Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Bakalářská práce

2008 **David Prokopič**

Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví

Studijní obor: informační studia a knihovnictví

David Prokopič

Historie šifrování od starověku do novověku

Bakalářská práce

Praha 2008-05-01

Vedoucí bakalářské práce: Doc. RNDr. Jiří Ivánek, CSc.

Oponent bakalářské práce:

Datum obhajoby:

Hodnocení:

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a že jsem uvedl všechny použité informační zdroje.

V Praze, 1. května 2008

……..

podpis studenta

Identifikační záznam

PROKOPIČ, David. Historie šifrování ve starověku a středověku [History of cryptography from antiquity to middle ages]. Praha, 2008-05-01. 52 s. Bakalářská práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí bakalářské práce Jiří Ivánek.

Abstrakt

Práce nejdříve definuje obor kryptografie a další termíny, které s ní bezprostředně souvisí. Poté popisuje stručný přehled vývoje kryptografie v období starověku a středověku a naváže popisem jednotlivých metod, v závěru shrne a vyhodnotí vývoj za dané období.

Klíčová slova:

kryptografie, kryptologie, kryptoanalýza, historie, starověk, středověk, kódování, šifrování

OBSAH

1. PŘEDMLUVA

Šifrování je dnes nedílnou součástí každodenní komunikace. Člověk už ani nevnímá, kolik informací, se kterými především v prostředí internetu pracuje, je v šifrované podobě, i když v jejich počáteční a finální fázi to není poznat.

Co však stálo na jejich začátku a kam až sahá jejich historie ví dnes málokdo. Kdekdo si vzpomene na Caesarovu šifru, či legendární Enigmu, ale dokáže Vám uvést i jiné metody, či vysvětlit přesný princip a okolnosti?

S šiframi jsem se poprvé setkal jako dítě ve skautském oddíle v rámci všemožných her a na základní škole, kdy jsme si posílali tajné zprávy mezi spolužáky pomocí vlastní, jednoduché substituční šifry, či inspirováni Tolkienovým dílem jsme komunikovali runami, které byly pro drtivou většinu spolužáků nečitelné. Už tehdy nám byl účel šifer jasný, skrýt obsah před nežádoucími čtenáři. Dlouhou dobu jsem se jimi potom nezabýval, teprve až na vysoké škole se opět dostaly mé pozornosti při výběrových přednáškách Internetová kriminalita a Kódování a šifrování. Hlavně díky těmto předmětům byla poté pro mne při výběru témat na bakalářskou práci Historie šifrování jasnou volbou.

Dalším důvodem byl i fakt, že je to téma velmi zajímavé a přitažlivé. Jak už jsem poznamenal na začátku, šifrování informací patří dnes ke každodennímu životu a rozhodně není na škodu vědět něco i o jeho historii.

Původní název této bakalářské práce byl Historie šifrování v průběhu vývoje lidstva. Toto téma by bylo však příliš rozsáhlé na bakalářskou práci. Proto jsem se po konzultaci s vedoucím práce rozhodl téma zúžit na první dvě epochy psané historie lidstva.

Cílem práce je zmapovat a popsat co nejpodrobněji metody šifrovaní (ale i zmínky o nich) z období starověku a středověku, včetně příkladů a historického kontextu a v závěru pak shrnout jejich vývoj, návaznost a kontext.

Práce je seřazena tak, že po teoretickém a terminologickém úvodu je stručně popsán a sumarizován vývoj v obou epochách. Následuje podrobný popis jednotlivých

kryptografických metod. Nejedná se o úplný výčet, ale o doložené metody, či díla, které byly nové a historicky významné.

Vzhledem k velkému počtu pramenů a drtivé většině elektronických zdrojů, převážně v anglickém jazyce, jsem se kvůli přehlednosti rozhodl nepoužívat doslovné citace, ale text parafrázovat a ke každé kapitole v poznámce pod čarou přiřadit čísla zdrojů z číslovaného seznamu použité literatury, který je zpracován dle norem ISO 690 a ISO 690-2.

.

2. ZÁKLADNÍ POJMY KRYPTOLOGIE

Kryptologie jakožto věda o utajení obsahu se stále drží v podvědomí lidí jako něco tajemného, pro normálního člověka neuchopitelného. Dokonce tomu není tak dávno, kdy se knihy o kryptografii a kryptologii daly v knihovnách najít na regálech společně s knihami o alchymii a hvězdopravectví.

V oficiálním třídění matematických věd také nebyla kryptologie dlouho uvedena a byla tak trochu skryta ve stínu mezi matematikou a informatikou.

Kryptologie, jako vědní obor, se dále dělí na kryptografii a kryptoanalýzu a často se do ní zahrnuje i steganografie.

Ve starších podáních byla kryptografie především obor, zabývající se převedením informace do podoby, v níž je vlastní obsah informace skryt. Úkolem kryptografie je tedy především učinit konečnou zprávu nečitelnou i za situace, kdy je plně prozrazená a zachycená třetí (nepovolanou) stranou. Tím se liší od steganografie, jejímž úkolem je skrýt samotnou existenci zprávy, ale samotná zpráva může být klidně napsána nebo předána ve nešifrované podobě.

Odborně řečeno: Kryptografie se zabývá matematickými metodami vztahujícími se k zjištění aspektů informační bezpečnosti jako je důvěrnost, integrita dat, autentizace entit a původ dat.

Kryptoanalýzu pak můžeme považovat za opačný ekvivalent kryptografie. Snahou kryptoanalytiků je získání původní podoby ze zašifrované zprávy, nebo alespoň část skrytých informací. Kryptoanalýza se tedy zabývá analýzou odolnosti (síly) kryptografického systému a metodami, které vedou k průniku do těchto kryptografických systémů. Tomuto procesu se říká luštění šifrové zprávy. Pokud je kryptoanalytik úspěšný a povede se mu proniknout do některého šifrového systému, říkáme, že šifra byla prolomena či rozbita.

Základním cílem kryptografie je tedy rozvoj algoritmů, které je možno použít ke skrytí obsahu zprávy před všemi s výjimkou odesílatele a příjemce. O mnoho později také přibyl rozvoj algoritmů sloužících k jednoznačné identifikaci osoby odesílatele a k ověření správnosti (autentizaci) zprávy příjemcem a další související algoritmy.

Originální vysílanou zprávu nazýváme otevřeným či prostým textem. Tato zpráva je následně zašifrována pomocí nějakého kryptografického algoritmu. Takto zašifrované zprávě říkáme šifrový text. Dešifrování je opačný postup ve vztahu k zašifrování, je to převedení šifrového textu zpátky do původní podoby otevřeného textu.[1]

2.1. Kryptologie

(Z řeckého kryptós (skrytý) a lógos (slovo)), je vědní disciplína, která se zabývá bezpečnou a tajnou komunikací, tedy věda utajení zpráv všemi formami, zahrnuje kryptografii a kryptoanalýzu.

2.2. Kryptografie

(Z řeckého kryptós (skrytý) a gráphein (psát)), věda o šifrování zpráv, je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí. Někdy je tento pojem obecněji používán pro vědu o čemkoli spojeném se šiframi jako alternativa k výše uvedenému pojmu kryptologie.

2.3. Kryptoanalýza

(Z řeckého kryptós (skrytý) a analýein (uvolnit, či rozvázat)), věda o tom jak bez znalosti klíče (a tajných informací, které jsou za běžných okolností potřeba) odvodit a získat původní text ze šifrovaného. Kryptoanalýza se tedy zabývá rozbíjením šifer samotných, získáváním klíče a pokusy o prolomení kódu zašifrovaného textu. Jde vlastně o opak kryptografie, která šifry vytváří.

2.4. Steganografie

(Z řeckého steganós (schovaný) a gráphein (psát)), nauka o skrývání existence zpráv samotných. Zpráva je ukryta tak, aby si pozorovatel, který zprávu zachytil, neuvědomil, že nějaká komunikace vůbec probíhá. Pokud zprávu zaregistruje / zachytí je steganografie prolomena. Rozdíl oproti kryptografii je ten, že steganografie se snaží skrýt existenci zprávy, kdežto kryptografie její obsah, proto se často steganografie s kryptografií kombinuje.

[1] - 1, 27, 44, 51, 69, 77

2.5. Šifra (šifrování)

Z arabského sifr (nula), obecně jakýkoli systém pro ukrytí smyslu zpráv tak, že je každé písmeno v původní zprávě nahrazeno jiným znakem. Jde tedy o kryptografický algoritmus (proces transformace), který převádí čitelný (otevřený) text na nečitelný, neboli šifrový text a naopak.. Tento systém by měl mít zabudovanou flexibilitu, známou jako klíč.

2.6. Kód (kódování)

Systém pro ukrytí smyslu zprávy. Nahrazuje slovo, pojem, označení či frázi v původní zprávě jiným znakem, či skupinou znaků. Je to postup, při kterém narozdíl od šifrování nepoužíváme heslo. Seznam, kde jsou kódy (kódová slova, kódová čísla) uveden, se nazývá kódová kniha. Obsah zakódované zprávy tedy může zjistit každý, kdo zná (či vlastní) kódovu knihu.

2.7. Klíč

Prvek, který změní obecný šifrovací algoritmus v ojedinělý postup šifrování – určuje pro něj logický postup. Laicky řečeno: Tajná informace, kterou se otevřený text šifruje a bez které nelze šifrový text přečíst. Nežádoucí osoba může tedy znát šifrovací metodu použitou odesílatelem a příjemcem, ale nesmí znát klíč.

2.8. Substituční šifra

Jednoduchý systém šifrování, ve kterém je každé písmeno zprávy dle určitého pravidla nahrazeno jiným, avšak pokaždé stejným znakem. A ve zprávě si zachovává svou pevnou pozici.

Monoalfabetická substituční šifra
Substituční šifra, ve které je (jedna) šifrovací abeceda pěvně určena po celou dobu šifrování.

Polyalfabetická substituční šifra
Substituční šifra, ve které se šifrová abeceda mění v průběhu šifrování a používá (střídá) rozmanité substituční abecedy. Tato změna je definována klíčem. K usnadnění šifrování se často šifrovací abecedy zapisovaly do speciálních tabulek.

Homofonní substituční šifra
Substituční šifra, v níž existuje pro určitá písmena otevřeného textu (zpravidla těch nejfrekventovanějších) několik možných substitucí. Například nejčastěji se vyskytující znak „E“ by mohl být nahrazen znaky 77, F, P, 3 atd. Počet znaků zašifrovaného textu pro jeden znak otevřeného textu se může lišit.

Posunová šifra
Substituční šifra, kdy každé jednotlivé písmeno tajné zprávy se posunuje v abecedě o pevný, předem určený počet pozic v předem určeném směru.

2.9. Transpoziční šifra

Šifrovací systém ve kterém se každé písmeno zprávy přemístí na jiné místo, ale zachovává si svou totožnost (zůstává nezměněno). Tyto šifry jsou tvořeny přesmyčkami, jde o prohození znaků v předem daných sledech (posunech). Jde například o čtení textu ve spirále, křížem, pozpátku, po sloupcích atd.

2.10. Kombinovaná šifra

Poslední fází většinou bývá spojení různých metod šifer dohromady (a jejich zpětné dešifrování předem známým způsobem). Touto kombinací se dají částečně odstranit některé nevýhody či slabiny jednotlivých šifer

2.11. Otevřený text

Též nazývaný prostý text, je původní zpráva před procesem šifrování.

2.12. Šifrový text

Zpráva (otevřený text) po zašifrování.

