Klasická kryptologie

Classic cryptology

Dagmar Zábojníková

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Dagmar ZÁBOJNÍKOVÁ**
Osobní číslo:	**A07116**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Téma práce:	**Klasická kryptologie**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Vypracujte studii o klasické (konvenční) kryptologii – zahrňte co nejvíce příkladů a ukázek klasických šifrovacích systémů, jejich vzájemné porovnání, včetně ukázek možností prolomení šifer.**
3. **Vytvořte prezentace obsahující popis problematiky, matematický popis a analýzu a grafické ukázky.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **SINGH, Simon. Kniha kódů a šifer.Argo, 2003. ISBN: 80-7203-499-5.**
2. **JANEČEK, J. Odhalená tajemství šifrovacích klíčů minulosti. Naše Vojsko, 1994.**
3. **VONDRUŠKA , P. Kryptologie, šifrování a tajná písma. Albatros, 2006. ISBN 80-00-01888-8.**
4. **HANŽL, T. Šifry a hry s nimi. Portál, 2007. ISBN 978-80-7367-196-9.**
5. **KATZ, Jonathan. Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall, 1 edition. 2007. 552 s. ISBN 978-1584885511.**
6. **MURPHY, Sean. Kryptografie - Průvodce pro každého . Dokořán, 2006. 157 s. ISBN 80-7363-074-5.**

Vedoucí bakalářské práce: **Ing. Roman Šenkeřík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **5. března 2010**

Termín odevzdání bakalářské práce: **1. června 2010**

Ve Zlíně dne 5. března 2010

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Klasická kryptologie je vědní obor zabývající se šifrováním a dešifrováním. Cílem práce bylo uvedení do problematiky klasické kryptologie. Od historie, která je velmi bohatá, po vysvětlení, rozdělení základních šifer a kódů, až ke steganografii a tajemství dešifrování. Z velkého množství šifer a kódů bylo vybráno to nejdůležitější, zároveň nejzajímavější a věnováno tomu dostatečná pozornost. Následně byla vytvořena prezentace obsahující popis této problematiky, matematický popis a analýzu a grafické ukázky.

Klíčová slova: kryptologie, kódování, substituční šifry, transpoziční šifry, steganografie, kryptoanalýza.

ABSTRACT

Typical cryptology is the scientific discipline based on coding and cryptanalysis. The target of my piece of work is to clarify the problems of this issue. I mention not only the rich history, the explanation, the separation of basic secret codes and ciphers but also steganography and the secret of cryptanalysis. Due to paying attention to this topic I selected the most important and the most interesting secret codes from the whole range. Subsequently, I created the prezentation including the description of this problems, mathematical characterization and graphical illustration.

Keywords: cryptology, coding, substitution cipher, transposition cipher, steganography, cryptanalysis.

Chtěla bych poděkovat panu Ing. Romanu Šenkeříkovi, Ph.D. za zadání velmi zajímavého tématu a za odborné vedení mé bakalářské práce. Zároveň mé poděkování patří i rodině hlavě mamince, sestře, babičce a taťkovi dále příteli a kamarádům za veškerou podporu během psaní bakalářské práce a během studia.

Démokritos z Abdér :

Vzdělání má hořké kořeny, ale sladké ovoce.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Klasická kryptologie je velice zajímavý vědní obor, který pro lidi má dosud nádech tajemství. Lze ji taky označit jako vědu o utajeném obsahu zpráv. Rozděluje se na kryptografii, kryptoanalýzu a v neposlední řadě na steganografii. Má velký vliv na lidskou historii. Provází jí snad od samého začátku.

23. září 480 př. n. l. v Řecku, kdy perské a sparťanské lodě se střetávají v boji u zátoky. Peršané v domnění, že Sparťany překvapí, pronásledují řecké lodě až do zálivu. Řekové si uvědomují, že mají menší, a ohebnější lodě a proto mají v zátoce velkou výhodu. Tím pádem se z perského vítězství stává hořká porážka. Otázkou zůstává, jak se Sparťané dozvěděli o útoku? Odpověď je velmi jednoduchá. Řek ve vyhnanství v Persii poslal zprávu vydlabanou na spodku tabulky, která byla poté zalita voskem, aby vypadala jako prázdná a neporušená vosková tabulka. Nebo také 15. října 1586 v Anglii, kde skotská královna Marie Stuartovna doplatila životem na rozluštění šifrových zpráv, které posílala svým spojencům v době, kdy byla držena ve vězení. A tak by se dalo pokračovat snad do nekonečna.

Šifry teda mají velké použití. Člověk měl vždy nějaká svá tajemství, která bylo potřeba chránit, ať už tajemství ohně, později tajemství oceli či potřeba utajení informací typu "kdy a jak se vrhnout na protivníka". Taky jsou důležité v politice, obchodě či milostném životě. Většinou šlo o různé transpoziční (přehození znaků) či substituční (náhrady znaků) změny ve zprávě tak, aby nebylo poznat, co je jejím obsahem. A pokud náš partner není tak blízko, abychom mu mohli tajemství pošeptat, je šifrování tím nejlepším způsobem, jak zprávu utajit.

V momentě kdy šifrovaná zpráva přijde do rukou někomu jinému, tedy nesprávné osobě, pak přichází na řadu lidská zvědavost, která je stará jak lidstvo samo a člověk pociťuje velmi silné nutkání vědět, co se nachází v utajené zprávě. Tedy na řadu přichází motivace. Je vskutku jedno, zda se jedná o politické spiknutí nebo spiknutí dvou spolužáku proti třetímu, ale vždycky je tu pravidlo při utajování zpráv, které říká, že když chceme něco utajit, tak hlavně zajímavým způsobem.

Pojem šifry jsou taky chápány jako výzvy. Je to výzva pro autora šifry, který musí vymyslet co nejtěžší šifrový systém. Měl by se dát snadno a rychle používat a zároveň pro třetí stranu

se musí stát nerozluštitelnou. Pro luštitele to znamená přijít na zdánlivě nesmyslnou zprávu. Je to vlastně takový druh adrenalinu, který mnoho lidí fascinuje.

TEORETICKÁ ČÁST

1 ZÁKLADY KRYPTOLOGIE

1.1 Základní rozdělení věd

Tato podkapitola uvádí základní rozdělení vědního oboru kryptologie. Její rozdíly a definice.

1.1.1 Kryptologie

Můžeme zjednodušeně označit jako vědu o utajení obsahu zpráv. Kryptologie se dělí na kryptografii a kryptoanalýzu a steganografii.

1.1.2 Kryptografie

Slovo kryptografie pochází z řeckých slov kryptós - skrytý a gráphein – psát. Zabývá se matematickými metodami se vztahem k takovým prvkům informační bezpečnosti, jako je zajištění důvěrnosti zpráv, integrity dat (neporušenosti), autentizace entit (ověření subjektu) a původu dat, včetně zkoumání jejich silných stránek a slabin i odolnosti vůči různým metodám útoků.

Dříve tato věda popisovala, jak navrhovat a používat šifrovací systémy, tedy byla to disciplína, která se zabývala převedením informace do podoby, v níž je tato informace skryta. Tedy úkolem bylo učinit výslednou zprávu nečitelnou i v situacích, kdy je úplně prozrazena.

Kryptografové jsou ti, kteří se zabývají návrhem, používáním a zkoumáním šifrovacích systémů a dalších aspektů informační bezpečnosti.

Kryptografie se po staletí vyvíjela, aby poskytla ochranu pro důležité informace, zejména utajení strategických vojenských informací, ale také politických intrik, příprav atentátů nebo vztahu milenců atd.

Spartští generálové používali první zaznamenaný šifrovací systém - Scytale.

Základní pravidla kryptografie:

- Stejným klíčem by neměly být nikdy zašifrovány dva různé texty
- Dbát na dostatečnou délku klíče

- Klíč by měl být co nejméně „uhodnutelný”
- Pokud používáme více klíčů, ze znalosti jednoho by nemělo být možno odvodit další klíče
- Kryptologický systém by měl být jednoduchý a přehledný, aby zbytečně neodradil uživatele
- Pokud je to možné kombinujeme se steganografickou technikou - kde není viditelná zpráva, není podezření a zvědavost
- Snaha o co největší kompresi dat - čím delší zpráva tím více materiálu pro kryptoanalýzu

1.1.3 Kryptoanalýza

Lze vyjádřit jako opak ke kryptografii. Tedy jedním z hlavních cílů je studium metod luštění šifrovacích systémů. Obecněji můžeme kryptoanalýzu definovat jako analýzu odolnosti kryptografických systémů.

Lidé zabývající se kryptoanalýzou jsou kryptoanalytici a jejich cílem je získat ze zašifrované zprávy její původní podobu nazývanou jako otevřený text. Avšak cílem může být získání jen části utajené informace.

Kryptoanalytické techniky:

- Metoda pokus - omyl
- U klasických šifer frekvenční analýza (rozhodnutí zda se jedná o substituci či transpozici - v případě substituce vede k rozluštění)
- Luštění transpozic v tabulce - postupné přeskupování bloků (sloupce atd.) v tabulce a vyhledávání bigramů a trigramů (častých pro konkrétní jazyk)
- Luštění polyalfabetických šifer - algoritmus založen na výskytu stejných dvojic a klíče
- Slovníková metoda hledání klíče
- Brute force attack - útok hrubou silou, zkoušení všech kombinací klíče

1.1.4 Steganografie

Slovo steganografie pochází z řeckého steganós - schovaný a gráphein - psát. Steganografie je věda zabývající se utajením komunikace, ukrýváním zpráv a zatajováním probíhající komunikace.

Do oblasti steganografie patří například takzvané neviditelné inkousty nebo modernější mikrotečky. Pomocí steganografie dosáhneme jistého stupně utajení, ale když se ukrytou zprávu podaří odhalit, je celý její obsah prozrazen - pouhé odhalení ukryté zprávy prozradí celý její obsah. Aby nedošlo k prozrazení obsahu zprávy, zpravidla se steganografické postupy kombinují s kryptografií. To znamená, že ukrytá zpráva je navíc ještě zašifrována šifrovacím klíčem, pomocí šifrovacího systému, který přeskupí nebo jinak zašifruje znaky ve větě podle předem dohodnutého hesla nebo jinak.

První známý případ použití steganografie byl zaznamenán v 5. století před naším letopočtem. Jednalo se o zprávu, která pomohla Řekům v dnes již legendárním boji proti Peršanům[1]. Demaratus[2], zjistil, že král Xerxes[3] plánuje vojenský výpad proti Řekům. Zprávu s popisem jeho plánu a času předpokládaného vylodění na řeckém pobřeží zaslal svým krajanům. Nemohl však zprávu poslat otevřeně, a proto se ji pokusil ukrýt - seškrábal vosk ze dvou voskových psacích destiček, umístěných v dřevěných formách, a přímo dovnitř dřevěné formy zprávu vyryl, následně formu opět zalil voskem a zprávu tak vhodně překryl. Když se zpráva dostala do Řecka, manželka krále Leonida[4], královna Gorgo, odhalila tajemství voskových destiček, ukrývajících důležitou zprávu o invazi.

Tajné zprávy se podle záznamů ukrývaly například v žebráckých berlách, dutých holích, částech oděvu, v dámských doplňcích, keramice či jinde.

---

[1] Peršani - jsou iránští lidi, kteří mluví perským jazykem a sdílejí obyčejnou kulturu a historii.

[2] Demaratus – byl sparťanský král od 519 do 491 př.n.l.

[3] Xerxes - byl perský král z rodu Achaimenovců vládnoucí v letech 486–465 př. n. l.

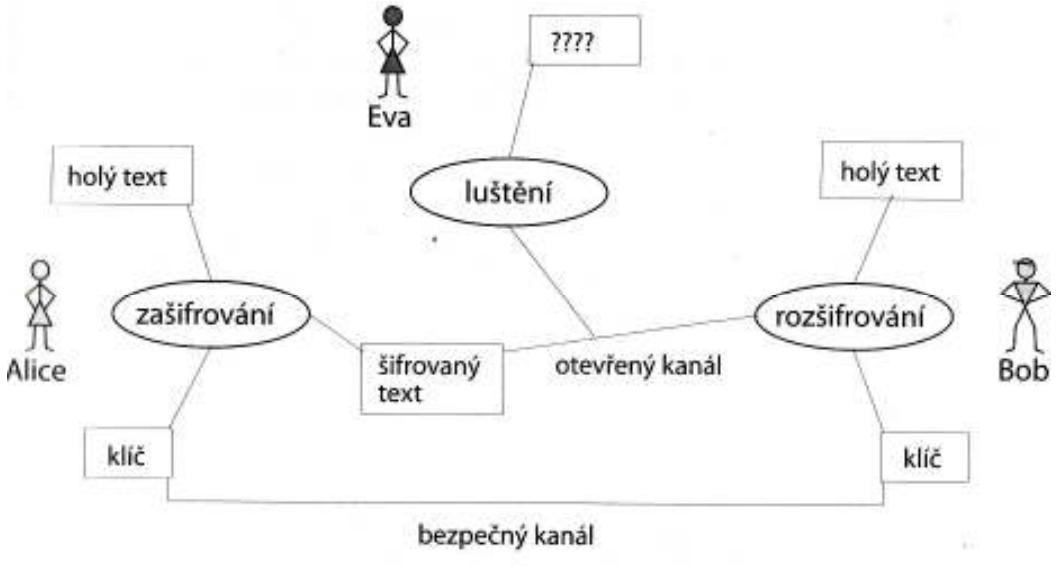
[4] Leonid - byl spartský král z dynastie Ágidovců, jenž panoval v období mezi léty 489 až 480 př. n. l.

