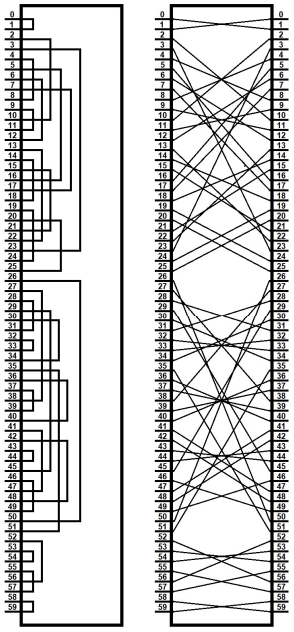


Obrázek 26: Podrobnější principiální schéma Enigmy použité v programu

Na obrázku 24 a 25 lze vidět 8 použitých rotorů. Jejich četnost otáčení je naznačena barevnými šipkami. Například rotory č. 1 a 5 se otáčejí současně s každým právě šifrovaným/dešifrovaným znakem. Používaly i stejný index nastavení pozic rotoru. Rotory č. 2 a 6 (označené oranžovou šipkou) se pootočily, až když 1. (i 5.) rotor překonal index o hodnotě 60. Postupně stejný systém fungoval i pro rotory č. 3 a 7, a následně 4 a 8.

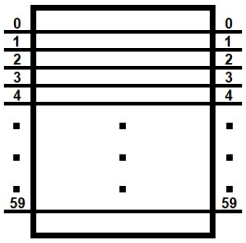
Enigma měla jednu velkou nevýhodou a tou byl fakt, že písmeno se po zašifrování nemohlo nikdy stát samo sebou. Kryptoanalytik mohl díky tomu odhadovat, na kterém místě šifrového textu se může ukrývat konkrétní hledaný tahák. Pokud si ale Enigmu představíme jako systém rozkreslený na obrázku 25, nikoliv jako elektrický obvod na obrázku 24, pak je realizace již možná. V elektromechanickém stroji se tento problém ukrýval v jeho reflektoru. Elektrický proud protékající rotory a otáčející se v reflektoru nemohl téci rozpojenými vodiči až do reflektoru, kde by se odrazil a tekl sám proti sobě zase zpět, aby rozsvítil žárovku. Aby se mohlo písmeno stát samo sebou, potřebovalo zcela odlišné vstupy a výstupy, tedy dvoje klávesnice a dvoje sady žárovek. Taková fyzická realizace je však poměrně komplikovaná, a tak je mnohem

snazší ji vytvořit programem. Překreslený reflektor typu „A“ pak může vypadat jako na obrázku 27.



Obrázek 27: Původní a překreslený reflektor typu „A“

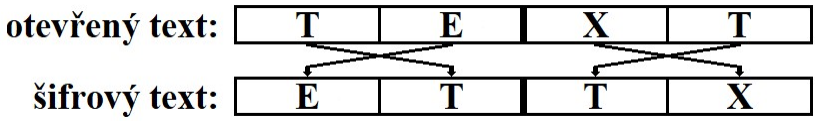
Nyní je zřetelné, že lze vytvořit i reflektor, jehož vodič by vedl z levého kontaktu o určitém indexu na pravý kontakt o stejném indexu. Jako příklad lze uvést již zmíněný reflektor typu „H99“, viz obrázek 28.



Obrázek 28: Zkráceně překreslený reflektor typu "H99"

S použitím takového reflektoru dojde po příchodu signálu k absolvování stejné trasy ven, ale s tím rozdílem, že ona trasa je zrcadlově obrácena. Jakýkoliv znak je zadán, takový se vrátí i zpět. To je ale velmi nepraktický krok, protože pak by skoro veškeré šifrování bylo zbytečné a vysílán by byl často pouze otevřený text. Proto program obsahuje několik reflektorů, jež na několika málo místech využívají přímého spojení kontaktů se stejným indexem.

Transpoziční šifra je zde použita před i po Enigmě dle volby uživatele. Znaky textu jsou uvnitř dvojic zaměněny mezi sebou, viz obrázek 29.