2.13. Frekvenční analýza

Analyzuje formální strukturu textu, je založena na měření četnosti výskytů písmen, skupin písmen, slov či slovních spojení. Frekvenční analýza vychází z předpokladu, že lze usuzovat obsah na základě četnosti výrazů s vyšší frekvencí. Laicky řečeno: pokud se frekvence užití jednoho konkrétního písmena v šifrovém textu blíží (nebo rovná) frekvenci jiného písmena užívaného v „normální“ řeči je velmi pravděpodobné, že se jedná o jedno a totéž písmeno (jeho ekvivalent v otevřeném textu). Metoda se využívá jako pomoc při rozbíjení klasických šifer.

2.14. Algoritmus

Princip řešení problému, nebo přesný návod či postup, kterým lze vyřešit daný typ úlohy. Odborně řečeno: „Posloupnost konečného počtu elementárních kroků vedoucí k vyřešení úlohy.“

2.15. Anagram

Anagram, neboli přesmyčka je nové slovo, které vznikne z původního slova tak, že se použijí všechna písmena (či jen slabiky) ve slově obsažená a změní (přeskupí) se jejich pořadí.

2.16. Logogram

Logogram je jediný napsaný znak, který reprezentuje (zastupuje) kompletní gramatické slovo. Logogramy jsou například číslice 1 = jedna, znaky čínské abecedy či běžně užívané klávesové znaky jako % = procento, & = and atd.

2.17. Kryptogram

Kryptogram je šifrovaný text (nebo větný útvar), jehož písmena či slova mají skrytý význam. Například ve větě „Dobré poledne Arnolde!“ je kryptogram slovo dolar.

[2]

[2] - 53, 61, 63, 65, 67, 89, 90, 91

3. HISTORIE KRYPTOGRAFIE STAROVĚKU A STŘEDOVĚKU

Již od dávných dob vládci, králové a vojenští hodnostáři spoléhali na rychlé a účinné dorozumívací systémy, které jim umožňovaly vládnout jejich zemím a velet jejich armádám. Tito lidé si však museli být také vědomi své odpovědnosti a toho, jaké následky by mělo, kdyby jejich zprávy s životně důležitými informacemi padly do rukou nepovolaných. Museli si uvědomovat například riziko vyzrazení cenných tajemství cizincům, odhalení zásadních informací nepříteli či technologické postupy, které dávaly svým „vlastníkům“ oproti ostatním výhodu. Právě tato rizika byla hlavním hnacím motorem rozvoje kódů a šifer, tedy technik k ukrytí významu zprávy před všemi nežádoucími čtenáři.

Díky této snaze o utajení provozují jednotlivé státy svá šifrová pracoviště, která zodpovídají za bezpečnou komunikaci a vyvíjí a uvádí do praxe nejlepší možné šifry a šifrovací přístroje. Na druhou stranu se tato pracoviště snaží rozluštit a získat ukrytá tajemství cizích států či organizací. Historie kódování a šifrování je tedy vlastně jakousi „válkou“ mezi tvůrci a luštiteli šifer. Tyto intelektuální kryptologické boje probíhají po staletí a mají velký dopad na světové dějiny.

Stejně jako ostatní vědy i kryptografie procházela vývojem, doslova evolučním zápasem. Kód či šifra je sama o sobě vždy v ohrožení. Jakmile tedy luštitelé vyvinou nový způsob, jak v ní najít slabinu, ztratí celý kód svůj dosavadní význam. Pro takový kód / šifru zbývají již jen dvě možnosti. Buď zmizí, nebo je přetvořen v nový účinnější a zpravidla složitější kód. Ten se pak opět používá jen do té doby, než se podaří objevit jeho slabé stránky a tak stále dokola.

Permanentní boj mezi tvůrci a luštiteli šifer vedl k velké řadě velmi významných vědeckých objevů. Tvůrci šifer se vždy snažili o co nejdokonalejší formu utajení komunikace, zatímco jejich protivníci-luštitelé vyvíjeli ještě rafinovanější techniky útoku. Díky této snaze o zachování i rozkrytí tajemství musely chtě nechtě obě strany ovládat rozmanité obory a technologie od matematiky po lingvistiku, od teorie informace po kvantovou fyziku. Pro všechny související obory bylo toto vynaložené úsilí přínosem a jejich práce často vedla k urychlení technického pokroku. Asi nejvýraznějším příkladem je vznik moderních počítačů.

Kódy a šifry stojí v pozadí mnoha historických mezníků. Mají na svědomí smrti korunovaných hlav, rozkrytí politických intrik a často rozhodovaly o výsledcích bitev i celých válek.[3]

3.1. Starověká kryptografie

Kryptografie prodělala velmi dlouhý vývoj. Jedny z prvních pokusů o utajení obsahu zpráv jsou prokazatelné již z dob egyptského Starého Království a starověké Mezopotámie, tedy již přibližně před 5500 lety. Jednalo se o velmi primitivní systémy. Ty spočívaly většinou v nějaké drobné, zpravidla neobvyklé úpravě či pozměnění písma. Takovéto malé změny byly zcela dostatečné, protože již samotná znalost písma byla v těchto dobách vlastně jistým druhem umění a pro drtivou většinu populace zůstával stejně smysl nápisu utajen.

Kolem roku 1900 p. n. l. použil takto egyptský písař nestandardní hieroglyfické symboly namísto obvyklých hieroglyfů a ze starověké Mezopotámie se dochovala tabulka, která obsahuje zašifrovanou formuli na výrobu glazurované keramiky. Od hebrejců se nám z 6 stol. p. n. l. zase dochovala jednoduchá reverzní šifra atbaš, kterou najdeme i ve Starém zákoně.

Ve staré Indii se situace začala měnit. Zmínky o kryptografii dokonce nalezneme i ve známé učebnici erotiky Kámasútře a to přibližně z počátku našeho letopočtu. V kapitole "Smyslná žena" se hned v úvodu mezi 64 radami ženám, které chtějí mít úspěch u mužů dozvídáme: "Osvojte si tajná písma a šifry nebo si vynalezněte vlastní. Důležitá je také znalost nových způsobů mluvy, abyste mohla obratně měnit začátky a konce slov tak, jak právě potřebujete." V komentáři ke Kámasútře jsou popsány některé z používaných tajných písem. Jeden z uvedených systémů je "muladeviya". Zašifrování „muledeviya“ spočívá pouze v užití reciproční abecedy. Jsou dokonce dochovány záznamy, že tento systém byl používán mezi obchodníky i v mluvené podobě.

Kryptografie má dlouhou tradici v náboženských textech, kde se snaží zpochybnit dominantní postavení kulturních, či politických autorit. Snad nejslavnějším příkladem je tzv. „Ďáblovo číslo“ (Number of the Beast“) z knihy Zjevení, která je součástí Nového Zákona.

[3] - 4, 6, 51, 65, 69

„666“ je téměř jistě kryptografickým (zašifrovaným) způsobem ukryt nebezpečný - závadný odkaz. Mnozí učenci věří, že tímto nebezpečným odkazem je míněna Římská říše, či spíše přímo osoba Císaře Nera (a tím pádem jeho Římská politika perzekuování křesťanů). Toto označení tedy bylo srozumitelné pouze těm, kteří do něj byli zasvěcení, bylo lehce popiratelné, a tedy méně nebezpečné, pokud se dostalo k rukám autorit. Potřeba tohoto utajování skončila (především pro pravoslavné křesťany) s Konstantinovým přijetím křesťanství, jakožto oficiální víry Východořímské říše.

Původ skutečné kryptografie je však spjat až s řeckými dějinami. Skoro všechny učebnice šifrování začínají popisem toho, jak Řekové pro skrytí zpráv používali poněkud nepraktický a neflexibilní způsob. Oholili svému poslu-otroku hlavu, vytetovali na jeho lebku zprávu a poté co mu vlasy opět narostly, se mohl vydat na cestu.

Ve skutečnosti je však zaznamenán pouze jeden takový způsob použití, popsal jej slavný řecký historik Herodotos ve svých „Dějinách“. Původcem zprávy byl tyran Histiaeus a zprávu nechal vytetovat na hlavu svému oddanému otroku, který ji takto skrytou úspěšně dopravil do Milétu, kde tak pomohl ke koordinaci povstání proti Peršanům v 5 století před naším letopočtem.

Jedna z nejdůležitějších zpráv pro existenci západní civilizace byla také předána utajeně. Jednalo se o zprávu, která pomohla Řekům k vítězství nad Peršany. Demaratus, řecký vyhnanec žijící na území perské říše, zjistil termín, kdy perský král Xerxes vytáhne s armádou proti Řekům. I přes způsobenou křivdu se rozhodl touto informací své krajany varovat, seškrábal vosk ze dvou dřevěných psacích destiček a přímo na dřevěný podklad zprávu vyryl. Destičky opět zalil voskem, při náhodné kontrole to vypadalo, že nejsou použité. Zpráva byla doručena na místo na místo určení a Goro, manželka krále Leonidase náhodou odhalila tajemství destiček a zprávu přečetla a informovala ostatní. Po rozluštění se mohli Řekové na invazi připravit a následovaly slavné bitvy u Thermopyl, Salaminy a Platají. Postup perské armády do Evropy byl jednou pro vždy zastaven a v důsledku toho se mohla plně rozvinout západní civilizace.

Řekové samozřejmě neskončili jen u utajování přenosu zpráv (steganografie), ale dokázali vyvinout reálné šifrovací systémy. Sparťané vymysleli a prokazatelně používali již v pátém století před naším letopočtem první známé zařízení na utajení zpráv. Toto zařízení nazývané Skytale (někdy psáno scytale) se skládalo ze dvou holí přesně stanovené šířky. Na první hůl se navinul pás látky, papyru nebo pergamenu. Na takto omotanou tyč se poté napsala zpráva, a to směrem dolů po délce hole. Po odmotání pruhu získal odesílatel pás se sloupcem nic neříkajících písmen. Nepovolaná osoba sice mohla snadno přečíst všechna písmena otevřeného textu, ale díky použitému systému neznala jejich pořadí. Tento pás byl poté dopraven na místo určení, tam byl tento pás navinut na hůl stejné tloušťky a zpráva mohla být snadno přečtěna.

Toto zařízení pracovalo na principu dnes nazývaném jako transpozice (promíchání) otevřeného textu. Jedná se o nejstarší známé kryptografické zařízení.

Kolem roku 360 p. n. l. řek Aineias Taktikos ve svém díle o vojenském umění „Taktika“ popisuje 16 různých šifrovacích metod. Řecký spisovatel Polybios zase vynalezl systém signalizace, který byl později převzat jako jedna z dalších základních kryptografických metod. Polybios seřadil písmena do čtverce a jejich řady a sloupce očísloval. Každé písmeno je tak reprezentováno dvojicí čísel. Číslem řady a číslem sloupce. Polybios také doporučoval, aby tyto „souřadnice“ byly předávány pomocí světelných signálů. Zprávy tak mohly být odeslány bezpečně a rychle na velké vzdálenosti. Polybiův čtverec (šachovnice), umožňující převod písmen na číslice, se stal základem mnoha dalších šifrových systémů.

Římská říše nepřevzala tyto řecké systémy a vydala se vlastní kryptografickou cestou. Na začátku našeho letopočtu byla Římské říši prokazatelně zavedena vojenská kryptografie. Zprávy a rozkazy mezi jednotlivými legiemi nebyly zasílány otevřeně, ale pomocí záměny otevřeného textu za text šifrový. Julius Caesar popisuje využití těchto systémů ve svém díle "Zápisy o válce galské". Díky biografovi Suetoniovi se dokonce podrobně dozvídáme, jak Caesarův systém přesně vypadal. Každé písmeno zprávy bylo zaměněno za písmeno, které leželo o tři místa dále v abecedě. Suetonius dále uvádí, že Caesarův synovec Augustus používal podobný systém na stejném principu. Nahradil však písmeno otevřeného textu písmenem stojícím v abecedě těsně za ním. Výjimkou Augustovi metody bylo poslední písmeno

X, které nahradil dvojicí AA. Kryptografie ve starém Římě se stala naprostou samozřejmostí. Mimo podobných záměn se ještě používalo vkládání kódů pro jména osob, zemí apod.