Také jsou známy speciální steganografické pomůcky, kterými jsou neviditelný inkoust z mléčné šťávy pampelišky nebo citrónové šťávy, který se po zahřátí zviditelní, nebo inkousty ze složitějších syntetických sloučenin, viditelných jen pod speciálním světelným zdrojem nebo po styku s jinou chemikálií.

Krátké zprávy se také úspěšně ukrývaly pod poštovní známky nebo do darovaných předmětů. Kam až sahá lidská představivost a jak nebezpečné by bylo, kdyby byla zpráva odhalena, tak důmyslné postupy obohacovaly historii steganografie.

1.2 Základní pojmy

- Základní situace je znázorněna na obrázku. Dvě strany si přejí spolu soukromě komunikovat, tedy Alice a Bob. Jejich komunikaci však odposlouchává třetí strana, tedy Eva. Text zprávy, kterou si chce Alice s Bobem vyměnit, nazýváme *holý text*. *Šifrovaný text* je zpráva, která putuje po komunikačním médiu a kterou vidí Eva. *Klíč* je tajná informace, kterou si Alice a Bob dopředu vyměnili prostřednictvím bezpečnostního kanálu, tedy tak, že tento klíč nemůže Eva zjistit. Bezpečným kanálem je například osobní setkání, které se událo v minulosti a při kterém se Alice a Bob domluvili na klíči pro budoucí komunikaci.



Obr. 1. Základní situace komunikace pomocí šifer

- Šifrovací nebo kryptografický systém - je jakýkoliv systém, který lze použít ke změně textu nějaké zprávy s cílem učinit ji nesrozumitelnou komukoliv jinému s výjimkou adresáta.
- Šifrování / Zašifrování - pokud použijeme na zpracování nějaké zprávy šifrovací systém, říkáme, že zprávu *šifrujeme* nebo že jsme ji *zašifrovali*.
- Šifrový text - zašifrované zprávě říkáme *šifrový text* nebo také *šifrová zpráva*
- Otevřený text – je původní text zprávy, ještě před tím než byl zašifrován.
- Abeceda otevřeného textu / znak otevřeného textu - rozumíme jakékoliv písmeno, číslici, interpunkční znaménko atd.
- Šifrovací abeceda - je tvořeny abecedou otevřeného textu, ale mohou byt tvořeny i jinými obrazci. Od poloviny 19. století je zvykem zapisovat šifrové znaky do skupin po pěti šifrových znacích - zvyk souvisí s předáváním šifrových zpráv pomocí telegramů.
- Klamač - znak šifrové abecedy, který nemá žádný významový ekvivalent v otevřené abecedě a při dešifrování otevřeného textu se vynechává. Vkládají se pro zvýšení bezpečnosti.
- Šifry / Kódy - Pomocí šifry nebo přesněji šifrovacího systému se odesílatel a adresát snaží utajit obsah zprávy před nepovolenou osobou. Smyslem kódu, ale není zprávu utajit, ale upravit ji tak, aby ji bylo možné dále příslušným technickým prostředkem zpracovávat (přenos kanálem). Mezi nejznámější příklady kódu patří Braillovo písmo a Morseova abeceda.

Braillovo písmo funguje na principu plastických bodů vyražených do papíru, které čtenář vnímá hmatem. Morseova abeceda zas využívá tři symboly (tečku, čárku a mezeru) a původně byla určena pro přenos přes telegraf. Kdokoliv tedy dokáže na základě informace, že jde o Braillovo písmo nebo Morseovu abecedu převést text zpět do původní podoby.

- Klíč – hodnoty šifrového systému, které lze měnit a které mají vliv na výsledný šifrový text.
- Klíčové hospodářství - je domluva na používání klíčů, jejich distribuci, výběru, způsobu znehodnocení atd.

- Symetrické šifrové systémy - pokud je klíč pro šifrování a dešifrování stejný, pak systém je nazýván *symetrický šifrový systém* a pro klíč se používá označení *symetrický tajný klíč*.
- Asymetrické šifrové systémy - založen na tom, že jeden klíč - *veřejný klíč* slouží k zašifrování otevřeného textu a druhý klíč - *soukromý klíč*, slouží k dešifrování textu.
- Frekvenční analýza - Výpočet četnosti jednotlivých znaků ve zprávě. Frekvenční analýza je základem mnoha kryptoanalytických metod. Je účinná díky tomu, ze přirozené jazyky mají charakteristické frekvence písmen.
- Dešifrování - je opačný proces k šifrování. Jedná se rekonstrukci původního otevřeného textu zprávy z šifrového textu pomocí domluvené kryptografické metody a znalosti příslušného klíče. Dešifrování provádí zpravidla příjemce zprávy, ale může se stát, že i neoprávněná osoba, která se dostala k příslušnému klíči použitého šifrového systému.
- Luštění - kryptoanalytici se snaží získat ze zašifrované zprávy její původní podobu, tedy otevřený text. Cílem však může být i získání alespoň části skrytých informacích. Pokud je kryptoanalytik úspěšný a podaří se mu vniknout do některého šifrového systému pak tuto šifru *zlomil*.

Rozdíl mezi dešifrováním a luštěním je takový, že dešifrování provádí ten, kdo zná všechny potřebné informace k převodu šifrového textu na otevřený tvar, zatím co luštění provádí kryptoanalytik (nezamýšlený příjemce), který se snaží získat informace ze zašifrované zprávy bez znalosti klíče i šifrového systému.

Fáze luštěni:

- Identifikace - odhalení druhu použitého šifrovacího systému
- Prolomení - odhad, kolik šifrových zpráv bude kryptoanalytik potřebovat , aby měl přijatelnou naději, že jej prolomí. Prolomení je tedy nejtěžší část luštění
- Zjištění nastavení

Způsoby luštění:

1. Luštění se znalostí šifrového textu (Ciphertext-only attact). Kryptoanalytik má k dispozici pouze šifrové texty několika zpráv, které byly zašifrovány stejným šifrovacím algoritmem. Úkolem je získat otevřený text pokud možno co největšího počtu zpráv nebo odvodit klíč použitý k zašifrování zpráv a tím získat možnost dešifrovat jiné zprávy s tímto klíčem.
2. Luštění se znalostí otevřeného textu (Known-plaintect attact). Kryptoanalytik má k dispozici jak šifrové texty, tak také jim odpovídající otevřené texty, jeho úkolem je odvodit použitý klíč, který by mohl být následně použit k dešifrování dalších šifrových textů nebo najít algoritmus pro dešifrování všech dalších nových zpráv zašifrovaných stejným klíčem.
3. Luštění s možností volby otevřených textů (Chosen-plaintext attact). Kryptoanalytik má přístup k šifrovému textu a odpovídajícímu otevřenému textu několika zpráv, ale také si vybírá otevřené texty, které šifruje. Úkolem je tedy najít klíč nebo najít algoritmus pro dešifrování všech dalších nových zpráv zašifrovaných stejným klíčem.
4. Adaptivní metoda luštění s možností volby otevřených textů (Adaptive-Chosen-plaintext attact). Je to speciální varianta předchozího postupu. Kryptoanalytik si při ní může vybrat otevřený text, který bude šifrovat, ale může svůj výběr upravovat podle výsledků předchozího šifrování. Metoda pro posuzování nově zaváděných šifrovacích systémů. Šifrovací systém, který nelze rozluštit ani při této metodě, je opravdu silný.
5. Luštění s možností volby šifrových textů (Chosen-ciphertext-attact). Kryptoanalytik může dešifrovat šifrové texty dle vlastního výběru a má přístup ke vzniklým otevřeným textům. Útok je použitelný především v situaci, kdy má kryptoanalytik přístup ke kryptografickému zařízení, které umí dešifrovat vložený text, ale které luštitel nesmí porušit. Lze použít pro luštění asymetrických šifer.
6. Luštění s možností volby vybraného klíče (Chosen-key attack). Málo známá metoda a ve většině případů i těžko aplikovatelná. Využívá určitých vztahů mezi různými klíči.

7. Útok hrubou silou (Brute force attack). Úkolem kryptoanalytika je připravit test pro postupné zkoušení všech možných klíčů a vyhodnoceni, zda byl nalezen ten správný. Postup je teoreticky vždy správný, ale v praxi ne vždy vyjde. Existují však velmi účinné modifikace, kdy lze získat aspoň částečnou informaci. Tedy část parametrů kryptoanalytik získá jinou cestou a část touto metodou.
8. Útok postranními kanály (Side channel attacks). Útok může být veden za účelem získání klíče nebo otevřeného textu. První útoky tohoto typu byly spojené s únikem informací při elektromagnetickém vyzařování, s měřením spotřeby proudu a také s měřením času.
9. Agenturní, korupční kryptoanalýza (Agency/Purchase-key attack). Informace k používanému šifrovému systému a získání klíče jsou dosaženy podplacením nebo pomocí krádeží, ofocení, taky od osoby, která netuší, že vyzradila informace nesprávné osobě atd.
10. Pendreková kryptoanalýza (Rubber-hose attack). K získání klíče a dalších informací se využívá vydírání, vyhrožování a učení. Velmi účinné jsou poslední dva případy a tím lze vysvětlit, proč teoretická bezpečnost je vyšší než praktická.

1.3 Základní rozdělení klasických šifrových systémů

Následující tři způsoby šifrování lze spolu vzájemně kombinovat a používat vícekrát za sebou.

1.3.1 Substituce

Způsob zašifrování zprávy, spočívá v záměně použité abecedy otevřeného textu za znaky šifrové abecedy. Taková metoda je nazývaná *záměna* neboli *substituce* a šifry, které se takto vytvářejí, se nazývají *substituční šifry*. K převodu otevřeného textu na šifrový text lze použít jednu šifrovou abecedu pro celý text nebo může pro každé písmeno otevřeného textu být použita jiná šifrová abeceda. Příkladem nejjednodušší záměny může být Caesarova šifra nebo i klidně šifra, kterou si vytvoříme záměnou znaků v Morfeově abecedě.

Rozdělení substitučních šifer:

- Monoalfabetická šifra - též nazývaná jako jednoduchá substituce, jednoduchá záměna. V této šifře se každý znak otevřeného textu nahradí jedním znakem šifrové abecedy. Pro celý otevřený text se použije stejná šifrová abeceda. Může, ale i nemusí se skládat ze znaků abecedy otevřeného textu. Při luštění se využívá statických metod. Frekvenční analýza umožňuje srovnání s četností znaků otevřeného textu lehce odhalit pravděpodobný význam nejčetnějších znaků šifrové abecedy. Příkladem je Caesarova šifra.
- Homofonní substituce - šifra se snaží odstranit nedostatek jednoduché záměny, a proto k převodu některých vybraných znaků abecedy otevřeného textu, používá více znaků šifrové abecedy. Tím se ztíží luštění. Homofóny (šifrové znaky se stejným významem v otevřeném textu) se od samého začátku používaly u samohlásek. Příkladem je homofonní šifra Simone de Remy z Mantovy.
- Polyalfabetická substituce - šifra se snaží zakrýt statické závislosti v šifrovém textu, které by prozradily informace o otevřeném textu. Tedy další ztížení luštění. Skládá se z několika jednoduchých substitučních šifer, které jsou podle dohodnutého systému postupně použity na jednotlivé znaky otevřeného textu. Pokud tedy použijeme 26 různých jednoduchých substitučních šifer, pak každé písmeno otevřeného textu může být zašifrováno 26 různými způsoby. Systém byl považován za velmi dokonalý, protože z části vyřešil slabinu jednoduchých šifer. Dostavil se, ale jiný nedostatek. Šifru lze prolomit na základě analýzy vzdálenosti mezi opakováními řetězců šifrových znaků. Příkladem je šifra Vigenére.
- Bigramová substituční šifra, Polygramová substituční šifra - potřeba zvýšit odolnost, vedlo nejen k myšlence přiřadit ke každému znaku více znaků šifrové abecedy (homofonní nebo polyalfabetické substituce), ale i k nápadu zaměňovat celé skupiny otevřeného textu za skupiny šifrového textu. Pokud se zaměňují bigramy otevřeného textu za bigramy skládající se z šifrové abecedy, potom se šifra nazývá bigramovou substituční šifrou. Pokud se zaměňují skupiny tří znaků otevřeného textu za trojice znaků šifrové abecedy, jde o trigramovou substituční šifru. Souhrnně se těmto šifrám říká polygramová substituční šifra. Příkladem je šifra Playfair.

- Digrafická substituční šifra - je to speciální druh substituční šifry, kdy každý znak abecedy otevřeného textu je nahrazen dvojicí znaků šifrové abecedy. Příkladem je Polybiův čtverec.

1.3.2 Transpozice

Dalším způsobem, jak zašifrovat zprávu je zamíchání pořadí písmen v otevřeném textu. Jedná se o přeskupování písmen podle přesně určených pravidel, znalost umožňuje text zpětně sestavit – dešifrovat. Takovým šifrám říkáme *transpoziční šifry* neboli *transpozice*. Příkladem velmi jednoduché transpozice jsou přesmyčky nebo lištovky, známé z novin nebo napsání celého textu pozpátku.

1.3.3 Kódová kniha

Tento odlišný způsob spočívá v šifrování pomocí kódové knihy. Kódová kniha je vlastně slovníkem, ve kterém jsou vybraná slova nebo věty otevřeného textu nahrazované kódy. Obvykle to bývají čtveřice nebo pětice písmen nebo čísel. Účelem tohoto systému je ztížit luštiteli identifikaci obsahu nejužívanějších frází. Proto v případě nejčastěji používaných výrazů může kódová kniha obsahovat několik kódových skupin a odesílatel z nich může náhodně vybírat.