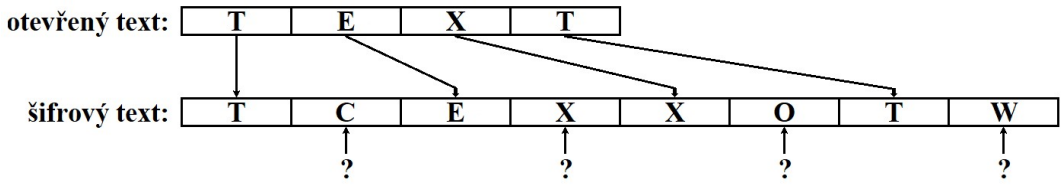


Obrázek 29: Jednoduchá transpoziční šifra

Ač taková jednoduchá transpozice sama o sobě není moc účinná, v kombinaci s Enigmou může třetí straně značně zamotat hlavu. Znaky ve dvojicích mohou být prohozeny na začátku celého šifrování programu, na jeho konci nebo v obou případech. I když to zpočátku vypadá, že provést dvakrát transpozici se stejným postupem povede k vzájemnému vyrušení obou procesů, opak je pravdou. Je potřeba si uvědomit, že při transpozici se mění pozice pro každý znak, tím pádem ho rotory zpracují o jednu svou pozici dříve nebo později, čímž je zašifrován na znak úplně jiný, než měl původně být. Kód je uveden na

```
static string Transposition(int textLength, char[] textArray)
{
     string text = null; ;
     char[] auxiliaryTextArray = new char[textLength];
     int i;
     for (i = 0; i < textLength; i++)
     {
          auxiliaryTextArray[i] = textArray[i];
     }

     for (i = 0; i < textLength; i++)
     {
          if (i < textLength - 1)
               { textArray[i + 1] = auxiliaryTextArray[i]; }
          if ((textLength % 2 != 0) && (i == textLength - 1))
               {textArray[i] = auxiliaryTextArray[i]; }
          else{textArray[i] = auxiliaryTextArray[i + 1];
          i++;
          }
          text = String.Concat(textArray);
          return text;
     }
```

Klamač (matoucí znak) se také vyskytuje před a po Enigmě. Jeho přínosem je změna délky textu, lehká transpozice znaků a ochrana proti vyhledávání taháků. Jeho algoritmus je patrný z obrázku 30.



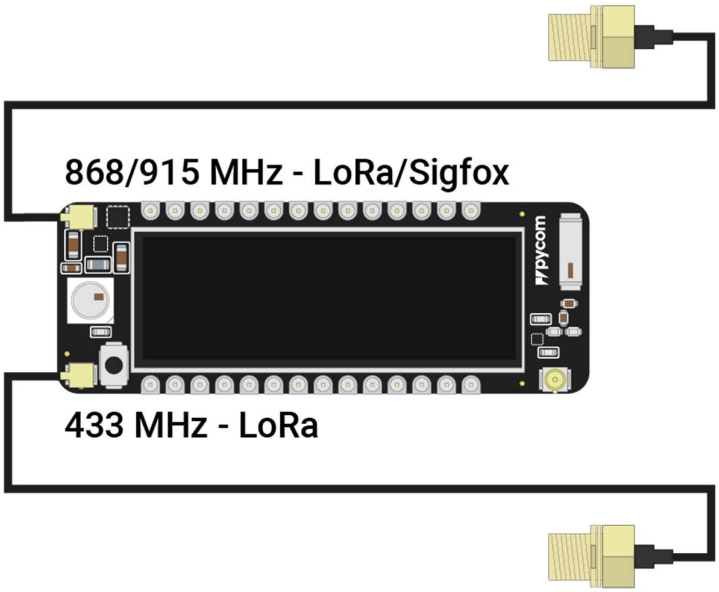
Obrázek 30: Přidání klamače do textu

U klamače není důležité, jakým znakem se prezentuje. Pouze vyplňuje místo a pokouší se splynout s ostatními znaky. Proto k jeho vytvoření postačí generátor náhodných čísel, jenž vytváří index použitelných znaků, podle nějž se přiřadí jeden z nich.

```
static string ConfusingCharacters(string text, char[] textArray)
{
     int j = 0;
     Random r = new Random();
     foreach (char character in text)
     {
          textArray[j] = character;
          j++;
          textArray[j] = char.Parse(usedCharacters[r.Next(0, N)]);
          j++;
     }
     text = String.Concat(textArray);

     return text;
}
```