Základní systémy pro bezpečný přenos informací byly na světě: utajování přenosu a obsahu zpráv, transpozice, používání kódů a záměny znaků otevřeného textu podle určitých pravidel za jiné znaky (substituce). Všechny tyto systémy jsou symetrické, tedy příjemce i odesílatel jsou dohodnuti na stejném principu a klíči.[4]

3.2. Středověká kryptografie

Kryptologie v dnešním slova smyslu se však zrodila teprve díky vynikajícím arabským matematikům. V roce 855 našeho letopočtu popisuje Abu Bakr Ahmad ben `Ali ben Wahshiyya an-Nabati ve svém díle Kitáb šauq Abú Bakr Ahmad ben Alí ben Wahšíja an-Nabati mustahán fí márifat rutúz al-aglán různé šifrové záměnné systémy. Jedna ze substitučních abeced popisovaných v tomto díle se v arabském světě dokonce bez jakékoli změny používala ještě v roce 1775, kdy byla použita v dopise s choulostivými informacemi pro alžírského vládce.

Kolem roku 1000 našeho letopočtu v arabském světě, nábožensky motivovaná textová analýza Koránu vedla k objevu techniky frekvenční analýzy, kterou bylo snadné prolomit monoalfabetickou substituční šifru.

Arabové byli také první, kdo objevili a popsali metody kryptoanalýzy. Soupis arabských objevů a poznatků je uveden v oddíle "Utajování tajných zpráv v dopisech" rozsáhlé čtrnáctidílné encyklopedie Subh al-a 'sha, kterou sepsal egyptský spisovatel Ahmad Abd Allah al-Qalqashandi a která byla dokončena v roce 1412.

Na práce arabských matematiků a kryptologů navázala středověká Evropa.

V roce 1379 sestavil Gabriel di Lavinde, tajemník vzdoropapeže Klementa VII. nejstarší dochovaný nomenklátor. Ten sloužil pro spojení papeže s jeho vyslanci a sestával kromě substituční abecedy i z dvojpísmených kódů pro 24 nejvíc frekventovaných slov či jmen. První práce o kryptografii v západní Evropě je spojena se jménem Leon Battista Alberti, ten ji sepsal v roce 1467, dílo obsahovalo výklad

[4] - 6, 27, 44, 51

luštitelských postupů na základě jazykových znalostí, roztřídění systémů šifrování na substituci a transpozici, objev polyalfabetické substituce a šifrování kódů.

Dalším významným představitelem evropské kryptografie byl benediktinský opat ze Spanheimu Johannes Trittheim. Ten okolo roku 1500 sepsal první významnější evropskou knihu o šifrování. Trittheim se zabýval v té době již překonanými substitučními systémy. Zavedl a doporučoval vkládání takzvaných klamačů do šifrovaného textu. Šlo o náhodné vkládání různých znaků do textu. Účelem bylo ztížení statistického rozboru – frekvenční analýzy. Panovnické rody, které tuto šifru používaly k běžné komunikaci, se však zalekly. Obvinili Trittheima, že vyzradil příliš mnoho tajemství a označily ho za čaroděje.

Hlavním základem všech těchto systémů šifrování byla vždy kombinace metod transpozice a jednoduché záměny s plánovanou snahou zakrýt typické charakteristiky používaného jazyka.

Každé nové poznání, že ve výsledku jdou šifrové texty na základě frekvenčních a statistických metod luštit, vedlo ve většině případů ke zdokonalování šifrových systémů. Převážně bylo snahou zahladit dodatečné a často frekventované informace, které byly v daném textu obsaženy. Tímto se dalo zabránit analýze šifrového textu, která by mohla vést k rozkrytí textu otevřeného. Spoléhání se na nedokonalý šifrovací systém stálo například skotskou královnu Marii Stuartovnu život. Dopisy, ve kterých vydala souhlas k připravovanému povstání a rozkaz k zavraždění anglické královny Alžběty, posloužily jako důkaz při soudním líčení. Použití slabé metody šifrování k uchování osobního tajemství a intimních záležitostí nám zanechalo i zajímavé svědectví ze života Karla Hynka Máchy. Mácha ve svých denících zašifrovaným způsobem popisuje své erotické zážitky velmi peprným způsobem, který by v dnešní době mohl být po dešifraci otištěn většinou erotických časopisů.

Kryptografie se tak v průběhu času nenápadně stávala více potřebnou a nabývala na důležitosti. Byl to důsledek soutěže politiků a církve. Například v Evropě po období Renesance občané mnoha italských států (včetně Papežství) byli odpovědni za podstatné zlepšení praktické kryptografie. Vývoj kryptografie je také bohužel pevně

spjat s válečnými konflikty, při kterých docházelo k nejintenzivnějšímu kryptografickému a kryptoanalytickému vývoji a úsilí.[5]

[5] - 6, 27, 44, 51

4. METODY ŠIFROVÁNÍ VE STAROVĚKU

4.1. Nestandardní hieroglyfy (1900 př. n. l.)

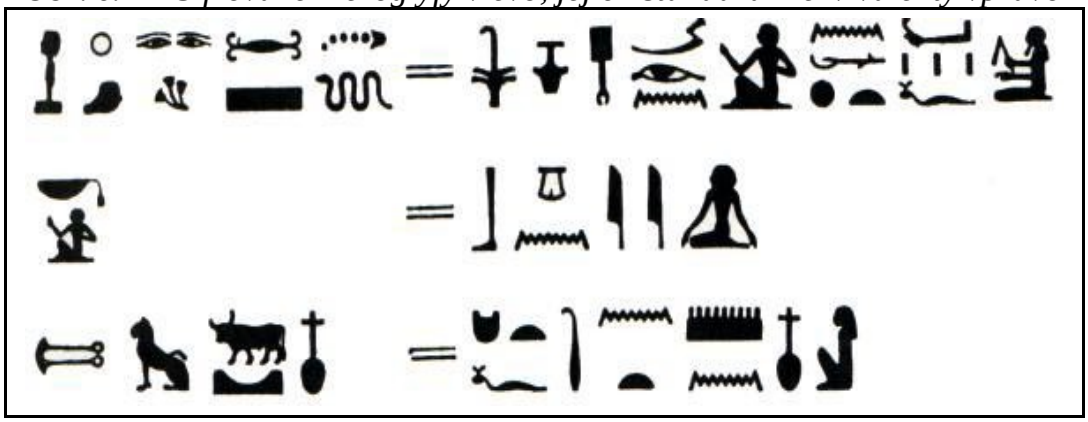
Nejstarším zaznamenaným způsobem šifrování je použití tzv. nestandardních hieroglyfických symbolů namísto hieroglyfů obvyklých. Touto metodou byly šifrované nápisy písaři vytesány do památníků za dob egyptského Starého království, tedy se přibližně jedná o období 1900 před naším letopočtem. V tomto kontextu si musíme však uvědomit, že hieroglyfické písmo je samo o sobě velmi složité a podařilo se ho rozluštit až roku 1822 francouzským archeologem-egyptologem Jeanem-François Champollionem. Slovo hieroglyf pochází ze starořečtiny a znamená „posvátné psaní“ („posvátné vyřezávání“). Porozumění a čtení tohoto písma vyžadovalo znalost přibližně 750 znaků (s postupem času až přes 2000 znaků, či jejich kombinací) a když uvážíme fakt, že v dané době byla gramotnost 1-5% a cizinci až do 4. stol. n. l. považovali hieroglyfy za primitivní obrázkové písmo, které se využívalo převážně k výzdobě chrámů a památníků, vyvstává otázka proč za takové situace písmo ještě dále šifrovat?

Z předchozích i všeobecně známých faktů je nanejvíc zřejmé, že do znalosti hieroglyfického písma byla zasvěcena výhradně elita z řad kněží a královské rodiny. Tímto si aristokracie mimo jiné upevňovala svou již tak nezměrnou moc.

Jako hlavní důvody k užívání nestandardních (či speciálně upravených) hieroglyfů se uvádí například intriky, zapisování osobních a citlivých dat, komunikace mezi úzkou skupinou lidí, ale i jen snaha o originalitu v tvorbě znaků, estetickou preciznost zpracování či dokonce pobavení gramotných diváků (čtenářů).[6]

[6] - 13, 22, 27, 37, 66

Obr. č. 1 - Šifrované hieroglyfy vlevo, jejich standardní ekvivalenty vpravo



4.2. Zašifrovaný recept na hrnčířskou glazuru (1500 př. n. l.)

Jedním z dalších důvodů proč užívat a zdokonalovat kryptografii je duševní vlastnictví. V případě prvního nálezu šifrovaného textu ve starověké Mezopotámii se jedná o utajení vysoce ceněného receptu na výrobu hrnčířské glazury.

Tento recept byl nalezen na destičce velké pouze 3x2 palců (2,54 cm) na břehu řeky Tigris na území dnešního Iráku a pochází přibližně z 15 století před naším letopočtem.

Samotná metoda zašifrování spočívala v transformaci psaného textu, založeného na korelaci (vzájemném vztahu) mezi výslovností a psaným ekvivalentem. Když víme, že klínové písmo, je písmo slabičné, můžeme se pokusit metodu šifrování pochopit na příkladu George Bernarda Shawa. Níže uvedený příklad se týká šifrování slova fish (ryba), které by se dle Shawa transformuje do slova ghoti.

xxxx tou**GH** xxx xx : **gh** : **f** -> touGH (výslovnost : ta**F**)

xx xxx w**O**men xxx : **o** : **i** -> wOmen (výslovnost: v**I**min)

xx xx na**TI**on xxxx : **ti** : **sh** -> naTIon (výslovnost nej**Š**n – š = sh)

Ovšem při dešifrování lze narazit i na problémy, ty se týkaly především klínového písma samotného. Klínové písmo totiž není vlastně písmo s konkrétní sadou znaků, ale způsob jeho zápisu. Šlo o zjednodušené piktogramy otočené o 90°. V Mezopotámii v tomto období se používalo několik sad znaků, než byly časem ustáleny. Jak už bylo zmíněno, klínové písmo, je písmo slabičné ale vzhledem

k neustálenosti je běžné, že se dá jeden znak číst více způsoby a naopak, jedna slabika může být zapsána několika různými znaky. V klínovém písmu taktéž přetrvávalo hodně logogramů, tedy znaků, které měly hodnotu celého slova, či znaků, které jen označovaly druh slova a nevyslovovaly se.

Na závěr jen zbývá dodat, že jak se postupem času znalost výroby glazury rozšířila, potřeba utajení vymizela a později se setkáváme s receptem psaným již jen v běžné formě.[7]

Obr. č. 2 – Mezopotamská hliněná destička

4.3. Hebrejská substituční šifra ATBASH (500-600 př. n. l.)

Při zkoumání knih Starého zákona (konkrétně prorocké knihy Jeremjáš) byl objeven fakt, že mnoho názvů slov a míst bylo záměrně utajováno pomocí šifry zvané Atbaš (též Átbaš, Atbsh či Temurah). Asi nejznámějším příkladem je zašifrování slova Babel (označující starověké město Babylon) slovem Šéšak. Jaký je tedy princip této metody?