2 HISTORIE

Kapitola bude stručně popisovat historii klasického šifrování. Jedná se o naznačení nejvýznamnějších mezníků, tady nepůjde o vyčerpávající pojednání.

2.1 Starověk

Šifrování je téměř staré jako lidstvo samo. Texty staré 3000 let obsahují šifry. Šifry tehdy nesloužily k ukrytí informace, jako spíš aby text udělaly zajímavějšími např. Atbaš. Brzy na to šifry nabývají strategické účely. K tomu se využívala Caesarova šifra a skytale, tedy transpoziční šifry.

Taky se začalo používat skrývání zpráv - Stenografie. Příkladem může být příběh Histiaia[5], který kolem roku 440 př. n. l. poslal zprávu tak, že ji nechal vytetovat na vyholenou hlavu otroka a vyslal ho s touto zprávou, až mu vlasy povyrostly nebo dalším příkladem je Démarét, který byl u perského soudu a varoval Spartu před invazí perského krále Xerxa. Použil voskovou tabulku, na kterou se tehdy psávalo, zašifroval to tak, že nejprve odstranil vosk, vyryl zprávu a zase zalil voskem, vypadala tedy jako nepoužitá. (na zprávu se ve Spartě přišlo náhodou, neuměli ji rozluštit)

Šifrování se nejen uplatňovalo ve vojenských a politických strategií, ale například i v Kámasútře (šifrování sloužilo párům k uchovávání a předávání korespondence).

2.2 Středověk a raný novověk

Kryptologie se v 5. až 15. století rozvíjela pomalu, používaly se jednoduché substituce a transpozice. Na Předním východě se začala vyvíjet kryptoanalýza. Ze 14. století pochází první dochovaný popis řešení jednoduché substituce založený na frekvenční analýze (zkoumání počtu jednotlivých písmen v textu). Objevili ji Arabové.

---

[5] Histiaia – jeden z mužů, který stál za Iónské povstání kvůli perské nadvládě.

V Evropě díky válkám a konfliktům nabývalo šifrování velkých rozměrů, například pro obležená města byly šifry velmi důležité, taky v politice hrají šifry velmi důležitou roli. Příkladem může být případ Marie Stuartovny[6], která přišla o hlavu kvůli rozluštěným šifrám, kde plánovala zabití své sestřenice Alžběty.

V té době mělo šifrování i své specialisty. Experti byly hlavně ve Francii, velikánem zde byl Antoine Rossignol[7]. Šifry byly pořád stále jednoduché, pouze se začínaly používat klamače (symboly bez významů), nomenklátorů (symbol pro často používané slovo) nebo komolení textu. Techniky luštění těchto šifer nejsou těžké a staly se všeobecně rozšířenými.

V roce 1466 Leon Battist Alberti[8] zdokumentoval složitější substituce. V roce 1553 Giovan Batista Belaso[9], vymyslel substituční šifrování podle hesla, tedy polyalfabetickou substituci a asi o 30 let později, to ve své knize vydal Blaise de Vigenére[10], který ji nazval jako Vigenérova šifra (považována dlouho za nerozluštitelnou).

V Anglii byl představitel šifrování sir Francis Bacon[11], který navrhnul šifru dnes nazývanou 5bitovým binárním kódem. Jeho schopnosti byly natolik fascinující, že to vedlo k podezření, že je autorem Shakespearovských děl.

Další technika, která se ve středověku rozšířila, je akrostich. Akrostich je báseň či jiný text, jehož počáteční (koncové) slabiky (písmena, slova) ukrývají informaci. Příkladem může být akrostich od Francesco Colonna[12] (Hypnerotomachia Poliphili z roku 1499).

---

[6] Marie Stuartovna - byla francouzskou (1559-1560) a vládnoucí skotskou (1542-1567) královnou.

[7] Antonie Rossignol - francouzský matematik a kryptolog

[8] Leon Battist Alberti - byl italský humanista, architekt, teoretik umění, spisovatel a matematik

[9] Giovan Batista Belaso – původně popsal Vigenérův kód v roce 1553 v knize La cifra del. Sig. Giovan Batista Belaso

[10] Blaise de Vigenére – francouzský diplomat, který se narodil v roce 1523. Vigenére vymyslel šifru, při které využíval několik abeced.

[11] sir Francis Bacon - byl anglický vědec, filosof a státník. Je považován za zakladatele empirismu

[12] Francesco Colonna - italský kněz a mnich, který psal básně

2.3 Devatenácté století

V této době se šifrování rozšířilo. Významným vynálezem byl telegraf. Umožňoval rychle předat zprávu na velkou vzdálenost, ale bohužel neposkytoval dostatečné soukromí, protože telegrafista si zprávu musel přečíst a tím pádem ostatní se mohli snadno "napíchnout".

V této době začíná šifrování být i významné v oblasti obchodnictví. Významné bylo i používání takzvaných polních šifer. Tyto šifry byly úzce spjaty s armádou. Velmi důležité bylo, aby šifra byla rychle zašifrovaná, ale i dešifrovaná. Uplatnilo se to například v americké občanské válce 1861-1865. Kde se objevilo použití Vigenérovy šifry, ale i Jeffersonova válečku (též zvaného jako Bazeriův cylindr). Váleček byl sestaven z 20 až 30 disků, každý z těchto disků obsahuje jinak přeházenou abecedu. Klíčem je posloupnost čísel udávající pořadí disků plus jedno číslo udávající posun. Odesílatel seřadí disky podle posloupnosti, poté je nastaví tak, aby se v jednom sloupci objevila zpráva, a jako šifrovaný text zapíše písmena ve sloupci udaném posunem. Šifra je poměrně bezpečná.

Toto období bylo taky velmi příznivé pro vznik nových šifer. Jedna z nejúspěšnějších šifer se stala šifra sira Charlese Wheatstona[13] z roku 1854, knižně ji popsal Lyon Playfair[14] a šifra měla tedy název Playfair.

2.4 První světová válka

V roce 1894 byl učiněn velmi důležitý objev v podobě rádia, které umožňovalo rychlejší komunikaci, ale zato soukromí zde nebylo žádné. Šifrování se tak stává nutností, z důvodu toho, že to slyší všichni a to bez nutnosti se napíchnout. Nejpoužívanější šifry byly polní šifry, založené na složitějších substitucích, jako je šifra Playfair a ADFGX.

---

[13] Charles Wheatston - byl anglický vědec a vynálezce mnoha vědeckých průlomů, objevil šifru Playfair

[14] Lyon Playfair – (1818 – 1898), anglický vědec a poslanec, pojmenována podle něj Playfair kód, kterou velmi velmi usilovně prosazoval.

Dál velmi časté bylo použití takzvané kódové knihy (slovníku), pomocí kterých se zprávy překládaly do tajných kódů, a jediným způsobem rozluštění bylo, když člověk vlastnil onu kódovou knihu. To vedlo k oblíbenosti takzvaných falešných kódových knih.

V té době, Anglické královské námořnictvo mělo kryptografickou jednotku, kterou vedl sir William Hall[15], pod názvem *Room 40*. Jejich úspěch stál u jednoho z klíčových okamžiků první světové války, zapojení USA do války. V roce 1917, když Němci se chystali začít ponorkovou válku v Atlantiku a báli se, že by tento krok mohl vyprovokovat Američany k zapojení do války. K odpoutání pozornosti šikovně využili Mexika. Německý ministr zahraničí Arthur Zimmermann, poslal v lednu 1917 německému velvyslanci v USA telegram, kde sděloval, že chtějí začít ponorkovou válku a v případě zapojení USA do války, přesvědčit Mexiko aby zaútočilo na USA (za to že jim poskytnou vojenskou podporu) a tak Mexiko zprostředkovalo jednání s Japonskem. Angličanům se podařilo telegram rozluštit, ale Hall se obával, že pokud by USA předal telegram přímo, tak by si mysleli, že jde o podvod, proto to narafičil tak, aby to vypadalo, že se anglický agent zmocnil rozšifrované zprávy v Mexiku, navíc do tisku poslal mylnou informaci o kritice svých služeb a tím Němce dokonale zmátl.

2.5 Druhá světová válka

Zde měla kryptologie velmi velký význam. Do roku 1931 využívala kryptologie převážně lingvisty. Po tomto roce se začali více uplatňovat matematikové. Další velká změna byla v mechanizaci šifrování. S rozvojem elektro-mechanických technologii rostly možnosti využití strojů. Základem šifrovacích strojů byly rotující disky, které obsahovaly dráty udávající substituci. Po zašifrování jednoho písmene se disk pootočil, takže další písmeno se šifrovalo jinou substitucí. Zapojením více propojených disků šlo vytvářet substituční šifry vysoké složitosti. Šifrovací stroje byly použity v USA (Sigaba), GB (Typex), Japonsku (Pyrole), Německu (Enigma).

[15] William Hall - byl britský důstojník Royal Navy

Nejznámější z nich je Enigma. Její rozluštění bylo jednou z klíčových událostí druhé světové války. Praktické použití probíhalo následovně: na každý den byl určen klíč, ale jednotlivé zprávy se vysílaly pomocí jednorázových, náhodně vybraných klíčů. Ty byly přeneseny jako první právě pomocí denního klíče. Aby se zabránilo chybám, vysílal se jednorázový klíč dvakrát po sobě. Tento detail byl základem k prolomení kódu. Počátek prolomení se datuje do roku 1931.

V Pacifiku dokázali Američané luštit šifry japonským mechanickým strojem Purple. Také se Američané proslavili kódem Navajo.

Důležitá byla taky stenografie. V roce 1860 byl vyřešen způsob zmenšování zpráv na velikost inkoustové skvrny, později zmenšena na velikost 1.3 mm.

2.6 Shrnutí nejvýznamnějších událostí klasické kryptologie

500 př.n.l.	Židé: jednoduchá substituční šifra (ATBASH)
400 př.n.l.	Řecko: jednoduché transpoziční šifry, steganografie
50 př.n.l.	Řím: Caesarova šifra
4.stol	Indie: šifrování mezi 64 uměními v Kámasútře
10.stol	Arabové: základy kryptoanalýzy včetně frekvenční analýzy
13.,14 stol.	Evropa:používá se substituční šifra, případně lehké nástavby
1412	Arabové: encyklopedie obsahující kapitolu o kryptologii
15.,16. stol.	první návrhy šifrování podle hesla
16. stol.	Evropa: kryptologie hraje důležitou roli v politice
1586	Anglie: poprava skotské královny na základě rozluštěné šifry
1843	USA: Poe píše o šifrách a zveřejní šifrovací výzvy.
1861	Prusko: metoda pro řešení polyalfabetické šifry (Kasiski)
1885	USA:Bealův poklad
19. stol	rozvoj telegrafu, rozvoj kryptografie pro komerční účely, polní šifry (Playfair), první mechanické přístroje pro šifrování
1. světová válka	důležitá role ve válce i v politice (Zimmermannův telegram), použití komplikovanějších šifer na klasických principech
1926	Německo: armáda začíná používat šifrovací přístroj Enigma
2. světová válka	klíčová role kryptologie ve válce, použití mechanických šifrovacích přístrojů

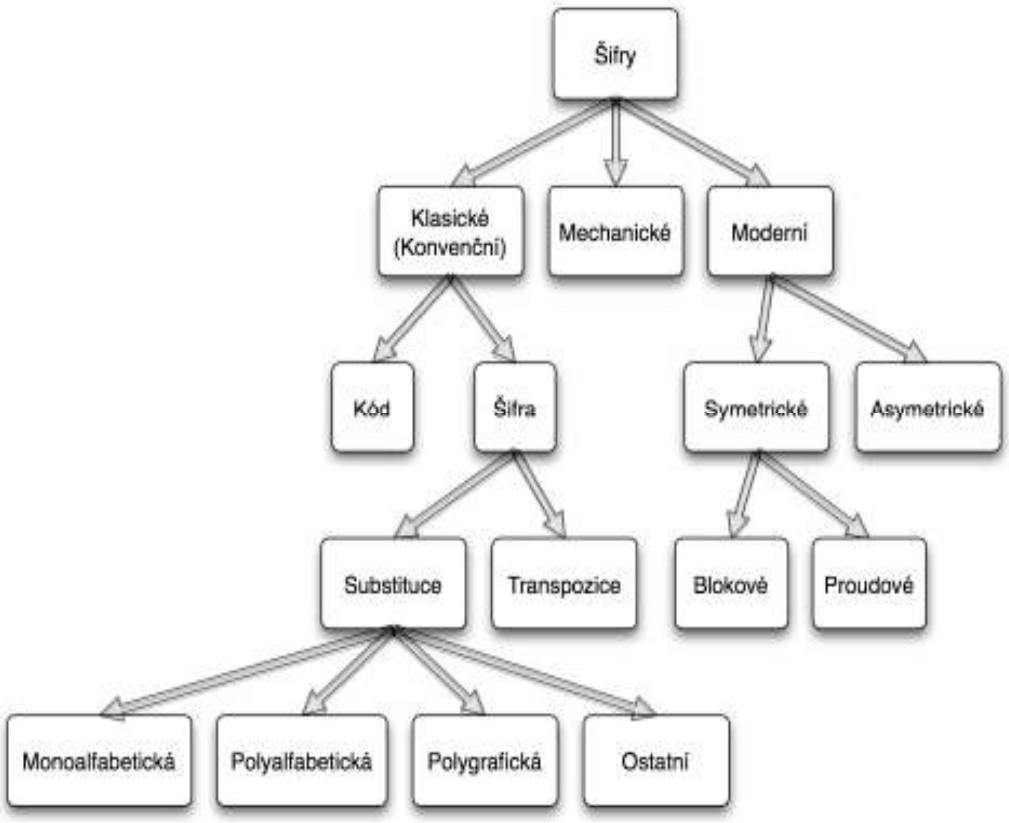
Tab. 1. Přehled nejdůležitějších událostí v kryptologii

PRAKTICKÁ ČÁST

3 PRAKTICKÉ UKÁZKY KÓDŮ A ŠIFER

Kapitola pojednává o šifrování a dešifrování. Zde jsou vybrány nejdůležitější kódy a šifry a jejich praktické použití.