3.2 Komunikační modul

Jako komunikační modul byl použit model „LoPy4“ technologie LoRa. Je to kvalitní vývojové prostředí podporující jazyk MicroPython, využívající pásem 433 MHz, 868/915 MHz a wifi, viz obrázek 31. V tomto případě bylo vybráno pásmo 868 MHz s vyšším povoleným vyzářeným výkonem 25 mW. Pásmo 915 se používá v Severní Americe.



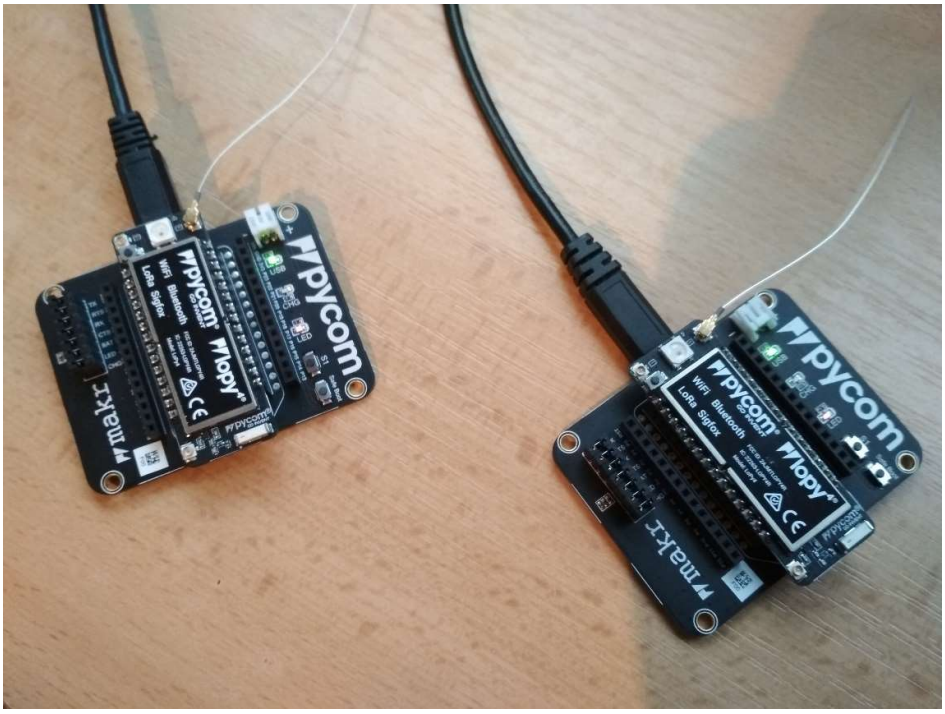
Obrázek 31: Modul LoRa – Převzato z

https://docs.pycom.io/gettingstarted/connection/lopy4.html#second

Jeho programovatelnost je poměrně snadná, viz zdrojový kód 4

```
# main.py -- put your code here!
from network import LoRa
from machine import UART
import socket
import machine
import time

#funkce na poslani (lze volat pres intepret pres seriovou konzoli)
def posli(str):
    s.setblocking(True)
    s.send(str)
    return


#funkce pro prijem (lze volat pres intepret pres seriovou konzoli)
def prijmi():
        s.setblocking(False)
        data = s.recv(64)
        print(data)
        return

# initializace LoRa in LORA mode
lora = LoRa(mode=LoRa.LORA, region=LoRa.EU868)
data=" "
#otevreni LoRa soketu
s = socket.socket(socket.AF_LORA, socket.SOCK_RAW)
```

Na obrázku č. 32 jsou zobrazeny komunikační moduly.