Atbaš je velmi jednoduchá substituční šifra, která ke svému šifrování-dešifrování využívá jedinou kódovací tabulku. Principem je prohození prvního písmene s posledním, druhého s předposledním atd. Pro její vytvoření tedy stačí jen zapsat na jeden řádek abecedu zleva doprava a pod něj v opačném pořadí. Písmeno A tedy nahradíme za písmeno Z, B za Y, C za X atd.

[7] - 7, 12, 23, 76

Obr. č. 3 – tabulka atbash v latince

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

Obr. č. 4 – tabulka atbash v hebrejštině

Princip této šifry je vlastně obsažen už v jeho samotném názvu. První písmeno hebrejské abecedy Alef se nahrazuje posledním Tav, druhé Bet předposledním Šin. Ve výsledku nám tedy vyjde A-T, B-Š ATBAŠ.

Písmena tvoří pevné dvojice a šifra je tedy velmi snadno prolomitelná, ovšem v kontextu mystičnosti židovského učení Kabala, zasazení Abstaše do mnohem složitějších a komplexnějších biblických kódů a nepřebernému množství nezodpovězených otázek obsažených přímo v Bibli získává tato metoda na zajímavosti.

Známým případem je například slovo Baphomet – symbol ďábla, jakožto jeden z důvodů, kvůli kterému byl zrušen Templářský řád. Pokud pomocí Atbaše dešifrujeme toto slovo, vyjde nám výraz Sophia – moudrost, základní pojem gnosticismu. Toto je jen malá část velkých tajemství a utajování se kterými je Atbaš úzce spojen.

V hebrejské literatuře jsou známy ještě další dvě podobné substituce: Albam a Atbah.[8]

[8] - 10, 15, 17, 20, 35, 46

4.4. Tetování (490 př. n . l.)

Jako častý způsob ukrytí zprávy před nepověřenými je v mnoha zdrojích uváděno vytetování zprávy na vyholenou hlavu otroka. Když otrokovi narostly vlasy do délky, kdy nebylo tetování poznat, byl vyslán doručit zprávu.

Ve skutečnosti je tato metoda v historických análech zachycena jen jednou a to v obsáhlém díle Histories apodeixis (Dějiny), které sepsal známý řecký historik, „otec dějepisu“, Herodotos.

Dnes můžeme tvrdit, že pokud je tato událost pravdivá tak se jedná patrně o nejstarší dochovaný důkaz o využití steganografie.

Datujeme ho do pátého století před naším letopočtem, kdy Perský král Darius I. držel v šachu řeckého tyrana Hisiaea. Histiaeus chystal povstání proti Perské říši a nutně potřeboval odeslat tajně zprávu o tomto povstání svému zeti Aristogorovi do Milétského Anatolianu. Histiaeus tedy nechal svému nejvěrnějšímu otrokovi vyholit hlavu a vytetovat na ni zprávu. Otrok se samozřejmě vydal na cestu až po té, co mu vlasy dorostly. Když otrok dorazil k Aristogorovi, stačilo jen zase oholit hlavu, aby si vytetovanou zprávu mohl přečíst.

Tato technika ale skýtá více záporů než kladů. Jednak se nesmí jednat o spěšnou zprávu, vzhledem k faktu, že se muselo čekat než vlasy dorostou do potřebné délky. Dále pak musíme vzít v úvahu, že jednou vytetovaná zpráva už nemohla být odstraněna bez toho aniž by byl posel zabit. A třetím záporem je, že jeden otrok , díky specifickému umístění a provedení, nemohl doručit více zpráv.

Na závěr jen snad dodat, že tato metoda steganografie byla po té zachycena až mnohem později a to u pirátů, kteří si nechávali tetovat na lebku tajné mapy s ukrytými poklady.[9]

4.5. Skytale (486 př. n. l.)

Za první vojenské šifrovací zařízení, které vymysleli a prokazatelně používali již v pátém století před naším letopočtem starověcí Řekové (konkrétně z městského státu Sparta) je systém Skytale (scytale). První zmínky o Skytale se však v náznacích objevují již v 7. stol. př. n. l. v díle řeckého básníka Archilochuse. K jakému účelu

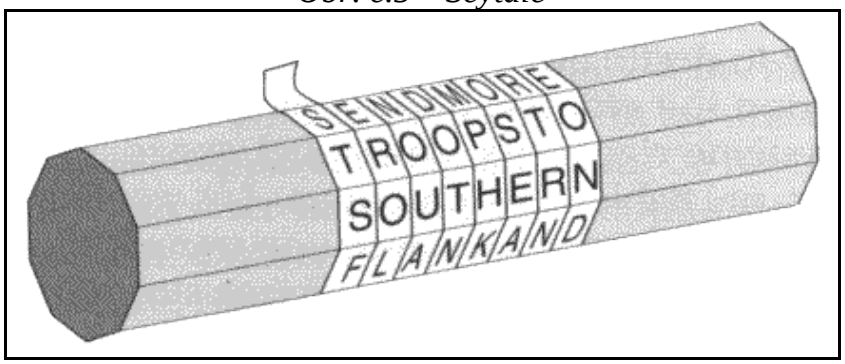
[9] - 2, 29, 34, 40, 45

přesně Skytale sloužilo se dovídáme v polovině 3 stol. př. n. l. a to jak se tento systém používal a fungoval až v 1 stol. n. l. díky řeckému historikovi Plutarchovi.

Toto zařízení pracovalo na principu transpozice, tedy promíchání otevřeného textu. Jedná se vcelku o jednoduchou metodu, kterou si může každý vyzkoušet doma v praxi. Skytale se skládá ze dvou holí přesně stanovené šířky (kulatin či čtyř, šesti a vícehranů) a pásu pergamenu (látky, kůže, papíru atd.). Stejná šířka holí je nejdůležitějším faktorem pro správné dešifrování zprávy, jedná se vlastně o symetrický klíč tohoto zařízení. Na první hůl se navinul pás látky, papyru či pergamenu, na který se posléze napsal text zprávy, a to směrem dolů po délce hole. Když se pás s textem sejmul z hole, dostal neobeznámený čtenář jen nesmyslnou posloupnost písmen. Po této fázi zbývalo již jen úspěšně doručit text přes území nepřítele k příjemci, který disponoval druhou holí se stejnou šířkou. I v této fázi projevovali staří Řekové důvtip a proto pásy pergamenu vydávali za opasky, popruhy, či jinak zakomponovávali do šatstva a výstroje. Pro úplnou představu ještě zbývá dodat, že každý sparťanský generál či admirál disponoval svou vlastní dlouhou černou holí, jejíž identická kopie zůstávala na spartském úřadě.

Příkladů užití Skytale v řeckých dějinách najdeme mnoho, například roku 404 př. n. l. předal raněný posel králi Sparty Lysandrovi svůj opasek se správou zašifrovanou touto metodou. Při použití správné tyče Lysandros zjistil, že se na něj chystá zaútočit perský král Farnabazus. Lysandros se díky této zprávě včas připravil a útok úspěšně odrazil.[10]

Obr. č.5 – Scytale



[10] - 14, 16, 87, 91

4.6. Vosk (479 př. n. l.)

Zpráva, která mohla zvrátit celé základy existence dnešní západní civilizace byla také předána utajeně. Šlo o zprávu, která pomohla Řekům k vítězství nad Peršany.

V 5. století před naším letopočtem Řek Demeratus, syn Aristona žijící v perských Sůsách zjistil přesné datum, kdy perský král Xerxes vytáhne se svou armádou proti Řekům (konkrétně na Spartu a Athény). Demeratus byl z Řecka vyhnán, ale jeho vlastenecké cítění bylo silnější a i přes způsobenou křivdu neváhal své krajany varovat. Seškrábal vosk ze dvou dřevěných psacích destiček (které se v té době běžně používaly na psaní), vyryl zprávu na dřevěný podklad, destičky opět zalil voskem a na tabulku napsal nezávadný text. Takto skrytá zpráva snadno prošla kontrolou na hranicích a dorazila až na místo určení. Ve Spartě však nevěděli, co s touto tabulkou mají dělat Ukrytou zprávu náhodou odhalila až Gorgo, manželka krále Leonidase a sdělila ji ostatním Řekům.

Díky této informaci se Řekové mohli na boj připravit a po mnoha slavných bitvách (bitva u Thermopyl, Salaminy a u Platají) byl postup perských vojsk do Evropy zastaven a jako důsledek se mohla rozvinout západní civilizace.[11]

4.7. Aenias Taktikos (360 př. n. l.)

Aeneas ze Stymphalus, dnes známý jako Aenias Taktikos, autor obsáhlého díla (Taktika o vojenském umění) o řecké válečné taktice, velké jméno pro vojenství, z jehož odkazu čerpali takové osobnosti jako Alexander Veliký či Hadrian. Z jeho díla „Aeniovo válečné pojednání“ se dokonce vycházelo ještě v 16. století!

Z tohoto díla, v části Poliorketika také Aenias uvádí 16 různých šifrovacíh metod. Jedná se vůbec o první popis použití válečné kryptografie!

Jedna z těchto uvedených metod je založena víceméně na stejném principu jako dnes známá Morseova abeceda a druhá používá nahrazování znaků řecké abecedy číslicemi. Tato poslední transformace je pratkicky základem matematické manipulace v dnešní kryptografii. Mezi tyto metody zahrnujeme i způsoby

[11] - 29, 34, 40, 45

steganografické, konkrétně je zde popsáno, jak skrýt zprávu, kdy se do kotouče vyrazí dírky a provlíkáním provázku se zašifrují jednotlivá písmena.[12]

4.8. Polybiův čtverec (203 – 120 př. n. l.)

Nejvýznamnějším historikem z období Helénismu a možná celého starověku vůbec je titulován řek Polibios.

Pro nás je zajímavý tím, že ve svém rozsáhlém díle „Historiai“ (Dějiny) popsal jednoduchou a zároveň velmi účinnou metodu šifrování. Ta je dnes známá jako Polybiův čtverec, nebo Polybiova šachovnice.

Obr. č. 6 - Polybiův čtverec

	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

Polybiův čtverec je velmi jednoduchá šifra, jde pouze o to seřadit abecedu do čtvercové tabulky 5 × 5 a očíslovat její řádky a sloupce. Každé písmeno původního textu se pak nahradí dvojicí písmen, nejprve číslo řady, pak číslo sloupce.

Pokud tedy chceme zašifrovat slovo Polybios, bude šifrovaný text vypadat takto: „41 35 32 54 12 24 35 44“

Polybius sám doporučoval aby tato čísla byla předávána pomocí pochodní, tedy k nočnímu vysílání na dálku, vznikl tak první telegraf umožňující vysílat předem nedomluvené zprávy. K vysílání bylo potřeba deset hořících loučí, pět za každým ze dvou neprůhledných panelů. Počet loučí zdvižených nad levý panel udával číslo

[12] - 4, 24, 55

sloupec, louče nad pravým panelem pak číslo řádku daného písmene v Polybiově čtverci. Zprávy tak mohly být odeslány bezpečně a rychle na velké vzdálenosti.

Známé jsou taky případy využívání tzv. „vyťukávací metody“, kdy se dvojčíslí označující písmena vyťukávala na roury či zdi. Její používání bylo zaznamenáno ve věznicích Carského Ruska či z dob války ve Vietnamu. Existují samozřejmě i další jednoduché způsoby jak šifru předávat: blikajícím světlem, bubny, kouřovými signály atd.

Polybiův čtverec není sám o sobě nijak extra bezpečný, ani když používá smíšenou abecedu. Tato šifra je stále jen jednoduchou substitucí, kde se písmena nahrazují párem číslic.