3.1 Grafický přehled



Obr. 2. Souhrnný přehled šifer

3.2 Kódování

Podkapitola rozebírá dva nejdůležitější typy kódování. Je to Morseova abeceda a Braillovo písmo.

3.2.1 Morseova abeceda

Morseovu abecedu vymyslel na konci na konci 19. století americký fyzik Samuel F. B. Morse (1791–1872).

Jednotlivé znaky Morseovy abecedy se vysílají v kódu, který se skládá z krátkých a dlouhých signálů, každé písmenko se skládá z jednoho až čtyř znaků. V psané podobě se používají tečky a čárky, jednotlivá písmena se oddělují lomítkem, slova dvěma lomítky a věty lomítky třemi.

Pomocná slova slouží ke snadnějšímu zapamatování – krátká slabika znamená tečku a dlouhá čárku. Existují i jiná pomocná slova. Na háčky a čárky v překládané zprávě nebereme zřetel.

Znak	Zápis	Pomocné slovo	Znak	Zápis	Pomocné slovo
A	**. -**	Akát	N	- .	Nástup
B	- . . .	Blýskavice	O	- - -	Ó náš pán
C	- . - .	Cílovníci	P	. - - .	Papírníci
D	- . .	Dálava	Q	- - . -	Kvílí orkán
E	.	Erb	R	. - .	Rarášek
F	. . - .	Filipíny	S	. . .	Sobota
G	- - .	Grónská zem	T	-	Tón
H	. . . .	Hrachovina	U	. . -	Uličník
CH	- - - -	Chvátám k vám sám	V	. . . -	Vyučený
I	. .	Ibis	W	. - -	Wagón klád
J	. - - -	Jasmín bílý	X	- . . -	Xénokratés
K	- . -	Krákorá	Y	- . - -	Ýgar mává
L	. - . .	Lupíneček	Z	- - . .	Známá žena
M	- -	Mává			

Tab. 2. Morseova abeceda

Číslo	Zápis	Číslo	Zápis
1	. - - - -	6	- . . . .
2	. . - - -	7	- - . . .
3	. . . - -	8	- - - . .
4	. . . . -	9	- - - - .
5	. . . . .	0	- - - - -

Tab. 3. Číslice v Morseově abecedě

Číslo	Zápis	Číslo	Zápis
.	. - . - . -	Zač. vysílání	- . - . - . - .
,	- - . . - -	Jsem připraven	. - - .
;	- . - . - .	Rozumím	- - - - . -
!	- - . . . -	Nerozumím	. . . . .
?	. . - - . .	Pomaleji	- . - . - ..
:	- - - . . .	Omyl	. / . / . / . / . / . / . / .
-	- . . . . -	Čekej	. - . . .
=	- . . . -	Opakuji	. . / . . / . . / . . / . .
"	. - .. - .	Konec vysílání	. . . - . -
()	- . - - . -	Zlomková čára	- . . - .
@	. - - . - .	SOS	. . . / - - - / . . .

Tab. 4. Další znaky používané v Morseově abecedě

Příklad šifrování:

Otevřený text: S H A M A N

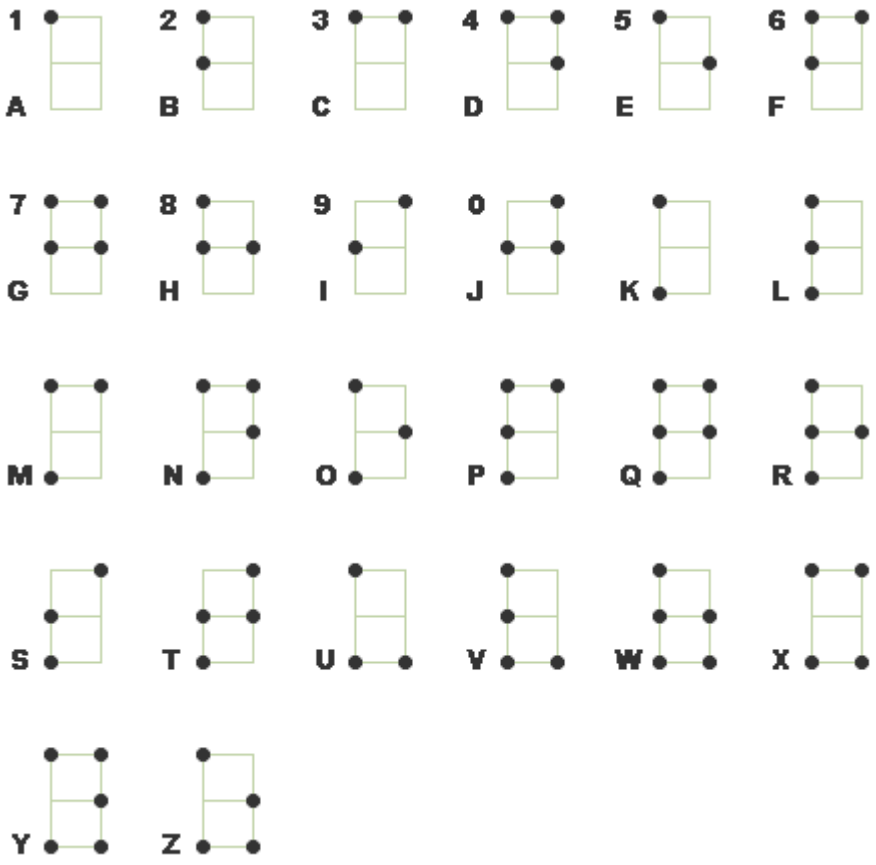
Šifrový text: . . . / . . . . / . - / - - / . - / - . //

3.2.2 Braillovo písmo

Je zvláštní způsob zápisu textu, umožňující čtení hmatem.

Každý znak Braillova písma tvoří 6 bodů uspořádaných do obdélníku 2 x 3. Na každém z těchto bodů může nebo nemusí být do papíru vytlačena hmatatelná tečka. To dává 64 možných kombinací, pokud prázdný znak (bez teček) považujeme za mezeru, zbývá nám 63 znaků. Šifrujeme tak, že znaky opíšeme nebo špendlíkem vyznačíme na papír. Je třeba psát zrcadlově obráceně – vytlačujeme zespoda, aby bylo možné číst shora. Typická velikost Braillova písmena je asi 5 x 7,5 mm, na jeden řádek by se mělo vejít asi 30 znaků.

Základní znaky:



Obr. 3. Základní znaky Braillova písma

3.3 Šifrování

V této podkapitole jsou popsány nejdůležitější symetrické šifry, jejich správné rozdělní šifrování.

- SUBSTITUČNÍ

1. Monoalfabetická
    - Pevný posun (Caesar, Rot 13 atd)
    - Obrácená abeceda (ATBASH)
    - Lineární posun (ax + b mod 26)
    - Zpřeházená abeceda
    - Využití klíčového slova
    - Vernamova šifra
    - Baconova šifra
2. Polyalfabetická
    - Vigenérova šifra
    - Autoklíč (autokláv)
3. Polygrafická
    - Playfair
    - Bifid
    - Trifid
    - Hillova šifra
4. Ostatní
    - Homofonní substituce
    - Šifra s nomenklátory a klamači (šifra Marie Stuartovny)
    - Polybiův čtverec
    - Tabulka 5x10
    - Tabulka 4 x 7 jedno a dvojmístné šifry
    - Knižní šifra

TRANSPOZIČNÍ

- Přesmyčky
- Hadovky, spirály
- Jednoduchá transpozice v tabulce
- Jednoduchá transpozice v tabulce s klíčem
- Transpozice v tabulce s dvěma hesly
- Dvojitá transpozice
- Zubatka
- Cardanova mřížka
- Šifrovací mřížka – otočná mřížka

3.3.1 Monoalfabetická substituce

- Caesarova šifra

Julius Caesar byl nejen římským císařem a politikem, ale také se významně zapsal do kryptografie. Jeho šifra je psána tak, že každé písmeno zprávy bylo zaměněno za písmeno, které leželo o tři místa dále v abecedě a z konce abecedy se přejde na začátek abecedy. Je to velmi jednoduchá záměna. Systém nemá klíč.

Šifrování je ukázáno na textu Mundus vult decipi - Svět chce být klamán. Otevřený text se přepíše do abecedy a potom se každé písmeno zprávy zamění za písmeno, které leží o tři místa dále v abecedě:

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
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

Tab. 5. Caesarova šifra

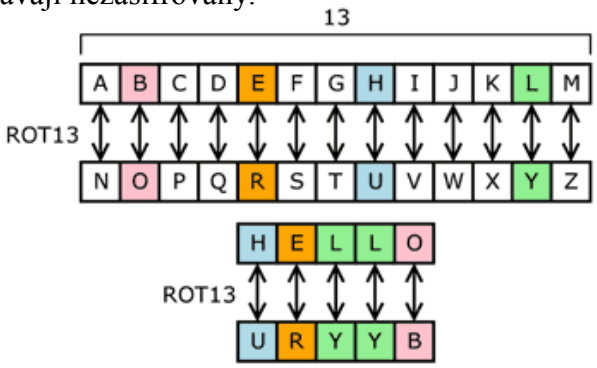
Příklad:

Otevřený text: SVĚT CHCE BÝT KLAMÁN

Šifrový text: VYHW FKFH EBW NODPDQ

- Rot13

Jedná se o pevný posun abecedy. Ale na rozdíl od Caesarovy šifry používá ke kódování rotace písmen o 13 míst (A->N,B->O,…,Z->M). Čísla a další speciální znaky tak zůstávají nezašifrovány.



Obr. 4. Šifra Rot13

- Atbash

  Šifře se říká převrácená abeceda a to z důvodu, že se vezme písmeno, spočítá se jeho vzdálenost od začátku abecedy a nahradí se písmenem, které se nachází v téže vzdálenosti od konce abecedy. Princip šifry je naznačen už v samotném názvu, neboť písmena A-T-B-Š jsou postupně prvním (alef), posledním (thav), druhým (bet) a předposledním (šin) písmenem hebrejské abecedy.

  Pro mezinárodní abecedu by podle tohoto pravidla vypadala převodová tabulka následným způsobem:

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
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Tab. 6. Šifra Atbash

Příklad:

Otevřený text: OKO ALBATROS

Šifrový text: LPL ZOYYGILH

- Lineární posun

  Nebo taky lineární transformace ax + b mod 26 (taky zváno *afinní šifra*). Lineární posun částečně eliminuje zásadní nevýhodu Caesarovy šifry - málo možností transformace a tím i velmi primitivní kryptoanalýzu. Základem tohoto kryptografického systému je následující transformace:

$$C_i = a * T_i + b \pmod m$$

C_i – i-té písmeno šifrovaného textu

T_i – i-té písmeno otevřeného textu

a – parametr a

b – parametr b

m – modulo (jako modulo se obvykle volí 26)

Příklad:

Otevřený text: THEINITIAL

Šifrový text: ASDXWXAXJM

a = 5 b = 9 m = 26

	v abecedě	a*T +b mod(26)	výsledek	v abecedě
T	19	5*19+9 mod(26)	0	A
H	7	5*7 + 9 mod(26)	18	S
E	4	5*4 + 9 mod(26)	3	D
I	8	5*8 + 9 mod(26)	23	X
N	13	5*13+9 mod(26)	22	W
I	8	5*8 + 9 mod(26)	23	X
T	19	5*19+9 mod(26)	0	A
I	8	5*8 + 9 mod(26)	23	X
A	0	5*0 + 9 mod(26	9	J
L	11	5*11+9 mod(26)	12	M

Tab. 7. Lineární posun ax + b mod 26

- Zpřeházená abeceda

Je to jednoduchá substituce. Nahrazuje jednotlivá písmena jinými písmeny z abecedy. Klíčem je *substituční tabulka*, ve které je pod každým písmenem abecedy ve spodním řádku písmeno, které jej v šifrovém textu nahrazuje. Spodní řádek je vlastně nějakou permutací písmen abecedy. Prostor klíčů je dostatečně velký (26!). Nelze tedy řešit hrubou silou.

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
E	L	Q	D	X	B	P	K	Y	R	W	V	A	M	O	I	U	S	Z	C	F	H	N	T	J	G

Tab. 8. Zpřeházená abeceda

- Využití klíčového slova

  Je to převod dle klíčového slova: slovo, ze kterého vynecháme opakující se písmena, tvoří začátek šifrovací abecedy, zbylá písmena se doplní v abecedním pořadí. Slovo veslo je zde jako klíč.