Obrázek 32: Komunikační moduly

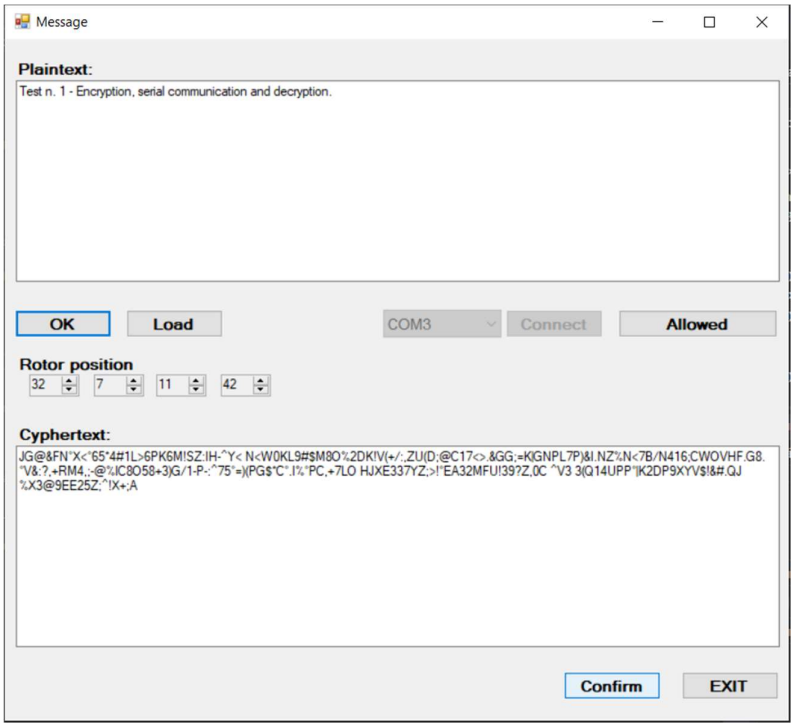
3.3 Test přenosu

3.3.1 Test funkčnosti

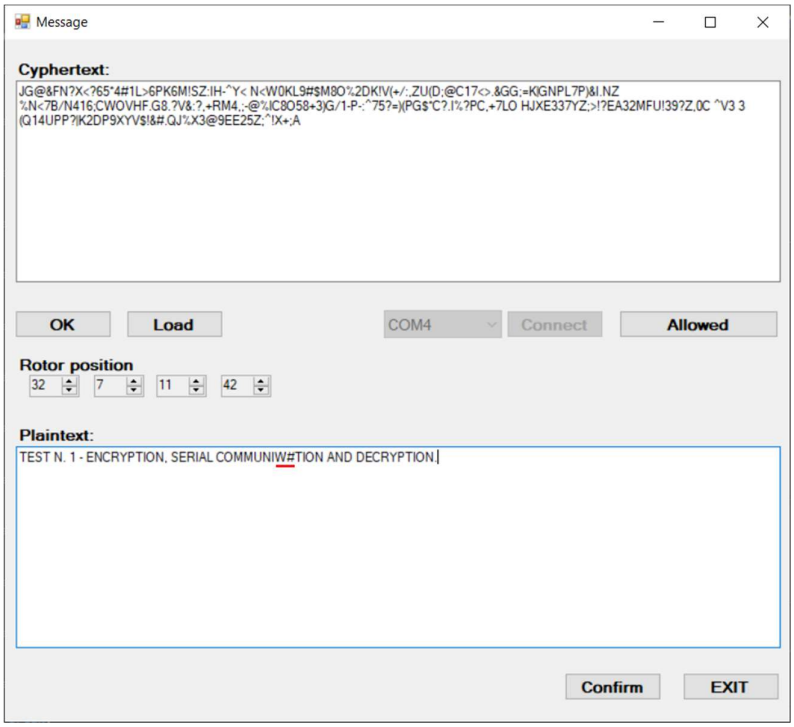
Test byl proveden pro ověření funkčnosti obou modulů a části programu, která umožňuje propojení dat šifrovacího programu s komunikačním modulem.