Je zřejmé, že velkou výhodou Polybiova čtverce je rychlé šifrování/dešifrování zprávy, proto se stal základem mnoha dalších šifrových systémů, jako například šifra ADFGVX, Nihilistická šifra a bifid kód.[13]

4.9. Caesarova šifra (50 př. n. l.)

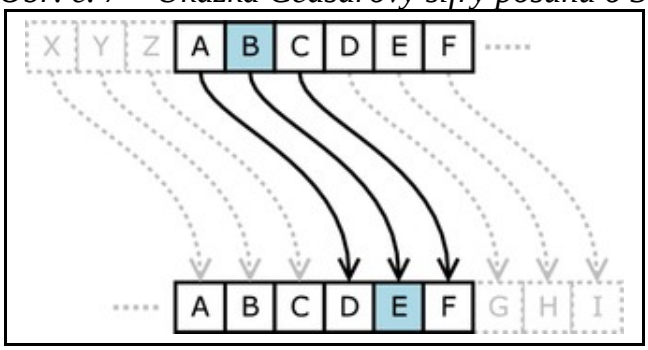
Gaius Julius Caesar, vládce Římské říše díky své moci a svému postavení nemohl důvěřovat ani svým nejbližším přátelům. Jeho pozice, způsob jakým ji nabyl a množství válek, které vedl ho přiměli k tomu, že používal velké množství šifer. Všechny byly údajně popsány ve spisu, který napsal Caesarův pobočník Valerius Probus. Tento spis se bohužel nezachoval, avšak o jedné z metod se dovídáme z díla De vita Caesarum od římského polyhistora jménem Gaius Suetonius Tranquillus.

Tato metoda (dále Caesarova šifra) se datuje do období galských válek, kdy Římané v letech 59 až 48 před naším letopočtem dobývali území dnešní Belgie, Francie, Německa, Rakouska a Španělska. Pro udělování rozkazů a veškerou další komunikaci se svými legiemi používal Caesar jednoduchou monoalfabetickou substituční šifru.

Způsob šifrování spočíval v tom, že každé písmeno zprávy se nahradilo (substituce) jiným písmenem, které se nacházelo o 3 pozice dále vpravo. Takže například písmeno A bychom nahradili písmenem D. Proto se také někdy Caesarova šifra nazývá „Caesar Shift Cipher“ neboli Caesarova posunová šifra.

[13] - 47, 51, 83, 84

Obr. č. 7 – Ukázka Ceasarovy šifry posunu o 3



Tento způsob se zdá velmi primitivní a jednoduchý na rozluštění. Ve své době ale představoval nevídanou metodu a osvědčil se velmi dobře. Také díky různým kombinacím se dala šifra nesčetněkrát obměňovat. Číslo všech těchto kombinací je údajně větší než 1×10^{26}.

Způsobem obměny či vylepšením byla například změna počtu pozic o které se abeceda posouvala (tehdejší latina měla 25 znaků), změna směru posunu, rozdělení textu do pevného počtu písmen, transliterace z latiny do řečtiny, proměnlivá hodnota posunutí v abecedě a další jednoduché algoritmy.

Ačkoli je Caesarova šifra snadno prolomitelná, setkávám se s ní v různých obměnách až do dneška. Například v roce 1915 ji používala ruská armáda zkrátka proto, že ostatní šifry byly pro jejich vojáky příliš složité. Na internetových diskusních fórech se spíše pro pobavení a skrytí obskurních výrazů v 80 a 90 letech 20 století používal systém ROT13 ("rotate by 13 places") neboli klasická Caesarova šifra s posunem o 13 pozic. A dokonce ještě v roce 2006 byl v Sicílii dopaden uprchlý mafiánský boss Bernardo Provenzano, zčásti díky tomu že byly rozluštěny jeho zprávy psané variantou Caserovy šifry.[14]

4.10. Kama Sutra (cca 0 - 400 n. l.)

Kamasutra, starověké indické dílo, které sepsal indický filozof Mallanaga Vatsyayana dává rady týkající se lidského sexuálního chování, řízení domácnosti, vztahů mezi partnery obecně, ale také rady týkající se kryptografie. Toto dílo sepsal Vatsyayana ve čtvrtém století našeho letopočtu, ale vycházel však z rukopisů až o 800 let starších!

[14] - 5, 21, 43, 58, 74, 86

Kamasutra obsahuje 64 dovedností, které by měli muž a žena v praxi ovládat. 44. a 45. místo je určeno kryptografii. Doslova na těchto místech v seznamu čteme:

44. - Umění pochopení psaní šifer a slov pro utajování věcí.

45. - Umění dorozumět se změněnými formami slov, v různých podobách. Například vyměnit začátek nebo konec slova, nebo přidat do slova navíc nějaká písmena.

Kamasutra dále radí ženám studovat umění tajného písma proto, aby mohly ukrýt informace o svých vztazích. Jednou z doporučovaných technik je náhodně spárovat písmena abecedy a poté nahradit původní písmeno ve zprávě jeho partnerem. Použito na latinské abecedě, mohla by zpráva vypadat asi takto:

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

NUKXUCU NU E YUHU = SEJDEME SE U TEBE

Pokud tedy tento způsob aplikujeme na standardní latinku dostaneme překvapivě velké číslo 7,9 x 10^{12} možných klíčů. Tudíž rozluštění bez použití moderních technologie bylo v té době téměř nemožné.

Teprve o 4 století později bylo možné luštit tuto substituční šifru díky technice frekvenční analýzy slavného arabského filozofa, „otce kryptoanalýzy“ jménem Abu Yusuf al-Kindi.[15]

4.11. Neviditelné inkousty (cca 50 n. l.)

Římský válečník a filosof Gaius Plinius Secundus (Plinius Starší) je autorem jedné z nejvýznamnějších přírodovědných encyklopedií starého Říma, Historia naturalis a také se jako první popsal výrobu tzv. duběnkového inkoustu.

Duběnkový inkoust je jistě zajímavým přínosem, ale pro nás zajímavějším je Piliniův návod, jak použít mléko z pryšce (Tithymalus) jako neviditelný inkoust.

Mléko z pryšce je totiž po zaschnutí zcela průhledné, teprve po zahřátí zhnědne.

[15] - 33, 48, 75

Tímto objevem byla odstartována další významná steganografická metoda neviditelných inkoustů, které se v mnoha způsobech a provedeních používaly až do druhé poloviny 20. století. Tato dlouhá tradice sice ukazuje, že jde o techniku, která poskytuje určitý stupeň utajení, ale má jednu zásadní vadu. Pokud je totiž zpráva jednou objevena, je prozrazena celá. Již pouhé její zachycení znamená ztrátu veškerého utajení!

Dalšími příklady neviditelných inkoustů jsou například: moč, mléko, citrónová šťáva, ocet atd. [16]

4.12. Leidenský papyrus (cca 200 n. l.)

Velmi známý egyptský papyrus, který sepsal za časů Starého Království (2575 – 2150 př. n. l.) mudrc Ipuwer se nyní nachází v nizozemském městě Leiden. Tento papyrus proslul hlavně díky kontroverzní knize Worlds in Collision (Světy ve srážce) ruského psychiatra a spisovatele Immanuela Simonoviče Velikovského. V této knize z roku 1950 Velikovskij prezentuje odvážnou teorii biblického exodu Židů do Egypta. Prezentuje jej jako důsledek přírodní katastrofy zapříčiněný padajícími meteority, čímž způsobil ve světě velké pozdvižení. Velikovskij v tomto díle čerpá právě z Ipuwerova papyru.

Ovšem Ipuwrův papyrus je zajímavý také proto, že dokazuje, že již za časů Starého Království se ve starověkém Egyptě používal tzv. číselný symbolismus. Konkrétně tato metoda byla používána pro nejdůležitějších částí magických receptů a kouzel.

[16] - 29, 34, 40, 45, 81

Obr. č. 7 – Leidenský papyrus

Systém číslovaní Ipuwerova papyru identifikuje podstatu, hledisko stvoření a přiřadí k němu symbolické číslo.

Papyrus sestává z 27 slok (dochovalo se jich pouze 21), číslovaných nejdříve od 1 do 9, pak po desítkách od 10 do 90 a následně po stovkách od 100 do 900. Každé první slovo sloky je jakousi slovní hříčkou příslušného čísla.

Samotný číselný systém tohoto papyru je sám o sobě velmi významný. Čísla od 1 do 9, které jsou následně umocněny desítkami 10, 20, 30 atd. představují základní vyjádření pro fyzikální veličiny.[17]

[17] - 22, 25, 59, 72, 73

5. METODY ŠIFROVÁNÍ VE STŘEDOVĚKU

5.1. Abu `Abd al-Rahman al-Khalil ibn Ahmad ibn `Amr ibn Tammam al Farahidi al-Zadi al Yahmadiho kniha kryptografie (725-790 n. l.)

Abu `Abd al-Rahman al-Khalil ibn Ahmad ibn `Amr ibn Tammam al Farahidi al-Zadi al Yahmadi napsal knihu o kryptografii a kryptoanalýze (Kitáb Mu'amma). Tato kniha byla inspirována jeho vlastním řešením a rozluštěním kryptogramů pro vládce Byzantské říše za období starověkého Řecka. Kniha je bohužel již nenávratně ztracena.

Jeho řešení šifrovaného textu bylo založené na znalosti (správném odhadu) části otevřeného textu na začátku šifrované zprávy.

Konkrétně byzantinskou šifru (zapsanou v řečtině) vyluštil díky tomu, že správně odhadl začátek textu „Ve jménu Božím". Díky této hypotéze byl schopen následně dešifrovat zbytek textu.

Nutno podotknout, že tato (dnes již standardní) kryptologická metoda byla použita například během 2. světové války proti německému šifrovacímu stroji ENIGMA.[18]

5.2. Abu Bakr Ahmad ben `Ali ben Wahshiyya an-Nabati (855 n. l.)

Významný arabský vědec Abu Bakr Ahmed ben Ali ben Wahsiyya an Nabati (dále jen Wahshiyya) je dnes znám spíše proto, že vše naznačuje tomu, že rozluštil a byl schopen číst starověké egyptské hieroglyfy o 9 století dříve než Jean-François Champollion. Byl to všestranně zaměřený člověk, který sepsal mnoho knih z oborů alchymie, zemědělství, fyziky, medicíny a magie.

Právě z poslední jmenované kategorie pochází dílo Kitáb šauq Abú Bakr Ahmad ben Alí ben Wahšíja an-Nabati mustahán fí márifat rutúz al-aglán (Kniha přání oddaného fanatika naučit se něco o hádankách ve starých dokumentech), ve kterém Wahshiyya uveřejnil několik šifrových abeced, které se užívaly tradičně pro praktikování magie.

[18] - 3, 7, 32, 42

Dochovalo se pouze několik dokumentů psaných šifrovaným písmem z období po pádu Persie. Ze záznamů v kronikách se ještě dozvídáme, že vysocí úředníci opatřovali každou novou poštovní zprávu tzv. osobním kódem.

K většímu rozšíření a vývoji kryptografie ve středověké Arábii také nepřispíval fakt, že jednotlivé arabské státy mezi sebou moc nekooperovaly a také celková absence nějaké trvalejší státní správy či budování velvyslanectví.[19]

5.3. Benátská politická kryptografie (1226 n. l.)

Z dob hlubokého středověku, z 13. století byla v Benátských archivech nalezena jednoduchá substituční šifra politických textů.

Princip této kryptografické metody byl velmi jednoduchý. V některých (důležitých) slovech byly samohlásky (a, e, i, o, u) nahrazeny tečkami či křížky.