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
V	***E***	***S***	***L***	***O***	A	B	C	D	F	G	H	I	J	K	M	N	P	Q	R	T	U	W	X	Y	Z

Tab. 9. Caesarova šifra s použitím klíčového slova

- Vernamova šifra

  Vernamova šifra nebo také jednorázová tabulková šifra (anglicky one-time pad). Postup šifrování je následující:

  Vezmou se jednotlivá písmena tajné zprávy a každé z nich se posune o několik pozic v abecedě. Například první písmeno je posunuto o 5 pozic, druhé o 1, třetí o 14, čtvrté o 24, další o 9, 0, 3, 9, 19. Když se při posouvání překročí konec abecedy, pokračuje se od jejího začátku. Ze slova ALDEBARAN se dostane šifrový text FMRCKAUJG. Posloupnost 5, 1, 14, 24, 9, 0, 3, 9, 19 je klíčem k rozluštění zprávy.

- Baconova šifra

  Přesně vzato Baconův kód je spíše steganografický kód, než skutečnou šifrou. Zpráva je ukryta v textu ne v obsahu. Některá písmena jsou nahrazena tučně nebo kurzívou. Text je rozdělen do skupin po pěti písmenech a písmena v těchto skupinách jsou zastoupena 'A' nebo 'B'. Existují dvě verze Baconova kódu.

A = AAAAA	G = AABBA	N = ABBAA	T = BAABA
B = AAAAB	H = AABBB	O = ABBAB	U + V = BAABB
C = AAABA	I + J = ABAAA	P = ABBBA	W = BABAA
D = AAABB	K = ABAAB	Q = ABBBB	X = BABAB
E = AABAA	L = ABABA	R = BAAAA	Y = BABBA
F = AABAB	M = ABABB	S = BAAAB	Z = BABBB

Tab. 10. První verze Baconovy šifry

A = AAAAA	G = AABBA	M = ABBAA	S = BAABA	Y = BBAAA
B = AAAAB	H = AABBB	N = ABBAB	T = BAABB	Z = BBAAB
C = AAABA	I = ABAAA	O = ABBBA	U = BABAA	
D = AAABB	J = ABAAB	P = ABBBB	V = BABAB	
E = AABAA	K = ABABA	Q = BAAAA	W = BABBA	
F = AABAB	L = ABABB	R = BAAAB	X = BABBB	

Tab. 11. Druhá verze Baconovy šifry

3.3.2 Polyalfabetická substituce

- Vigenérova šifra

  Jedná se o nejpoužívanější variantu polyalfabetické šifry. Je to metoda šifrování, která používá sérii různých Caesar kódů.

  Vigenérova šifra jako hlavní prvek pro šifrování používá heslo, jehož znaky určují posunutí textu a to způsobem, kdy je text rozdělen na bloky znaků, jejichž počet je řízen počtem znaků hesla. Každý znak je poté sečten s příslušným znakem hesla. Tímto se stává jedním z nejsložitějších šifrovacích algoritmů. Je tedy založena na využití tabulky, kterou používá Trithemiova šifra. Na rozdíl od ní, však určuje výběr převodové tabulky nikoli pořadí znaků v otevřeném textu, ale znak hesla. Heslo zná pouze odesílatel a příjemce. Toto heslo si uživatel zapíše opakovaně nad text, aby věděl, jakou abecedu má pro zašifrování konkrétního písmena použít. Proto se tomu říká taky *periodické heslo*.

  Příklad:

  Klíč: OKNOOKNO

  Otevřený text: ALBATROS

  Šifrový text: OVOOHBBG

Nad otevřený text vepíšeme klíč (Okno). Klíč je opakován tak dlouho, až pokryje celý otevřený text. Nyní se začne šifrovat a k tomu je použit Trithemiův postup, který spočívá v tom, že šifra používá tabulku sestavenou z 26 seřazených abeced. Tato tabulka se nazývá *tabula recta*.

Tedy v příkladu je první písmeno otevřeného textu je A, to se vyhledá v první abecedě a odpovídající šifrový znak se nalezne pod ním v abecedě tedy písmeno O. Druhé písmeno je L najde se v první abecedě a odpovídající šifrový znak je nalezen pod ním v abecedě, tedy K a hledaný šifrový znak je v tomto případě V atd.

	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
A	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
B	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Obr. 5. Tabula recta

- Autoklíč (Autokláv)

  Autoklíč otevřeného textu. Princip šifry spočívá v tom, že osoba, která text šifrovala, se domluví s příjemcem na počátečním písmenu. Toto písmeno tvoří začátek autoklíče a pak se doplní o otevřený text. Vznikne tak autoklíč otevřeného textu. Dále se šifruje pomocí známého postupu, tedy systému Vigenére.

Princip autoklíče spočívá na domluveném písmenu, které je K a otevřený text ALBATROS

Klíč: *K*ALBATRO

Otevřený text: ALBATROS

Šifrový text: KLMBTKFG

Autoklíč šifrového textu. Je to postupné vytváření autoklíče ze vzniklého šifrového systému. Osoba, která šifruje, se domluví s příjemcem na počátečním písmenu – tvoří začátek autoklíče. Vytváření: je známo počáteční písmeno a první znak textu určí znak šifrového textu. K tomu je potřeba znalost Vigenérova postupu. První znak šifrového textu se zapíše do šifrové zprávy a taky nad druhý znak otevřeného textu a tím je vytvořen druhý znak.

Příklad:

Klíč: *D*DOPPIZN (domluvené písmeno D)

Otevřený text: ALBATROS

Šifrový text: DOPPIZNF

3.3.3 Polygrafická substituce

- Šifra Playfair

  Je odolná vůči frekvenční analýze. Jedná se o digramovou záměnu. Nejprve se upraví podle jednoduchých pravidel text a potom se podle abecedního čtverce záměny podle čtyř prostých pravidel zašifruje. Abecední čtverec se vytváří podle dohodnutého slova, které je klíčem tohoto systému.

Příklad:

Otevřený text: TATO ŠIFRA JE DOCELA JEDNODUCHÁ

Odstraní se diakritiky a interpunkce, náhrada I za J:

TATO SIFRA IE DOCELA IEDNODUCHA

Rozdělení na bigramy, v případě dvou stejných písmen v digramu vložíme x a y, sudý počet písmen se doplní z:

TA TO SI FR AI ED OC EL AI ED NO DU CH AZ

Za domluvené klíčové heslo bylo zvoleno slovo HESLO:

H	E	S	L	O
A	B	C	D	F
G	I	K	M	N
P	Q	R	T	U
V	W	X	Y	Z

Tab. 12. Abecední čtverec

Písmena TA neleží ani ve stejném řádku ani ve stejném sloupci a proto podle pravidla 3 je nahrazeno PD a tak se pokračuje až do osmého digramu, kde na EL se použilo pravidlo 1, pak to bude SO a na jedenáctý digram NO použilo druhé pravidlo, pak výsledek je UF. Konečný text se rozdělí do pětic, poslední skupina tří písmen byla doplněna o dvě X.

Šifrový text: PDULE KCUBG LBSFS OBGLB UFFTA SFVXX

- Bifid

U této šifry se vezme čtverec 5 x 5 polí a očíslují se řádky i sloupce čísly 1 až 5. Poté se zpráva rozdělí na skupinky pevné délky po pěti písmenech a pod každé písmeno se napíše pod sebe řádková a sloupcová souřadnice.

	1	2	3	4	5
1	P	E	T	R	K
2	L	I	C	A	B
3	D	F	G	H	M
4	N	O	Q	S	U
5	V	W	X	Y	Z

Tab. 13. Abecední čtverec šifry Bifid

DOCKE	JCASU	JAKOH	USAKL	ASU
3 4 2 1 1	2 2 2 4 4	2 2 1 4 3	4 4 2 1 2	2 4 4
1 2 3 5 2	2 3 4 4 5	2 4 5 2 4	5 4 4 5 1	4 4 5

Tab. 14. Rozdělená zpráva šifry Bifid

Pak se přepíšou čísla po řádcích, rozdělí se do dvojic a pomocí tabulky je to zpětně přepsáno na písmena.

3 4 2 1 1 1 2 3 5 2	2 2 2 4 4 2 3 4 4 5	2 2 1 4 3 2 4 5 2 4	4 4 2 1 2 5 4 4 5 1	2 4 4 4 4 5
H L P C W	I A O H U	I R F U I	S L B S V	A S U

Tab. 15. Konečný výsledek šifry Bifid

- Trifid

  Tato šifra používá tříčíselné kódy z čísel 1, 2, 3, která kódují písmena v trojrozměrné tabulce o 27 polích.

  Příklad:

1				2				3			
Q	Y	F	1	S	A	L	1	D	O	T	1
B	M	R	2	K	V	E	2	Z	G	C	2
Y	I	W	3	U	J	?	3	H	P	N	3
1	2	3		1	2	3		1	2	3	

Tab. 16. Tabulka Trifid

Čísla jsou získána po převodu pomocí těchto tabulek. Opět se zapisují do řádků.

Otevřený text: NOVY TYP SIFRY

Po úpravě: NOYVT YPSIF RY

Přepis podle tabulky:

1. řádek	*3*3213 13211 11
2. řádek	*3*1211 13131 21
3. řádek	*3*2223 22123 32

Tab. 17. Přepis tabulky Trifid

Následně se šifrují souřadnice, které sdružujeme na trojice v rámci jednoho číselného vyjádření, pak se pokračuje řádkem pod ním atd. a tyto skupiny se převedou zpět na písmena.

Převod: v prvním sloupci vyšlo: PWBIE, Ve druhém: IQTMR a ve třetím: YI

Šifrový text: PWBIE IQTMR YI

- Hillova šifra

Je založena na lineární transformaci bloku zprávy pomocí násobení matic. Šifruje se tak, že je zvolena délka bloku *n*. Zpráva je následně zapsána pomocí číselné reprezentace a potom se vše rozdělí na bloky zvolené délky. Klíč tedy bude matice A stupně *n*. Blok zprávy je šifrován tak, že se vezme jeho vektor a ten je vynásoben jeho maticí A. Výsledek modulo 26 a zapíšeme pomocí písmen.

Příklad:

Matice A: 1 -2 1

2 0 1

2 -1 1

Přepis na čísla a rozděleno do trojic:

d o c	k e j	c a s	u j a	k o h
3 14 2	10 4 9	2 0 18	20 9 0	10 14 7

Tab. 18. Rozdělení a přepis u Hillovy šifry

Každá trojice se zašifrujeme pomocí násobení trojic se zvolenou maticí. Takže písmena *d o c* se zašifrovala na (-23, 8, -6). K záporným číslům připočte 26, což v abecedě je (3, 8, 20) a značí nám to písmena *c i u*.

3.3.4 Ostatní substituce

- Homofonní substituce

Je vylepšená monoalfabetická šifra, protože umožňuje šifrovat jedno písmeno z otevřené abecedy několika různými způsoby, takže v šifrovém textu může být původní písmeno „a“ zastoupeno několika různými symboly, čímž luštiteli efektivně znemožníme použití jednoduché frekvenční analýzy. Přestože se může jedno písmeno zašifrovat na různé symboly, jedná se stále o šifru s jednou šifrovou abecedou. Šifra se hojně používala především díky své jednoduchosti oproti polyalfabetickým šifrám a díky – na svou dobu – dostatečné bezpečnosti.

Příklad:

Otevřený text: LAKOMÁ LOKOMOTIVA

Substituční tabulka

A: 10 15 17	K: 18
O: 11 27 30	M: 07 54
I: 26	T: 01
L: 33 34	V: 09

Tab. 19. Substituce

Šifruje se tak, že za A je na výběr z 10, 15, 17 zvolí se třeba 17, za L 33 nebo 34 zvolí se třeba 33 a tak postupuje až ke konci.

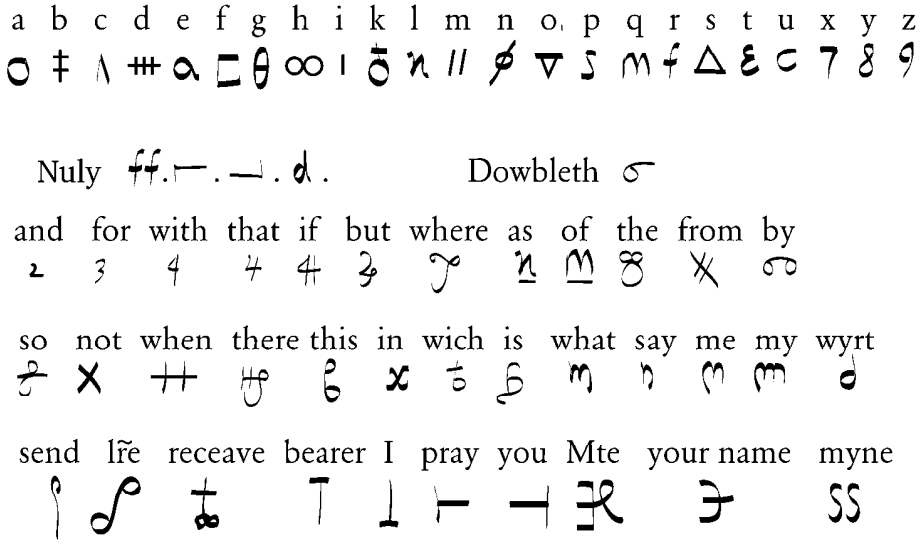
Šifrový text: 33 17 18 27 07 10 34 11 18 30 54 27 01 26 09 10

- Šifra s nomenklátory a klamači

Vybraným frekventovaným slovům se přiřadí speciální symbol. Tato kódová slova se nazývají nomenklátory. Klamač (nula) je dalším ztížení šifry, tyto znaky totiž

nemají žádný význam, slouží pouze pro zmatení nepřítele. Další komplikace, která stíží analýzu je použití úmyslně zkomoleného textu.