První test byl uskutečněn v městské zástavbě na vzdálenost jednoho metru s úspěšným výsledkem, kdy krátké odeslané i přijaté otevřené texty byly identické.

Pro druhý test byl již zvolen dlouhý šifrový text, který se až na dva znaky přenesl správně, viz obrázek 34.



Obrázek 33: Otevřený a šifrový text na straně odesílatele



Obrázek 34: Šifrový a otevřený text na straně příjemce

Nejdříve se vyskytlo podezření, že došlo k rušení jiným zařízením, avšak fakt, že byly zkresleny rušením pouze dva znaky, ukazoval na jiný problém. Při bližším ohledání a porovnání šifrových textů byla objevena drobná nedokonalost modulu. Znak „°“ je při odeslání změněn na „?“. Modul se zřejmě takto „vypořádává“ se všemi jemu neznámými znaky.

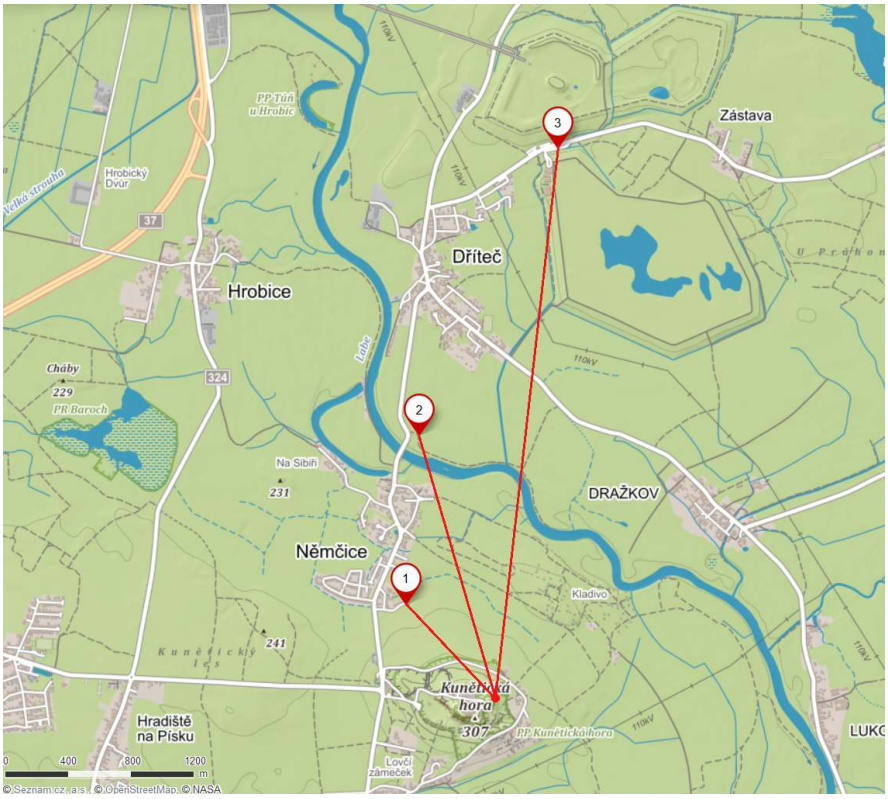
3.3.2 Test přenosu na delší vzdálenost

Cílem testu bylo prověřit, zda je komunikační modul opravdu schopen dosáhnout vzdáleností v řádech jednotek kilometrů, aniž by obsah zprávy byl výrazně narušen. Proto byl jako vhodný testovací terén zvolen vyvýšený bod mimo městskou zástavbu. Ideálním takovým prostředím se jevila Kunětická hora s nadmořskou výškou 307 m. Městská zástavba pro bezdrátovou komunikaci s přímou viditelností je na delší vzdálenosti nepoužitelná. Pro optimální příjem a vysílání byla 9 cm dlouhá prutová anténa namířena na východ.