Alexander d'Agapayeff ve své knize Codes and Ciphers tvrdí, že tato metoda byla využívána mnichy Benediktinského řádu již dávno předtím. Jednalo se o údajně o tradiční benediktinské šifrování. S první důkazem se však setkáme v 9. století, kdy bylo použito v díle „Pojednání o demokracii“ a princip šifrování vypadal zhruba takto:

i = .
a = :
e = :.
o = ::
u = ::.
Slovo Florencie bychom tedy zašifrovali jako Fl::r:.nc.:.

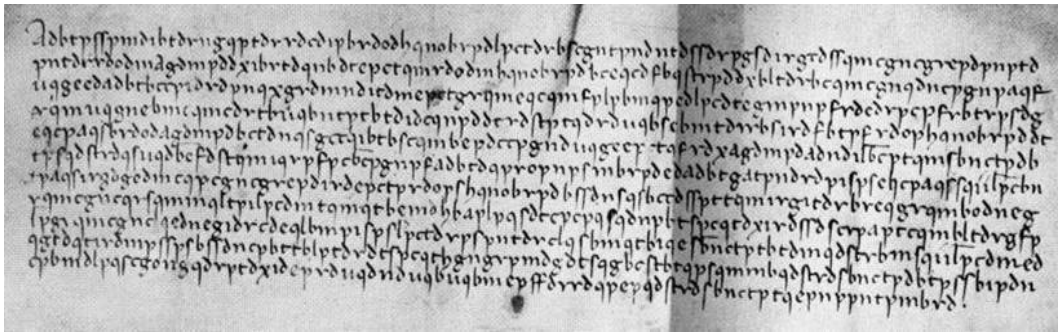
David Kahn v „The Codebreakers“ tuto metodu připisuje Svatému Bonifáci, který ji přinesl z Anglie do Německa již v 8. století.

Ačkoli byla tato metoda primitivní, těšila se poměrně velké oblibě a byla používána v různých obměnách ještě 150 let po Benátském „Pojednání o demokracii“. Samohlásky nebyl již nahrazovány jen tečkami a křížky, ale i jinými písmeny či znaky. Například v roce1332 neapolský král Robert I zašifroval touto metodou dopis

[19] - 33, 49, 71

do sídla vzdorpapeže Avignonu. Jednalo se o důležité informace o dohodě mezi Rakouskem, Uherskem a Českým královstvím. Viz. Obrázek.

Obr. č.8 – Dopis krále Roberta I. Papeži



Jako modifikaci tohoto typu se dá považovat i pravděpodobně první dochovaný doklad od kryptografii na českém území a tím jsou listy Mistra Jana Husa z Kostnice, pocházející z roku 1415!

Modifikace spočívala v tom, že namísto teček, nahrazoval samohlásky písmenem, které samohlásku v abecedě následuje. Konkrétně tedy

A=b

E=f

I=j

O=p

U=v

Dalo by se tedy říct, že se jednalo o jakýsi mix Ceasarovy a benediktinské metody šifrování.[20]

5.4. Roger Bacon (1250 n. l.)

„Bláznivý je ten, kdo zapíše tajemství jiným způsobem tajnopisu, než tím, který ho chrání před nepovolanými.“ Autorem tohoto citátu je známý františkánský mnich, filozof a vědec Roger Bacon.

Bacon je také mimo jiné autorem první rukopisné knihy o kryptografii a to De secretis artis et naturae operibus et de nullitate magiae (List o tajných postupech a neexistenci magie), ze které pochází i výše zmíněný citát. Dále v tomto díle popisuje

[20] - 39, 51, 52

sedm jednoduchých šifrovacích metod. Poslední tři kapitoly jsou psány v alchymistickém žargonu a hojně v nich využívá kryptogramy.

Mezi jednu z mnoha Baconových zásluh patří to, že dal světu ustálenou a bezpečnou recepturu na střelný prach, ale ani tu nezapomněl zašifrovat.

„We can, with saltpeter and other substances, compose artificially a fire that can be launched over long distances... By only using a very small quantity of this material much light can be created accompanied by a horrible fracas. It is possible with it to destroy a town or an army ... In order to produce this artificial lightning and thunder it is necessary to take saltpeter, sulfur, and **Luru Vopo Vir Can Utriet**.“

Povšimněme si posledních zdánlivě nesmyslných slov. Tato slova jsou tvořena anagramy, které měly za úkol utajit poměr práškového dřevěného uhlí potřebného k vytvoření exploze.

Dalším dílem, jehož autorství je připisováno Baconovi a jež by mohlo také spadat do kategorie kryptografie, je záhadný Voynichův rukopis.

Okolo Voynichova manuskriptu je více otazníků, než-li odpovědí. Jedná se o dílo psané písmem, které se dodnes nepodařilo rozluštit. Rukopis má 235 stran a je rozdělen do 6 části: Botanická část, Biologická část, Astronomická část, Kosmologická část, Farmakologická část a Recepty. Ovšem všechny tyto části popisují věci, které se na naší planetě nevyskytují, takže rukopis vzbuzuje ještě větší pozornost.

Je hodně teorií o Voynichově rukopisu, setkáváme se s tvrzeními, že je psaný neznámým jazykem, návštěvníky z vesmíru, pozměněnou staroukrajinštinou, foneticky přepsanou čínštinou, že jde o naprosto nesmyslnou, úmyslně sepsanou podvodnou fabulaci či alchymistické dílo psané šifrovaným písmem.

Jediné, co o Voynichově manuskriptu můžeme s klidným srdcem říct, je to, že ani za pomoci nejmodernějších vědeckých postupů a technologií se ho nikomu nepodařilo „rozlušit“

Voynichův rukopis je volně dostupný v elektronické formě na stránkách Yale University Beinecke Rare Book and Manuscript Library[21]

http://beinecke.library.yale.edu/dl_crosscollex/default.htm

pod signaturou ms 408

Obr. č. 9 – Ukázka z Voynichova manuskriptu

5.5. Muqaddimah (1377 n. l.)

Historik, státník, teolog, tím vším byl arabský učenec Abū Zayd ‘Abdu r-Rahman bin Muhammad bin Khaldūn, který je považován za předchůdce mnoha dnešních sociálních věd jako demografie, kulturní historie, historiografie, sociologie, ekonomika a filozofie historie.

Pro nás je zajímavý zejména tím, že sepsal obsáhlé dílo Muqaddimah (latinsky Prolegomena, 1. část sedmičlenného celku), kde popisuje arabský pohled na všeobecnou historii.

V tomto díle mimo jiné citoval použití názvů parfémů, ovoce, ptáků nebo květin jako označení písmen a nebo jako formy odlišení od všeobecně používaných typů písmen.

[21] - 18, 19, 85, 92

Byly to vlastně velmi speciální kódy a sloužily jako šifra na výměnu informací mezi mýtnicemi a vojenskými posádkami.

Na použití jednotlivých kódů se nejdřív oba korespondenti museli shodnout, aby byli vůbec schopni porozumět myšlenkám obsaženým v šifrovaném textu.

Ibn Khaldun také v Muqaddimah zanechal „kryptoanalytický“ citát:

„Dobře známé spisy o kryptografii jsou vlastnictvím lidstva“[22]

5.6. Nomenklátor Gabrieliho di Lavinde (1379 n. l.)

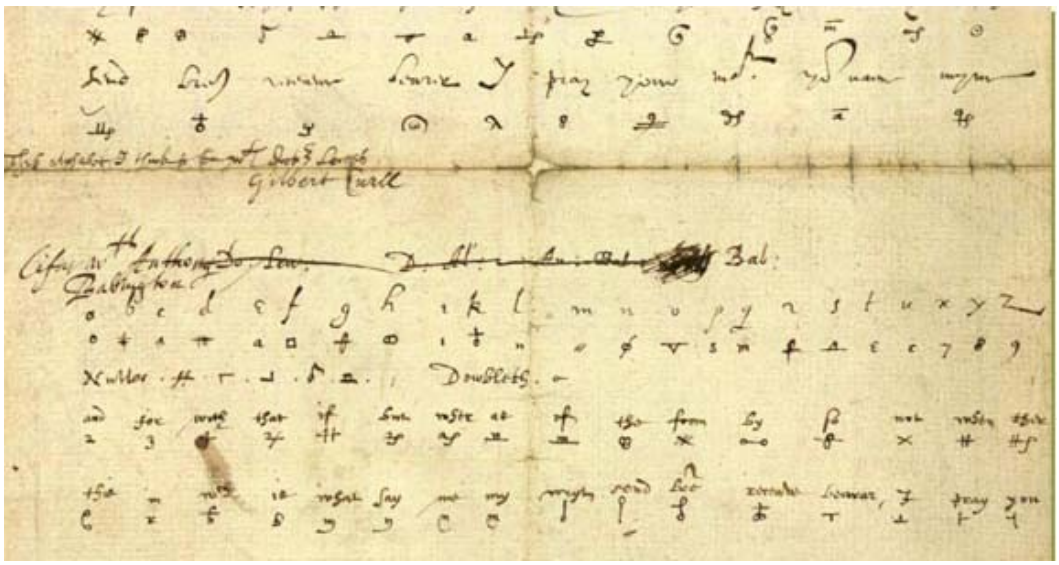
V roce 1379 na příkaz vzdorpapeže Klementa VII vytvořil Gabrieli di Lavinde sadu individuálních šifer pro 24 jeho vyslanců.

Tato metoda je kombinací substituční šifry a jednoduchého kódu. V praxi to znamená, že písmena byla nahrazena za jiná písmena a určitá, (většinou klíčová slova, jména, názvy,...) byla vyjádřená pomocí kódového ekvivalentu (v tomto případě 24 dvojpísmenných kombinací). V pozdějších dobách byly do těchto šifer zakomponovány i tzv. klamače, což jsou nevýznamové skupiny písmen, které měly za úkol ztížit rozluštění zašifrovaného textu. Tento kombinovaný systém se nazývá nomenklátor.

Nomenklátory se brzy staly velmi populární, zejména mezi šlechtou a diplomaty, pomocí nomenklátoru psal své milostné dopisy i například Casanova. O jejich oblíbenosti svědčí i fakt, že se používaly ještě 500 let po jejich vzniku, a to i přes skutečnost, že mezitím byly vynalezeny mnohem silnější metody šifrování.

[22] - 7, 42, 70, 79

Obr. č. 10 – Nomenklátor



S průběhem času a potřeby utajení se slovníky nomenklátorů rozšiřovaly na stovky až tisíce kódových slov. Hlavní výhoda této metody byla ta, že je velmi jednoduchá, rychlá a zvládl ji vytvořit téměř každý.

Zvláštním paradoxem této metody je, že o co propracovanější a obsažnější nomenklátor byl, o to lépe se luštil. Nevýhoda byla v tom, že pro rychlé vyhledávání byla slova řazena abecedně-vzestupně. Pokud tedy bylo kódové slovo například čtyř místné číslo a tato čísla byla také řazena vzestupně, mohl luštitel odhadnout jaké písmeno je na začátku slova, které kód představuje.

Nejznámějším luštitelem nomenklátorů se stal Francouz Antoine Rossignol, který mimo jiné pracoval i pro známého Kardinála Richelieu a těšil se díky svým schopnostem velké přízni francouzského krále Ludvíka XIII. Rossignol také odstranil nedostatek tehdejších nomenklátorů tím, že promíchal číselné kódy. Nomenklátory se poté vytvářely dva – jeden šifrovací, abecedně seřazený a druhý dešifrovací numericky, seřazený vzestupně.