Příkladem je šifra Marie Stuartovny:



Obr. 6. Substituční šifra Marie Stuartovny

- Polybiův čtverec

Polybiův čtverec je velmi jednoduchá šifra. Jde pouze o to, seřadil abecedu do čtvercové tabulky 5 × 5 a očísloval její řádky a sloupce. Každé písmeno původního textu pak nahrazovala dvojice písmen, nejprve číslo řady, pak číslo sloupce.

Příklad:

Jednoduše vepíše abeceda s vynecháním háčků, čárek a písmen Ch a W. Někdy se vynechává Q, méně obvyklou možností je vynechat písmeno J (resp. považovat J a I za stejné písmeno), podobně jako se činí u šifry Playfair.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

Tab. 20. Polybiův čtverec

Otevřený text: P O L Y B I U V Č T V E R E C

Šifrový text: 41 35 32 54 12 24 51 52 13 45 52 15 43 15 13

- Tabulka 5 x 10

	1	2	3	4	5	6	7	8	9	0
1	A	Á	B	C	Č	D	Ď	E	Ě	É
2	F	G	H	I	Í	J	K	L	M	N
3	Ň	O	Ó	P	Q	R	Ř	S	Š	T
4	Ť	U	Ů	Ú	V	W	X	Y	Ý	Y
5	Ž	;	"	-	/	'	+	?	!	

Tab. 21. Šifra 5 x 10

Otevřený text: P R A H A J E K R Á S N Á

Šifrový text: 34 36 11 23 11 50 26 18 50 27 36 12 38 20 12

- Tabulka 4 x 7

	-	1	2	3	4	5	6
7	A	B	C	D	E	F	G
8	H	I	J	K	L	M	N
9	O	P	Q	R	S	T	U
0	V	W	X	Y	Z	/	+

Tab. 22. Šifra 4 x 7

Otevřený text: Z I T R A M I Z A V O L E J

Přepíšeme podle tabulky: 04 81 95 93 7 85 81 04 7 0 9 84 74 82

Šifrový text: 04819 59378 58104 70984 7482

- Knižní šifra

  Použije-li se jeden klíč $k_1k_2...k_n$ k zašifrování otevřeného textu $p_1p_2...p_n$,

  Dostane se šifrový text $c_1c_2\ldots c_n$, kde

  $$c_i = p_i + k_i \mod 26$$

  pro i=1,2,…,n.

  Použije se stejný klíč $k_1k_2...k_n$ k zašifrování jiného otevřeného textu $q_1q_2...q_n$,

  Dostane se šifrový text $d_1d_2\ldots d_n$, kde

  $$d_i = q_i + k_i \mod 26$$

  pro i=1,2,…,n.

  Odečtením obou šifrových textů se dostane

  $$c_i - d_i = p_i - q_i \mod 26$$

  pro i=1,2,…,n.

3.3.5 Transpoziční šifry

Transpoziční šifry mění pouze pořadí písmen, nikoliv jejich vzhled. Většina šifer je založena na určitém geometrickém postupu. Text je napsán do geometrického obrazce, nejčastěji obdélníku či čtverce, a poté je jiným způsobem přepsán do výsledného textu.

- Přesmyčky

  Mění pouze pořadí písmen, nikoli jejich vzhled. Nejjednodušší přehazují písmena v rámci jednoho či dvou řádků

  Příklad:

  Otevřený text: KDO HONÍ DVA ZAJÍCE NECHYTÍ ŽÁDNÉHO

  Šifrový text: KDOH ON IDVAZ A JIC ENEC HY TIZADN EHO

- Hadovky, spirály

  To že se jedná o hadovku lze poznat z uspořádání textu: obvykle bývá text uspořádán do čtverce o stejném počtu řádků a sloupců nebo alespoň do obdélníku. Text tvoří jednu dlouhou souvislou řadu písmen – tedy hada.

  Jde o to najít si smysluplné slovo a k němu dohledat návaznosti.

  Příklad:

  Otevřený text: HESLO PRO TUTO ÚLOHU JE NÁCELNÍK

  Šifrový text:

H	L	O	O	T	O	U	H	U	N	A	L	N	X
E	S	P	R	U	T	L	O	J	E	C	E	I	K

Tab. 23. Hadovka

- Jednoduchá transpozice v tabulce

  Jednoduchá transpozice v tabulce spočívá v tom, že heslo, které může být stanoveno podle smluveného textu nebo přímo číselně, se napíše při šifrování jenom jednou a otevřený text se píše pod heslo vodorovně zleva doprava a shora po řádcích.

  Příklad:

12	9	19	10	13	4	6	15	7	1	3	14	20	17	11	2	18	5	8	16
N	I	C	N	E	N	I	T	A	K	T	E	Z	K	E	A	B	Y	S	E
T	O	H	O	D	A	R	E	B	A	C	T	V	I	M	N	E	D	O	S
A	H	L	O	X	P	E	T	R	O	N	I	U	S						

Tab. 24. Jednoduchá transpozice

Šifrový text se získá výpisem sloupců tabulky v pořadí podle hesla (vzestupně). Zapisuje se do pětimístných skupin:

Šifrový text: KAOAN TCHNNA PYDIR EABRS OIOHN OOEMX

NTAED XETIT ETESK ISBEC HLZVU

- Jednoduchá transpozice v tabulce s heslem

  Písmena se přeskupují podle hesla konstantní délky, která je označena n. Heslo se vytvoří podle smluveného slova nebo několika slov. Například smluvené heslo je PRAZSKEJARO (n = 11), potom jeho číselné vyjádření získáme postupným očíslováním písmen vybíraných podle abecedy od A do Z zleva doprava.

  Příklad:

P	R	A	Z	S	K	E	J	A	R	O
		1						2		
						3	4			
					5					6
7	8								9	
				10						
			11							

Tab. 25. Heslo a očíslování

7	N	E	H	I	X
8	I	Z	O	M	P
1	C	K	D	N	E
11	N	E	A	E	T
10	E	A	R	D	R
5	N	B	E	O	O
3	I	Y	B	S	N
4	T	S	A	A	I
2	A	E	C	H	U
9	K	T	T	L	S
6	T	O	V	O	X

Tab. 26. Zašifrování

Každý blok 11 písmen musí být plný. Výsledná šifra je zapsána do pěti-místních skupin.

Šifrový text: CAINT TNIKE NKEYS BOEZT AEDCB AEVHO TRANH SAOOI MLDEE UNIOX XPSRT

- Jednoduchá transpozice v tabulce s dvěma hesly

  Příklad:

  Heslo 1 (vodorovné): K O M U N I K A C E

  5 9 7 10 8 4 6 1 2 3

  Heslo 2 (svislé - voleno až podle délky textu):

	5	9	7	10	8	4	6	1	2	3
1	V	I	C	E	L	Z	E	D	O	S
2	A	H	N	O	U	T	R	O	Z	V
3	A	H	O	U	N	E	Z	S	I	L
4	O	U	X	T	A	C	I	T	U	S

Tab. 27. Zápis otevřeného textu

Protože nejvyšší délka sloupce je 4, je vybráno heslo NOHA, což je v číselném vyjádření 3 4 2 1. Řádky tabulky se přetransponují:

	5	9	7	10	8	4	6	1	2	3
3	A	H	O	U	N	E	Z	S	I	L
4	O	U	X	T	A	C	I	T	U	S
2	A	H	N	O	U	T	R	O	Z	V
1	V	I	C	E	L	Z	E	D	O	S

Tab. 28. Transponovaná tabulka

Nyní jsou vypsány sloupce podle vodorovného hesla:

Šifrový text: STODI UZOLS VSECT ZAOAV ZIREO XNCNA ULHUH IUTOE

- Dvojitá transpozice

  Skládá se ze dvou jednoduchých tabulek a různými hesly. Otevřený text se nejprve zašifruje prvním heslem. Získaný text se potom šifruje druhým heslem.

Příklad:

Heslo 1 : 7 4 8 1 3 9 5 2 10 6

Heslo 2: 3 8 11 6 10 1 13 4 12 2 7 9 5

Zapsán otevřený text do tabulky s heslem 1:

7	4	8	1	3	9	5	2	10	6
K	D	O	P	R	O	K	A	Z	A
L	D	O	B	R	O	D	I	N	I
N	E	C	H	T	M	L	C	I	X
A	T	V	Y	P	R	A	V	I	T
E	N	K	T	E	R	Y	J	E	P
R	I	J	A	L	X	S	E	N	E
G	A	X	X	X					

Tab. 29. Dvojitá transpozice s prvním heslem

Poté do tabulky s heslem 2 zapisuje po řádcích shora dolů sloupec tabulky 1 podle jejího hesla:

3	8	11	6	10	1	13	4	12	2	7	9	5
P	B	H	Y	T	A	X	A	I	C	V	J	E
R	R	T	P	E	L	X	D	D	E	T	N	I
A	K	D	L	A	Y	S	A	I	X	T	P	E
K	L	N	A	E	R	C	O	O	C	V	K	J
X	O	O	M	R	R	X	Z	N	I	I	E	N

Tab. 30. Dvojitá transpozice s druhým heslem

Šifrový text získáme vypsáním sloupců druhé tabulky:

Šifrový text: ALYRR CEXCI PRAKX ADAOZ EIEJN YPLAM VTTVI BRKLO JNPKE TEAER HTDNO IDION XXSCX

- Zubatka

Navazuje na jednoduchou transpozici v tabulce. Jestliže je délka textu velká tak, že délka sloupců tabulky převyšuje délku hesla a rozdělí se sloupce tabulky na dvě části podle příslušné hodnoty hesla. Text vpisujeme po řádcích shora dolů a to do první části této tabulky a potom do části druhé.

Příklad:

Heslo: S E D M I K R A S K A

10 4 3 8 5 6 9 1 11 7 2

	10	4	3	8	5	6	9	1	11	7	2
1	V	P	R	A	T	E	L	S	T	V	I
2	N	E	L	Z	E	N	I	r	C	P	O
3	V	A	Z	O	V	A	T	i	Z	A	t
4	Z	H	a	O	U	B	N	k	E	J	a
5	S	v	a	I	N	E	Z	n	P	O	i
6	C	x	c	H	i	L	E	c	B	O	e
7	V	r	o	A	x	p	N	o	I	L	t
8	I	a	j	C	i	p	H	r	O	i	t
9	C	e	l	e	n	a	E	p	N	o	m
10	I	i	n	e	j	a	l	e	A	v	e
11	r	e	j	n	e	c	h	v	P	a	I
12	x	s	e	n	e	c	a	x	x	x	x

Tab. 31. Zubatka

Šifrový text: SRIKN CORPE VXIOT AIETT MELXR LZAAC OJLNJ EPEAH IESTE VUNIX INJEE ENABE LPAA CCVPA JOOLI OVAXA ZOOIH ACEEN NLITN ZENHE LHAVN VZSCV ICIRX TCZEP BIONA PX

- Cardanova mřížka

Mřížka je transpoziční klíč. Cardanova mřížka byla stabilní. Na určitých pozicích v mřížce jsou napsány znaky, které nepatří do otevřeného textu. Jsou to klamače a jsou zapsány malými písmeny, pro odlišení os otevřeného textu. Otevřený text se vpisuje do mřížek po řádcích a šifrový text obdržíme výpisem znaků po sloupcích. Mřížka má 63 okének a otevřený text je délky 55 písmen a 8 klamačů

Příklad:

N	I	C	N	u	E	N	I	T
A	K	o	T	E	Z	K	E	A
B	Y	S	E	e	T	O	H	O
D	A	R	E	B	A	i	C	T
V	I	a	M	N	E	D	O	S
y	A	H	L	O	X	P	E	e
T	R	O	N	I	a	U	S	X

Tab. 32. Cardanova mřížka

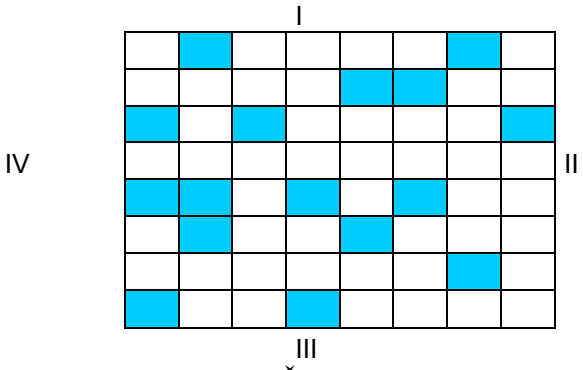
Šifrový text: NABDV YTIKY AIARC OSRAH ONTEE MLNUE EBNOI XANKO IDPUI EHCOE STAOT SEX

- Šifrovací mřížka – otočná mřížka

  Původní verze mřížky byla stabilní, její zdokonalenou formou je mřížka otočná. Mřížka musí být čtvercová a osově symetrická, má 8 x 8, tj. 64 políček. Protože se šifrovaný text vypisuje do mřížky ve čtyřech polohách, pokaždé pootočených o 90°, zabere každé políčko mřížky čtyři znaky. Políčka se v žádné další poloze nesmějí překrývat.

  Šifrování: Otevřený text je vepsán do čtverce velikosti mřížky po řádcích shora dolů, do každého pole jedno písmeno. Potom je přiložena mřížka v poloze I a po řádcích shora dolů vypisovány písmena. Mřížka se otočí do polohy II a opět jsou vypsány viditelná písmena a tak dále. Je-li otevřený text delší, je vytvořen další čtverec a pokračuje se stejným způsobem.