První test vyznačený na obrázku 35 bodem č. 1 byl uskutečněn na vzdálenost 800 m. Příjem i vysílání zprávy proběhlo bez problémů.

Druhý test označený bodem č. 2 byl provedený na vzdálenost 1,7 km a bezchybně proveden.

Třetí test označený bodem č. 3 byl proveden na vzdálenost 3,5 km a opět úspěšně realizován.



Obrázek 35: Mapa testovaných dosahů spojení

ZÁVĚR

Cílem této práce bylo navrhnutí šifrovacího programu propojeného s komunikačním modulem. Tento program s pomocí odesílatele zprávy měl dle konkrétního klíče obsah zašifrovat a odeslat vysílačem směrem k přijímači, kde byl příjemce připravený k dešifrování zprávy identickým klíčem.

V teoretické části byla nejprve rozebrána dostupná frekvenční pásma s jejich omezeními týkajícími se vyzářeného výkonu, aplikace použití a zacházení. K některým pásmům byl přidán i teoretický dosah signálu. Dále byly popsány jednoduché metody šifrování textu, které byly rozebrány z hlediska jejich bezpečnosti a možnému počtu nastavitelných klíčů. U každé šifry bylo uvedeno i její historické pozadí, které i skrývalo příběh o vývoji kryptoanalýzy. Byly zde uvedeny i čtyři moderní šifrovací algoritmy.

V praktické části byl předveden návod pro užívání programu se zvláštním zřetelem na správné zadání klíčů pro monoalfabetickou substituci spolu s příklady zakázaných stavů. Dále zde byl uveden princip fungování programu s rozborem pozitiv a negativ v případě typu kryptoanalýzy již úspěšně použité k prolomení Enigmy. Na konec praktické části byl zařazen test funkčnosti a dosahu signálu modulu pro ověření bezchybného přenosu na krátkou vzdálenost a potvrzení předpokladu schopnosti překonat vzdálenosti v řádech jednotek kilometrů.

Praktickou část provázely problémy spojené s mými neprofesionálními znalostmi programování, což mělo za následek příliš zdlouhavý kód, který se rozprostíral na 26 000 řádcích a před spuštěním programu 70 sekund načítal. Po nějaké době byl však kód razantně zkrácen v důsledku nově nabytých znalostí o programování v jazyce C#. Druhou obtížnou překážkou byly dlouho neúspěšné snahy o ošetření proti zadávání nežádoucích hodnot při nastavování šifrové abecedy monoalfabetické šifry do programu. Nakonec k ošetření došlo, ale za cenu velké ztráty času. Poslední a největší překážkou se stal problém opakující se u vícera počítačů, který odmítal aktualizaci ovladačů nutných pro navázání spojení komunikačního modulu s počítačem. Bez spojení nebylo možné otestovat funkčnost modulu a dosah signálu, což si opět vyžádalo vysokou daň v podobě ztraceného času. Nakonec se podařilo tento problém vyřešit a otestovat moduly na kratší (10 m) i delší vzdálenost (3,7 km) se zcela úspěšným přenosem. S větší anténou by byl dosah jistě větší. Šifrovací program byl několikrát odzkoušen při šifrování i následném dešifrování a vždy svou úlohu úspěšně splnil.

4 POUŽITÁ LITERATURA

[1] *Český telekomunikační úřad* [online]. Praha: ČTÚ, 2018 [cit. 2019-05-01]. Dostupné z: https://www.ctu.cz/

[2] SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii*. 1. vyd. v českém jazyce. Praha: Dokořán, 2003. Aliter (Argo: Dokořán). ISBN 80-86569-18-7.

[3] CIMINO, Al. *Příběh kryptologie: od starověkých šifer po kvantovou kryptografii*. 1. Přeložil Marek ČTRNÁCT. Praha: Dobrovský s.r.o., 2018. Knihy Omega. ISBN 978-80-7390-887-4.

[4] OULEHLA, Milan a Roman JAŠEK. *Moderní kryptografie*. 1. Praha: IFP Publishing, 2017. ISBN 978-80-87383-67-4.