Pro úspěšné luštění nomenklátorů se používala analýza frekventních slov. Hlavním vodítkem při luštění byla aspoň částečná znalost kontextu či obsahu, který nomenklátor obsahuje. Dalo by se říci, že základem pro luštění nomenklátoru je dobrá znalost příjemce, odesílatele, okolností a tématu, o čem si mohou psát. Za pomoci těchto indicií je možné se následně pokusit odhadnout jednotlivé kódy.

Největší chybou při užívání nomenklátorů byla skutečnost, že její majitel jej často používal i celý svůj život. Čím více zpráv měli luštitelé k dispozici, tím jednodušší bylo šifru prolomit. Pokud se tedy nomenklátor často obměňuje a poopravuje, je relativně bezpečný.

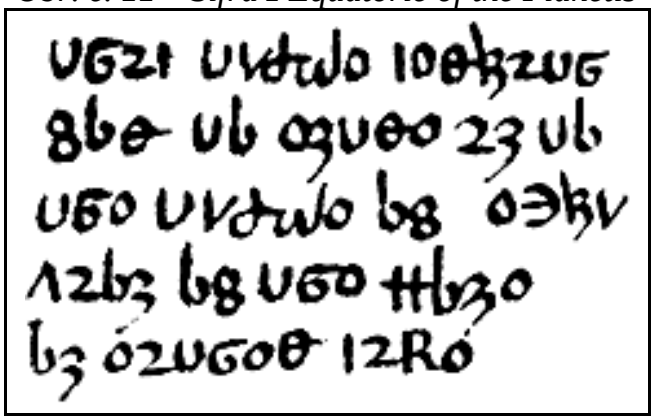
Obsažnější a tištěné nomenklátory se již nazývají kódová kniha.[23]

5.7. The Equatorie of the Planetis (1392 n. l.)

Slavný anglický básník a politik Geoffry Chaucer je také údajně autorem knihy The Equatorie of the Planetis. Tato kniha je vlastně jen doplňkem ke známějšímu Chaucerovu dílu Treatise on the Astrolabe, ve kterém detailně pojednává a popisuje formu a užívání Astrolabu (Astrolab je historický astronomický přístroj na určování a předpovídání poloh hvězd a Slunce užívaný navigátory a astronomy již z dob 4 stol. př. n. l.)

The Equatorie of the Planetis obsahuje šest šifrovaných pasáží. Jedná se opět o jednoduchou substituční šifru, kde písmena abecedy jsou nahrazena číslicemi a symboly.

Obr. č. 11 – Šifra z Equatorie of the Planetis



Na výše uvedeném obrázku je napsáno:

"This table servith for to entre in to the table of equacion of the mone on either side."

"Tato tabulka slouží k zaznamenávání do tabulky postavení měsíce po obou stranách.".[24]

[23] - 6, 11, 53, 80

[24] - 8, 19, 57, 68

5.8. Simeone de Crema (1401)

V arabském světě bylo využití frekvenční analýzy pro dešifrování jednoduchých substitučních šifer známé již v devátém století. V západní Evropě však tato metoda byla pravděpodobně objevena až ve století čtrnáctém.

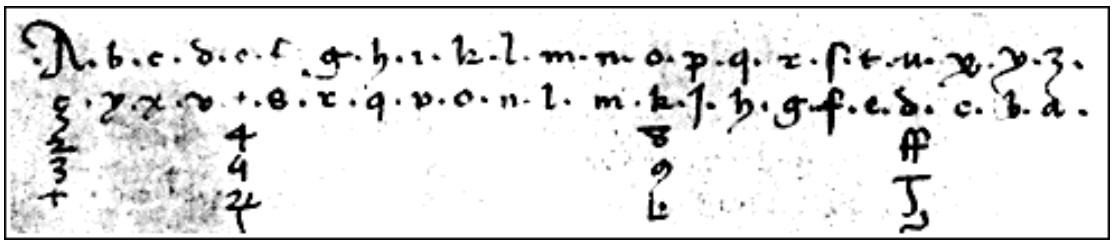
V důsledku tohoto objevu začali učenci a kryptografové hledat nová vylepšení pro tento typ šifrovacího systému. Kvůli principu frekvenční analýzy se samozřejmě jednalo o zakrytí statistických vlastností jazyka v šifrované zprávě, podle kterých by bylo snadné šifru rozluštit.

Výsledkem tohoto snažení byly ve druhé polovině čtrnáctého století homofonní šifry.

Nejstarší dochovaný důkaz (v Evropě) o použití této metody pochází z díla vévody z Mantovy jménem Simeone de Crema a je datován do roku 1401.

Simeone použil klíč, každá samohláska otevřeného textu měla několik možných ekvivalentů.

Obr. č. 12 – Homofonická šifra Simeone de Crema



Tento postup se vlastně snažil vyrovnat frekvenci všech písmen v šifrovém textu a tím ztížit luštění, které je založeno na frekvenční analýze, to sice pomáhalo, ale i přesto mohl být šifrovaný text dekódován.

Primární použití na samohlásky (tedy na písmena, která se nejčastěji opakují) svědčí o tom že Západ v této době již znal kryptoanalýzu a dešifrování pomocí frekvenční analýzy. Homofonní šifra se velmi rychle ujala, ale byla velmi brzy nahrazena novým vylepšeným systémem – nomenklátorem. (viz. nomenklátor)[25]

[25] - 19, 30, 53

5.9. Šifrovací disk Leona Battisty Albertiho (1466 n. l.)

Renesanční umělec, nadaný varhaník, humanista, architekt, lingvista, básník a kryptograf, tím vším je titulován Ital Leone Battista Alberti, který je též často označován za otce evropské kryptologie. Alberti byl velmi všestranně založený člověk, ve své době se zabýval skoro všemi uměními a vědami a jako architekt byl i dokonce jedním z těch, jehož dílo De re aedificatoria posloužilo k přechodu od gotického stylu k renesančnímu.

Battista Alberti se později na podnět svého přítele, papežského sekretáře Leonarda Data, začal věnovat otázkám šifrování. L. Dat měl ve své profesi na starosti právě kryptografii a kryptoanalýzu, se kterými Leona Battistu věrně seznámil, ten pak v roce 1466 (nebo 1467) sepsal 25 stránkovou práci De Cifris (O šifrách), jež byla prvním dílem v západní Evropě, které se věnovalo kryptoanalýze.

De Cifris obsahuje popis luštitelských postupů na základě statistických vlastností a zákonitostí jazyka (tedy i frekvenční analýzu), rozřazení metod šifrování na substituci a transpozici, objev šifrování kódů a hlavně polyalfabetické substituční šifry!

Alberti si povšimnul, že frekvenční analýza textu vede dříve či později k rozluštění monoalfabetických šifer. Tento fakt ho přivedl k vymyšlení polyalfabetické šifry a kombinaci se zašifrováním kódových slov.

Zjednodušeně řečeno by se dalo říct, že polyalfabetická šifra jsou vlastně dvě Ceasarovy šifry u sebe. Je založená na vícenásobné substituci a užití rozmanité abecedy, její princip snadno pochopíme na příkladu šifrovacího disku, který ještě bude podrobněji rozebrán. Tento způsob, i když v mnohem komplexnější a propracovanější, formě byl využit například i ve slavném šifrovacím stroji 2. světové války Enigmě.

Na rychlé a snadné šifrování pomocí polyalfabetické substituce sestrojil Alberti šifrovací disk. Polyalfabetická šifra za užití šifrovacích disků byla v diplomatických kruzích běžně užívaná až do začátku 19. století, kdy byla prolomena. Avšak technika šifrování kódových slov, ač byla mnohem silnější metodou než tehdy užívaný nomenklátor, upadla prakticky v zapomnění a byla vzkříšena až v druhé polovině 19. století!

Velkým přínosem pro kryptografii byl Albertiho vynález, šifrovací disk. Jedná se o nejstarší šifrovací zařízení, které mechanicky uskutečňuje polyalfabetickou substituci.

Šifrovací disk

Šifrovací disk (nazvaný Albertim Formula) se skládá ze dvou otočných kotoučů reprezentujících otevřené a šifrované znaky abecedy. Vnější, větší, nepohyblivý kotouč, zvaný Stabilis, obsahoval písmena, která byla psána normálně postupně za sebou. Vnitřní kotouč byl menší a mohl se otáčet kolem společného středu. Nazývá se Mobilis a písmena na jeho obvodě byla zpřeházená

Každý z kotoučů obsahoval 24 polí. Vnější kotouč také obsahoval číslice od 1 do 4 pro „superzašifrování“ kódové knihy obsahující 336 frází asociovaných s numerickými hodnotami. Toto je velmi účinná metoda jak utajit kódová čísla, dokud jejich ekvivalenty nejsou rozpoznané z ostatních schválně zaměněných písmen.

Obr. č. 13 – Albertiho šifrovací disk

Princip šifrového disku tedy spočíval v tom, že textu po obvodě vnějšího kotouče, se jako zašifrovaná písmena přiřazovala ta, které jim odpovídala z kotouče vnitřního. Pokud by se vnitřní kotouč nemohl pohybovat, jednalo by se jen o další variantu Ceasarovy šifry, tedy další pevnou substituční šifru. Ale proto, že byl pohyblivý,

musela se vždy stanovit vzájemná poloha kotoučů. Proto se vždy na začátku zprávy napsalo například písmeno A, což znamenalo, že v našem případě (viz. obrázek) oproti referenčnímu, prvnímu písmenu g na vnitřním kotouči bude nastavené A na vnějším. Takto je tedy substituce jednoznačně určená! Sám Alberti doporučoval posunout abecedy vždy po třech nebo čtyřech slovech a to náhodně zvoleným nastavením (pootočením) kotoučů. V šifrovaném textu bylo toto nové nastavení opět signalizované novým nastavovacím písmenem.

Máme tedy dva způsoby jak šifrovat. Buď vycházíme z toho, že abeceda otevřeného textu je na vnějším kotouči a nebo na vnitřním. Princip se nemění, záleží jen na domluvě komunikujících

Další Albertiho objev zašifrování kódů, je též veskrze jednoduchý. Využívá se opět šifrovacího disku, akorát na vnitřním kotouči jsou krom čísel také číslice od 1 do 4. Bylo tedy možné zašifrování i těchto číslic. Alberti jen přidal malý slovník (kódovou knihu), kam jednotlivým kódům přiřadil kódový význam a danou kódovanou číslici opět pomocí šifrovacího disku zašifroval tak, jako by to byla písmena. Příjemce nejprve kódy podle použitého systému dešifroval a pak je teprve použil k získání otevřeného textu pomocí kódové knihy.

Princip Albertiho šifrovacího disku se díky jeho dlouholeté odolností vůči rozšifrování stal velmi populární a v mnoha obměnách se k různým účelům používal až do druhé poloviny 20 století!

Velmi známým příkladem je například dekódovací odznak Kapitána Půlnoc (Captain Midnight Decoder Badge) z rozhlasové hry Captain Midnight, nebo použití specielně upraveného šifrovacího disku během Americké Občanské války. Dále se můžeme setkat s různými názvy jako Code-o-graph, Key-o-matic, Plane-puzzle, PF, Ovaltine decoder ring, Mystery dial, Photo-matic, Magni-magic či Mirro flash, ale princip zůstává vždy stejný.[26]

5.10. Sicco Simonetta (1474 n. l.)

Francesco „Cicco“ Simonetta, italský státník a tajemník vlivné rodiny Sfoza, která vládla Milánské republice v 15 století. Dokonce byl Milánským vévodou Francescem

[26] - 28, 31, 33, 56, 60, 64, 78, 82, 88

Sfozou za své zásluhy jmenován „zlatým rytířem“, což odstartovalo jeho pozdější třicetiletou politickou kariérou.