Příklad:



Obr. 7. Šifrovací mřížka

Otevřený text zapisuje do čtverce po řádcích:

K	D	E	J	E	P	O	T
L	A	C	E	N	A	S	V
O	B	O	D	A	L	I	D
U	T	A	M	P	R	E	S
T	A	V	A	S	V	O	B
O	D	A	S	L	O	V	A
X	P	U	B	L	I	L	I
U	S	S	Y	R	U	S	X

Tab. 33. Tabulka s otevřeným textem

Následně je přiložena mřížka. A výsledný text:

Šifrový text: DONAO ODTAA VDLLU YELSB ATRSB AXLIS RXETA DIAPE BSSKJ PCEVL UMVOS VPIU

3.4 Steganografické metody

Úkolem steganografie je skrýt samotnou existenci zprávy, zpráva přitom může byt napsána nebo předána ve srozumitelné podobě. Proto sem patří velké množství nejrůznějších technik pro utajený přenos zpráv.

3.4.1 Způsoby utajení zpráv

Během staletí byly použity stovky způsobů utajení. Tady jsou nejpoužívanější:

- použití neviditelného inkoustu
- vyznačení písmen v jinak nezávadném textu
- některá písmena v nezávadném textu byla propíchána špendlíkem, tato písmena tvořila utajený předávaný text
- některá písmena, v jinak nezávadném textu, jsou psána tučně či jiným sklonem
- ukrytí znaků otevřeného textu na domluvených pozicích
- prvá (druhá, poslední) písmena některých domluvených slov v dopise tvoří krátký utajený text
- text je napsán na předem domluvená místa a je obklopen nezávadným textem, příjemce přiloží dešifrovací tabulku a přečte si předávaný text
- zápis šachové partie
- zmenšení textu
- použití mikroteček

3.4.2 Agenturní systém

Systém lze řadit mezi typické steganografické metody. Oblíbený byl na obou stranách železné opony v době studené války. Byl využíván i v době totality při komunikaci mezi agenturní sítí v České republice a jejím řídícím centrem v cizině. Měl podobu nenápadných dopisů odesílaných z ČR na smluvené adrese v cizině. V textu bylo na domluveném místě – například konec druhého slova v každé větě, poslední slovo věty apod. písmeno otevřeného textu.

Příklad:

Otevřený text :	Kdo jinému jámu kopá, sám do ní padá
Pravidlo pro utajeni:	Otevřený text tvoří písmena slov odeslaného textu
Výsledný text:	„*K*arel *d*nes *o*djížděl. *J*indřich *i* *N*ataša *E*sterové *m*u *u*vařili *j*ídlo. *A* *m*oc *už* *k* *o*djezdu *p*ospíchal *a* *s*pěchal. *A* *m*usel *d*ocela *o*kamžitě, *n*ikoliv *i*deálně *p*obalit *a* *d*át *á*dijé.“

3.4.3 Neviditelné inkousty

Je to základní steganografická metoda. Zapsaný text není při běžném pohledu viditelný. Příjemce zobrazí neviditelný text známým způsobem například zahřátí, působení nějakou chemikálií nebo osvícení ultrafialovým, infračerveným světlem. Velmi se to uplatňovalo jako zpráva z vězení.

Typy inkoustu tvoří skupina organická jako je moč, mléko, ocet atd. Text zvýrazníme mírným zahříváním. Další skupinou jsou chemické látky. Například nasycený roztok dusičnanu draselného, který zanechá na papíru po odpaření malé bezbarvé krystalky a ty jakmile dojde k zahřátí, zuhelnatí. Nebo jiným příkladem může být chlorid kobaltnatý. Jako hydrát je jen slabě růžový, takže na papíru není téměř vidět, až po zahřátí. Třetí skupinou je využití chemických reakcí k zviditelnění písma. Například píše-li špión síranem železnatým, nebude nic vidět, dokud text nepotřeme kyanidem sodným. Poslední skupinu tvoří neviditelné inkousty, které aby byly zviditelněny, používají ultrafialové nebo infračervené záření. Získání záření můžeme pomocí lampiček na ověřování bank nebo z horského sluníčka či UV lampa.

Umění výroby dokonalého neviditelného inkoustu spočívá v nalezení sloučeniny, která bude reagovat s co nejmenším počtem chemikálií. Při testech na neviditelný inkoust se používaly „vývojky“

Vybrané příklady:

Inkousty vyvolané teplem

- Modré písmo: 1 g chloridu kobaltnatého a 2 g glycerinu se rozpustí v 90ml vody.
- Černé písmo: 1 g kyseliny sirové a 2 g cukru se rozpustí ve 100ml vody.

Inkousty vyvolané chemickou reakcí

- Černé písmo: 1 g octanu olovnatého se rozpustí v 25 ml vody. Písmo se vyvolá sirovodíkem
- Červené písmo: 5g chloridu železitého se rozpustí v 25 ml vody. Vyvolá se slabým okyselením roztokem rhodanidu draselného.

Inkousty viditelné v UV záření

- Jeden acylpyrin se rozpustí ve 2 ml vody a přidá se trochu hydroxidu sodného. Směs zahřejeme a za stálého protřepávání se udržuje ve varu minimálně jednu minutu. Po ochlazení se přidá 2 ml octa.

4 TVORBA KLÍČE A HESLA

Holandský kryptolog Auguste Kerckhoffs (1835-1903) ve své knize *Vojenská kryptologie* uvádí, v jedné ze zásad na požadavek dobrého šifrového systému toto:

Vyzrazení systému nesmí mít nepříjemné následky pro dopisovatele.

4.1 Klíč

V minulosti se šifrovalo velice jednoduchými metodami, kde bezpečnost často závisela pouze na utajení metody. Např. bezpečnost Caesarovy šifry, která převádí otevřený text na šifrový tak, že každé písmeno otevřeného textu nahradí písmenem, který leží 3 místo od něj vzdálené v abecedě. Je tedy samozřejmé, že jde o to, zda systém zná i osoba, která se snaží získat otevřený text, který pro ni není určen. Pokud tato neoprávněné osoba dešifruje zprávu a zjistí, že je tento systém používaný ke komunikaci, pak je jasné, že šifra je prolomena.

Pokud bychom šifru jen nepatrně změnily a to tak, že by posun nebyl 3 znaky, ale byl by různý, zjistíme, že se situace výrazně změnila. Protože luštitel může vyluštit konkrétní zprávu, ale nemá jistotu, že vyluští i ty další. Parametry šifrového systému, které lze změnit, a mají vliv na výsledný šifrový text, se nazývají klíč.

4.2 Heslo a jeho vytvoření

V době, kdy se používaly především polní vojenské šifry, tak klíčové hospodářství bylo velmi jednoduché. Důležité tedy bylo, aby vojáci vytvářeli klíče k šifrám kvalitní a dostatečně dlouhé. Další podmínka byla, aby klíče byly zapamatovatelné.

Postup při vytvoření hesla můžeme zmínit v knize Řeka Aineia Taktika *Obrana opevněných míst*, ze 4. století př. n. l. Autor zde radí římským vojákům, aby hesla byla co nejvíc zapamatovatelná a svým významem co možná nejblíže zamýšlené akci. Tedy na kvalitu hesla se moc nehledělo a přednost měla zapamatovatelnost.

Na tvorbu hesla existuje spousta doporučení a návodů. Jednou z nich je použití slova, které není ve slovníku daného jazyka nebo datum, pro nás důležité události a doplnění o nějaké písmeno. Existuje metoda motivu a výpočtu hesla.

Příklad:

motiv Mrazík – Ivanova píseň „Před naší za naší, cesta má ať se nepráší, hej“

odvozené heslo: Pnzncmanh

Není problém v tomto příkladě doplnit ještě číslice či střídat písmeno, pro větší bezpečnost.

5 TAJEMSTVÍ KRYPTOANALÝZY

V této kapitole si představíme kryptoanalytický útok na systém a obecné dešifrování některých vybraných systémů.

5.1 Kryptoanalytický útok

- dešifrování se znalostí zašifrovaného textu (základní úloha) - je k dispozici šifrový text několika zpráv, které byly zašifrovány stejným šifrovacím algoritmem, úkolem je odvodit klíč (nebo klíče) použitý k zašifrování.
- dešifrování se znalostí přímého textu - je k dispozici zašifrovaný text, ale i odpovídající otevřený text.
- dešifrování se znalostí vybraných otevřených textů - k dispozici zašifrovaný a odpovídající otevřený text, ale jsou k dispozici otevřené texty, které lze šifrovat (vybrané bloky).
- adaptivní metoda luštění se znalostí vybraných otevřených textů - výběr bloků otevřeného textu na základě výsledků získaných prvým výběrem.

Mezi základní znalosti patří:

- frekvence výskytu písmen je odlišná u různých jazyků.
- použití polyalfabetické šifry vede (v závislosti na délce klíče) ke zploštění frekvence výskytu písmen.
- dešifrování nemusí dát jednoznačný výsledek, např. pro Vigenérovu šifru a šifrovaný text.

Mezi základní metody patří:

- statistická analýza výskytu písmen resp. skupin písmen v textu různých jazyků - podklad pro využití koeficientu koincidence, u dosti dlouhého textu a monoalfabetické šifry porovnat frekvenci výskytu znaků přímého textu a šifrovaného textu.
- zjištění koeficientu koincidence - rozlišení monoalfabetická / polyalfabetická šifra + zjištění (odhad) délky klíče.
- u monoalfabetických caésarovských šifer stačí určit ekvivalent jediného znaku.

5.2 Analýza substitucí

5.2.1 Kryptoanalýza monoalfabetických šifer

Spočívá ve vyhledávání typických shluků znaků pro daný jazyk, typických prvních / posledních znaků slov a četnost výskytu jednotlivých znaků neboli *frekvenční analýza.* Je založena na vlastnostech jazyka.

- Pořadí hlásek v češtině:

  E,O,A,I,N,S,T,R,V,U,L,Z,D,K,P,M,C,Y,H,J,B,G,F,X,W,Q

- Pořadí hlásek v češtině na začátku slov:

  P,S,V,Z,N,T,O,J,K,D,A,B,M,R,U,C,I,H,E,L,F,G,W,Y,Q,X

- Pořadí hlásek v češtině na konci slov:
  E,I,A,O,U,Y,M,T,H,V,L,K,S,Z,D,N,R,C,J,B,P,G,F,W,X,Q

- Bigramy ST, PR, SK, CH, DN, TR

  Zvláštnosti souhláskových bigramů v češtině:

  - ST: S a T má přibližně stejnou frekvenci existuje i bigram TS

    Je součástí velkého počtu souhláskových trigramů (STR, STN, STL, STV)

    vyskytuje se uprostřed i na konci slova.

  - PR: P má asi poloviční frekvenci než R. Obrácený bigram RP se téměř nevyskytuje (chrpa). Zpravidla nelze rozšířit „dozadu“ na souhláskový trigram (PRV). Lze rozšířit dopředu na samohláskový trigram (SPR, ZPR,…). Zpravidla stojí na počátku slov.

  - CH: H má jen o něco menší frekvenci než C(u kratších textů nemusí platit). Bývá zpravidla na konci slov spolu se samohláskami Y,I,A,E (YCH, ICH, ACH, ECH) Většinou platí: předchází-li CH souhláska, pak je po něm samohláska a naopak (OBCHOD, NECHŤ).

  - Trigramy**:** PRO, UNI, OST, STA, ANI, OVA, YCH, STI, PRI, PRE, OJE, REN, IST, STR (nejběžnější souhláskový trigram!), EHO, TER, RED, ICH.

5.2.2 Kryptoanalýza polyalfabetických substitucí

Základem je určení počtu použitých substitucí, dále dokument rozdělíme na části, šifrované stejnou substitucí a na tyto části použijeme postupy analýzy monoalfabetických šifer. Určování počtu použitých substitucí

- Kasiského metoda

  pokud se v otevřeném textu vyskytuje *k*-krát stejný řetězec znaků a k šifrování bylo použito *n* substitucí, které se cyklicky střídají, bude daný řetězec zašifrován přibližně *k/n* krát stejně. Prohledáváme zašifrovaný text na výskyt opakujících se řetězců (délky aspoň 3). Zjistíme vzdálenosti začátků jednotlivých řetězců. Ke každé vzdálenosti získané v předchozím bodě vytvoříme seznam všech dělitelů tohoto čísla. Počet použitých substitucí by měl odpovídat některému z často se vyskytujících dělitelů.

- Index koincidence

  označme $Freq_i$ počet výskytů symbolů *i* ve zprávě. Index koincidence IC definujeme:

$$IC = \sum_{i=a}^{i=z} \frac{Freq_i * (Freq_i - 1)}{n * (n-1)}$$

  Pokud má odpovídající otevřený text rozložení znaků blízké normálu, lze z *IC* usuzovat na počet použitých substitucí. Složitost analýzy polyalfabetických šifer roste s počtem použitých substitucí. Je třeba použít každou substituci jen jednou

5.2.3 Kryptoanalýza transpozičních šifer

Jednoduchá transpozice. Je-li k dispozici pouze jeden šifrový text dané délky, nezbývá než jej přehazovat za použití častých bigramů tak, aby se dostal smysluplný text. Je-li k dispozici více textů téže délky zašifrované stejnou permutací, pak jsou napsány pod sebe,

rozstřiženy do sloupců a přeházeny opět tak, aby se ve všech řádcích současně dostaly smysluplné texty.

V případě *úplné tabulky* se může její rozměr najít tak, že se vyzkouší všechny možné tabulky, které lze celé vyplnit šifrovým textem dané délky. Pro každou možnost je spočítáno poměr samohlásek a souhlásek v jednotlivých řádcích. Tabulka, pro kterou se tyto poměry nejvíce blíží poměru samohlásek a souhlásek v přirozeném jazyce otevřeného textu, je ta nejpravděpodobnější. Text si potom rozstříhán do sloupců a pokračuje se stejně jako u více textů téže délky.

Při více textech téže délky postupujeme na počátku stejně jako u jednoduché transpozice. Pokud uspějeme, je třeba najít ještě obě hesla, abychom mohli luštit i zprávy jiných délek.

6 NEJVĚTŠÍ ŠIFROVACÍ ZÁHADA – ENIGMA

Enigma – německá „neprolomitelná“ šifra. Byl to první skutečný mechanicko-elektronický šifrovací stroj. Autor myšlenky byl Artuhur Scherbius[16]. Používala se za 2 světové války. Má mnoho variací a verzí, které jsou civilní, státní a vojenské.

Základní princip spočíval v mechanizaci klasické polyalfabetické šifry a odolnost proti frekvenční analýze zvýšena používáním „scramblerů“[17], které v průběhu kódování mění převodní funkci mezi abecedami.

Princip fungování jednoduché:

Enigmy spočíval v zjednodušené verzi pro abecedu s 6 znaky, po stisku klávesy se na signální desce rozsvítí patřičný znak odpovídající posunutí v rámci monoalfabetické šifry. Po uvolnění klávesy se „scrambler“ pootočí o 1/6 kola. Stejné písmeno je kódováno šesti různými způsoby (a), (b), (c) - to vytváří duplicitu, která je nežádoucí.

Princip fungování vojenské Enigma:

Enigma používala způsobem, že pro každý den existovalo v kódové knize zapsané zapojení propojovací desky, pořadí a orientace scramblerů. Operátor nastavil Enigmu do příslušného stavu, náhodně vybral trojici písmen a tu odeslal podle denního klíče. Potom přenastavil scramblery podle výše zmíněného pořadí náhodně vybraných písmen a kódoval samotnou zprávu. Příjemce pouze dekódoval nastavení scramblerů podle začátku zprávy, nastavil svůj stroj a mohl dekódovat zprávy. Počet „scramblerů“byl zvýšen na tři, které bylo možno permutovat. Následně přidána propojovací deska (pro 6 párů písmen) a přidán reflektor, který zdvojnásobil průchod scramblovacím ústrojím (bez vlivu na zvýšení počtu šifrovacích abeced), zjednodušil technickou konstrukci a umožnil na stejném stroji šifrovat i dešifrovat. Výsledný počet možných klíčů po všech úpravách byl 1015.

---

[16] Artuhur Scherbius – (20. října 1878 do 13 května 1929) byl německý elektrotechnik , který patentovaný vynález pro mechanické šifry stroj, později prodávány jako stroj Enigma.

[17] Scrambler - je zařízení, které přenese nebo převrátí signály nebo jinak zakóduje zprávu.

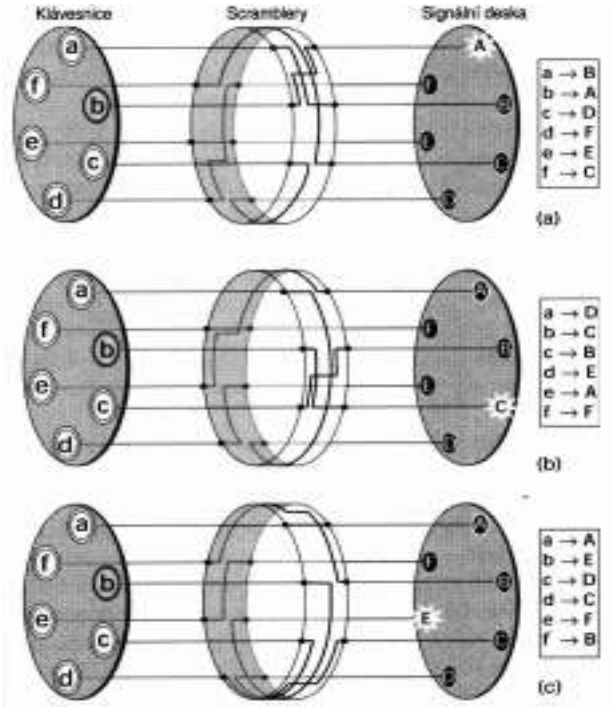
Obr. 8. Enigma

Boj s Enigmou podstoupil Marian Rejewski[18] a měl k dispozici:

- vlastnil vojenskou verzi Enigmy
- odposlech německé šifrované komunikace
- neomezené finanční a lidské zdroje

Princip analýzy tedy opakování vede k zákonitostem – v případě Enigmy se opakovaly první tři znaky (náhodného rozložení scramblerů) dvakrát – kvůli možným chybám. Dále vytvoření řetězců písmen, které se na sebe přepisovaly tzv. tabulka vztahů – každý den jiná. Následně vylučovacím způsobem dospěl k eliminaci počtů klíčů na 105 456 pro každý den a tyto možnosti bylo třeba vyzkoušet. Z úspěšného dešifrování se dal odvodit daný denní klíč. Celková doba potřebná k prolomení „neprolomitelné“ šifry byl 1. rok.

[18] Marian Rejewski - polský matematik a kryptolog



Obr. 9. Princip zjednodušené Enigmy

ZÁVĚR

Klasická kryptologie vznikla spojením kryptografie, kryptoanalýzy a steganografie. Tyto obory spolu úzce souvisejí, a tak je prakticky nemožné se věnovat jen jedné z nich. Kryptografie se zabývá šifrovacími postupy, kryptoanalýza se zabývá luštěním a dešifrováním a steganografie spočívá v ukrytí samotné existence zprávy.

Velmi důležitou roli v kryptologii hraje historie. Je nedílnou součástí této vědy. Všechny úspěchy a neúspěchy nás posouvají dál. Abychom pochopili smysl klasické kryptologie je nutné se dívat do minulosti

V práci byla věnována velká pozornost rozčlenění kryptologických kódů a šifer. Je jich totiž velké množství a snadno se v nich dá ztratit. V oblasti kódování jsou na špičce pomyslného žebříčku Braillovo písmo a Morseova abeceda. U šifer je to složitější, v zásadě byly objasněny tyto šifrovací systémy. První systém byl substituční, který se dál rozděluje na podsystémy monoalfabetická substituce, polyalfabetická substituce, polygrafická substituce a na sekci ostatní substituce. V tomto šifrovacím systému je uvedeno velké množství šifer, jak jsou správně rozděleny, jak je poznáme a v neposlední řadě jak se šifrují. Jsou zde uvedeny pro názornost příklady. Druhým systémem je transpoziční systém. Ten je definovaný šiframi, které jsou založeny na určitém geometrickém postupu. I zde je uvedeno velké množství vysvětlení a příkladů.

Dále bylo uvedeno použití steganografických metod, které jsou rozděleny, vysvětleny a v neposlední řadě jsou uvedeny i zajímavosti.

Důležitým prvkem klasické kryptologie jsou taky klíče a hesla. Jsou zde uvedeny správné postupy jak klíč změnit, aby šifra byla složitější. Klíče jsou vlastně parametry, kterými měníme šifrový systém. Tvorba hesla je popsána ve spoustě knih. Jedná se o to, aby heslo, které se používá, nebylo příliš primitivní. Jsou zde vysvětleny postupy a příklad jak udělat heslo složitější.

Analýza byla nastíněna trochu obecnějším výkladem a to pro monoalfabetické šifry, polyalfabetické šifry a transpoziční šifry.

V nepolední řadě byla v práci zařazena jedna neodmyslitelná událost a zároveň zajímavost ze světa kryptologie, která se věnuje rozluštění šifrovacího přístroje Enigma.

Doufám, že bakalářské práce poslouží i pro vzdělávací účely. Jak část teoretická, praktická tak i prezentace, které byly zpracovány k zadanému tématu.

ZÁVĚR V ANGLIČTINĚ

Typical cryptology originated by unification of cryptology, cryptanalysis and steganography. This subject areas are closely connected and it is almost imposible to focus on the only one.

The cryptology is based on the cipher progress, the cryptanalysis engages with decoding and deciphering and steganography lies in hiding the existence of message.

History is the very important part of the cryptology and also belongs to this science. Every success and every failure moves us further. It´s necessary to look into the past to understand the sense of the typical cryptology.

My piece of work is focused on dividing of cryptological codes and ciphers. There is a lot of that and it is very easy to be confused by that.

There is The braille and The morse code highly ranked in the area of the coding. It is more difficult with the ciphers and the cipher systems was clarified principally. The first system was interchangeable. It is divided into the subsystems like monoalphabetic substitution, polyalphabetic substitution, polygraphic substitution and the others. There are mentioned the examples of this cipher system, their correct separation, the way how to recognize them and also how to cipher them.

Here are some examples mentioned for the clearness. The second system is transpisitional system that is defined by the ciphers based on specific geometrical technique. Many explanations and some examples are also mentioned here. There are launched the use of steganographical methods which are divided, explained and last but not least the interests are brought out.

Very important element of the typical cryptology are keys and passwords. Here are mentioned correct methods how to change key, to make cipher to be more difficult. The keys,in fact, are the parametres used for changing the cipher system.

The creation of password is described in lot of books. That concerns the fact that the password should not be too primitive. The methods and the examples how to set up more difficult passwords are explained here.

Analysis was outlined by rather general interpretation for monoalphabetic, polyalphabetic and transpisitional ciphers.

Even the coding device The Enigma, one of the most important events and parts from the world of cryptology is dropped in my paper.

I hope my piece of work will serve for educatinoal purposes. Both the theory and the practical part and also the prezentation I put together for selected topic.

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1] SINGH, Simon. Kniha kódů a šifer. Argo, 2003. ISBN: 80-7203-499-5.

[2] JANEČEK, J. Odhalená tajemství šifrovacích klíčů minulosti. Naše Vojsko, 1994.

[3] VONDRUŠKA, P. Kryptologie, šifrování a tajná písma. Albatros, 2006.ISBN 80-00-01888-8.

[4] HANŽL, T. Šifry a hry s nimi. Portál, 2007. ISBN 978-80-7367-196-9

[5] KATZ, Jonathan. Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall, 1 edition. 2007. 552 s. ISBN 978-1584885511.

[6] MURPHY, Sean. Kryptografie – Průvodce pro každého. Dokořán, 2006. 157 s. ISBN 80-7363-074-5.

Internetové zdroje:

[7] Tajemství šifer – po stopách kryptografie a steganografie. [online] 2008 [cit. 2010-03-08]. Dostupný z WWW: <http://www.velkaepocha.sk/200806125316/Tajemstvi-sifer-po-stopach-kryptografie-a-steganografie.html>.

[8] Historie kryptografie a kryptoanalýzy. [online] [cit. 2010-03-11]. Dostupný z WWW: < http://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7022>

[9] Morseova abeceda. [online] 2006 [2010-04-06]. Dostupný z WWW:

<http://www.shaman.cz/sifrovani/morseova-abeceda.htm>

[10] Braillovo písmo. [online] 2005 [cit. 2010-04-06]. Dostupný z WWW:

<http://www.shaman.cz/sifrovani/braillovo-pismo.htm>

[11] Caesarova šifra. [online] 2005 [cit. 2010-04-14]. Dostupný z WWW: <http://www.shaman.cz/sifrovani/cesarova-sifra.htm>

[12] Baconian Cipher. [online] [cit. 2010-04-16]. Dostupný z WWW: <http://www.purplehell.com/riddletools/bacon.htm>

[13] Dvojí použití klíče. [online] [cit. 2010-05-05]. Dostupný z WWW: <http://www.karlin.mff.cuni.cz/~tuma/ciphers08/sifry2.ppt>

[14] Základy kryptoanalýzy. [online] [cit. 2010-05-16]. Dostupný z WWW: <http://www.referaty10.com/referat/Informatika/1/tema-1-20-Informatika.php>

[15] Úvod do klasických a moderních metod šifrování [online] 2009 [cit. 2010-05-16]. Dostupný z WWW: <http://www.karlin.mff.cuni.cz/~tuma/ciphers09/sifry2_09.ppt>

[16] Kryptologie – aneb šifry včera, dnes a zítra. [online] 2009 [cit. 2010-03-11]. Dostupný z WWW: <petrhanus.webovka.eu/download/kryptologie.pdf>

[17] 1. přednáška – Úvod, termíny, historie. [online] 2009 [cit. 2010-04-25]. Dostupný z WWW: <www.comtel.cz/files/download.php?id=4795 >

[18] Kryptografie a počítačová bezpečnost. [online] 2009 [cit. 2010-05-21]. Dostupný z WWW: <http://www.cs.vsb.cz/ochodkova/courses/kpb/KPB1_10.pdf>

[19] Kryptografie. [online] [cit. 2010-05-21]. Dostupný z WWW: <http://pef.czu.cz/~halbich/predn2.ppt>

[20] Základy kryptoanalýzy. [online] [cit. 2010-05-21]. Dostupný z WWW: <http://www.saturka.cz/uhk/obdai/zkouska/OBDAI%20-%2010%20-%20Z%E1klady%20krypt>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

atd. A tak dále

př. n. l. Před naším letopočtem

např. Například

SEZNAM OBRÁZKŮ

SEZNAM TABULEK