Pro nás je ovšem hlavní spis z roku 1474, který pro své spolupracovníky Simonetta uveřejnil. Jedná se vlastně o manuál pro diplomatické agenty vévodství.

Regulae ad extrahendum litteras zifferatas sine exemplo (Pravidla pro rozluštění šifrovaných dokumentů s příklady) je malý spis, který obsahuje 13 metod luštění zachycených zpráv a množství důležitých statistických dat. Uvádí v něm doporučení užívat jednoduché substituční šifry s potlačením opakování a s vkládáním příležitostných znaků (klamačů).

Tento fakt svědčí o tom, že italské státy v této době již dokázaly rozluštit jednoduché šifry a bylo nutné odbočit od zaběhnutých systémů.

Datum vydání Simonettova spisu se považuje za mezník, od kdy se kryptografie stala univerzální běžnou (vládní a vojenskou) pracovní praxí a kdy se z jednoduchých šifer začaly vyvíjet složité kryptogramy.

Koncem 15. století se stala kryptografie natolik důležitá, že většina států zaměstnávala na plný úvazek šifrovací tajemníky, kteří vytvářeli nové klíče pro šifrování a dešifrování a luštili zachycené zprávy.[27]

5.11. Manuskript Arnalda z Bruselu (1479 n. l.)

Mezi roky 1479 až 1490 sepsal alchymista Arnaldus z Bruselu (Arnaldus de Bruxella) rukopis, kde používá pět řádků šifry na ukrytí rozhodující částí postupu pro výrobu kamene mudrců (tzv. philosopher’s stone).[28]

[27] - 19, 33, 41, 59

[28] - 26

6. ZÁVĚR - SHRNUTÍ

Pro větší přehlednost uvádím tabulku se všemi v této práci popsanými metodami se zařazením do následujících kategorií.

HŠ = homofonní šifra
TŠ = transpoziční šifra
S = steganografie
SŠ = substituční šifra
N = nezařazené , jiné
DK = dílo o kryptologii

Časová osa	Název metody šifrování či díla	HŠ	TŠ	S	SŠ	N	DK
-1900	Nestandardní hieroglyfy				■		
-1500	Recept na glazuru					■	
-600	Atbash				■		
-490	Tetování			■			
-486	Skytale		■				
-479	Vosk			■			
-360	Aenias Taktikos			■	■		
-120	Polybiův čtverec				■		
-50	Caesarova šifra				■		
50	Neviditelný inkoust			■			
200	Leidenský papyrus						■
400	Kama Sutra				■		
725	Al Yahmadího kniha						■
855	Wahshiyya an Nabati				■		
1226	Benátská kryptografie				■		
1250	Roger Bacon						■
1377	Muqaddimah				■		
1379	Nomenklátor				■		
1392	Geofrey Chaucer			■			
1401	Simeone de Crema	■					
1466	Šifrovací disk				■		
1474	Sicco Simonetta				■		■
1479	Arnaldův manuskript					■	

Z výše uvedené tabulky vychází, že nejvíce frekventovanou metodou ve starověkém a středověkém šifrování byla substituční šifra a její různé modifikace a kombinace. Důvodem, proč právě tato metoda, se z dnešního hlediska zdá být právě její jednoduchost, nepřeberné množství možností a kombinací a při správném používání i relativní bezpečnost. Dalším důvodem je, že do objevu frekvenční analýzy byla při správném použití substituční šifra téměř neprolomitelná. Když si připomeneme, že

frekvenční analýza se začala používat v arabském světě kolem roku 1000 a v západní Evropě dokonce až o 400 let později, snadno si uvědomíme, že vlastně ani nebyl moc velký důvod a snaha pro rozvoj dalších způsobů šifrování, protože to nebylo potřeba.

Zaznamenalo tedy lidstvo za tento úsek trvající více než 3500 let velký či malý pokrok v oblasti šifrování? Z dnešního pohledu, kdy díky moderním technologiím jde každý den pokrok kupředu a nové metody jsou objevovány ze dne na den, by se zdálo, že nijak velký pokrok (například oproti posledním 100 letům) během starověku a středověku učiněn nebyl. Mějme však při tomto posuzování na paměti, že musíme brát nejvíc na zřetel celkovou situaci těchto období. Gramotnost, církev, aristokracie, armáda… to jsou hybatele, které měly při vývoji kryptografie až do konce středověku hlavní slovo.

Kryptografie se rozvíjela společně s civilizacemi a také s nimi zanikala. Vývoj byl podmíněn dochováním a následným využíváním odkazů, (především literatury), z nichž následující civilizace mohly čerpat a dosáhnout tak vyššího vývojového stupně. Byl to pomalý a „svízelný“ proces, při kterém bylo mnohem více ztraceno než dochováno. Jednotlivé státy této doby, namísto spolupráce, upřednostňovaly dominanci. Bohužel, stávalo se běžnou praxí, že po ovládnutí jednoho národa druhým, vítěz namísto osvojení si předností a vynálezů porobeného národa se snažil zahladit po poraženém veškeré stopy jeho existence. Tento postup byl kontraproduktivní, stejně jako vzdělání jen pro bohaté a šlechtické vrstvy, či církevní a armádní představitele. Šifrovaná komunikace v těchto dvou epochách probíhala výhradně mezi těmito vrstvami.

Při posuzování vývoje kryptografie také musíme brát v potaz, že přenos informací probíhal výhradně jen fyzickým doručením zprávy z bodu A do bodu B a to tehdejšími dostupnými prostředky... pěšky, na koni či lodí. Tento proces, který někdy trval i několik let, je pro nás téměř nepředstavitelný ve srovnání s dnešními komunikačními technologiemi, kde přenos informací probíhá v reálném čase.

Tato práce se zabývá vývojem kryptografie, který se uskutečnil přibližně od 2000 let před naším letopočtem do roku 1479 našeho letopočtu. Když se na toto rozpětí podíváme z odstupu a v kontextu historickém, uvědomíme si, že vlastní, obecně platné vymezení období starověku a středověku nelze na kryptografii uplatnit. To, co

je mezník pro dějiny lidstva z hlediska společensko politických událostí, není mezník pro dějiny konkrétního oboru, v našem případě kryptologie. Můžeme se proto setkat s historickým dělením na

- Klasickou kryptografii (3500 – 0)
- Středověkou kryptografii, (1 – 1799)
- Kryptografii let 1800 až 1900
- Kryptografii druhé světové války (1901 – 1950)
- Moderní kryptografii (1950 – dnes)

Hraničním letopočtem, kterým je tato práce omezena, je rok 1492, tedy oficiální konec středověku - objevení amerického kontinentu Kryštofem Kolumbem. Avšak další kryptografické mezníky, jako Vigenérova šifra, či rozluštění šifer a následná poprava Marie Stuartovny, se odehrály jen pár desítek let po „oficiálním“ konci středověku. V této práci byly popsány všechny důležité metody šifrování a další mezníky ve vývoji kryptografie v období starověku a středověku, ale historie středověkem nekončí a mnohé ještě zbývá, proto bych se k této tématice v budoucnu určitě ještě rád vrátil.

7. SEZNAM POUŽITÉ LITERATURY

1) ADAMS, Simon. *Šifry a kódy : od hieroglyfů po hackery*. Přeložil Jozef Koval. 1. vyd. Praha : Slovart, 2003. 96 s. ISBN 80-7209-503-X

2) ARGAWAL, Premendra. *Hided messages in Tattoo Scalp* [online]. Chennai : Sulekha.com, 1998-2008 , 24 Mar 08 [cit. 2008-04-09]. Dostupný z WWW: <http://premendra.sulekha.com/blog/post/2007/12/hided-messages-in-tattoo-scalp.htm> .

3) BECKER, Konrad, SÜTZL, Wolfgang . *Cryptography : timeline 00 - 1600 AD* [online]. Vienna : World-Information.Org, 2000-2007 , November 14 - 20, 2005 [cit. 2008-04-29]. Dostupný z WWW: <http://world-information.org/wio/infostructure/100437611776/100438658997> .

4) BEIL, Vojtěch. *Z historie šifrování* [online]. c2002 , 3. 2. 2003 [cit. 2008-04-24]. Dostupný z WWW: <http://sifry.sourceforge.net/extra_history.html> .

5) BITTO, Ondřej. *Historie kryptologie* [online]. Brno : Masarykova univerzita, 2003 , 2003-05-12 [cit. 2008-05-01]. Dostupný z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2003/xbitto.htm> .

6) BLAHO, Peter. *História kryptografie* [online]. Bratislava : Univerzita Komenského v Bratislavě, 2005 [cit. 2008-04-22]. Dostupný z WWW: <http://user.edi.fmph.uniba.sk/winczer/SocialneAspekty/BlahoHistoriaKrypt.htm> .

7) BOND, Chris. *Tales of the Encrypted : timeline* [online]. [1999] , 11/14/99 [cit. 2008-04-11]. Dostupný z WWW: <http://library.thinkquest.org/28005/flashed/timemachine/timeline.shtml> .

8) *Brief history of cryptography* [online]. [USA] : Thawte, c1995-2007 [cit. 2008-04-01]. Dostupný z WWW: <https://www.thawte.com/process/crypto/cryptoBriefHistory> .

9) BULANT, Michal. *Kryptografie a její aplikace*. Praha : CSTUG, 2001 [cit. 2008-04-03]. Dostupný z WWW: <http://www.cstug.cz/slt/01/plne_texty/17.pdf> .

10) COOMBS, Dean. *Atbash Bible Code* [online]. c1997-2008 , Last modified: 26 Apr 2008 [cit. 2008-04-22]. Dostupný z WWW: <http://www.bible-codes.org/atbash_bible_code_river.htm> .

11) *Crypto History : time-travel through cryptography and cryptanalysis* [online]. Frankfurt : Deutsche Bank, c1998-2008 , Site Last Modified: May 6, 2008 - 14:57 [cit. 2008-04-08]. Dostupný z WWW: <http://www.cryptool.org/content/view/28/54/lang,en/> .

12) *Cryptography History : 1500 B.C - Mesopotamia* [online]. Chicago : Trustwave, c2001-2008 [cit. 2008-04-04]. Dostupný z WWW: <https://www.securetrust.com/historyofcryptography/history/mesopotamia>.

13) *Cryptography History : 1900 B.C. Egyptian hieroglyphic writing* [online]. Chicago : Trustwave, c2001-2008 [cit. 2008-04-04]. Dostupný z WWW: <https://www.securetrust.com/historyofcryptography/history/egypt>.

14) *Cryptography History : 486 B.C. Greek Skytale* [online]. Chicago : Trustwave, c2001-2008 [cit. 2008-04-04]. Dostupný z WWW: <https://www.securetrust.com/historyofcryptography/history/greekskytale>.

15) *Cryptography History : 500 - 600 B.C. ATBASH cipher* [online]. Chicago : Trustwave, c2001-2008 [cit. 2008-04-04]. Dostupný z WWW: <https://www.securetrust.com/historyofcryptography/history/atbashcipher>.

16) ČERMÁKOVÁ, Kateřina. *Z dějin kryptografie*. Brno : Mendelova zemědělská a lesnická univerzita v Brně, 2003 [cit. 2008-04-19]. Dostupný z WWW: <https://akela.mendelu.cz/~lidak/bif/cermakova.doc> .

17) DAFOE, Stephen. *Baphomet : the Atbash cipher theory* [online]. Morinville : TemplarHistory.com , c1997-2007 [cit. 2008-05-08]. Dostupný z WWW: <http://www.templarhistory.com/atbash.html> .

18) DOSTÁL, Lukáš. *Voynichův rukopis* [online]. [2007] , 15-Oct-2007 [cit. 2008-04-06]. Dostupný z WWW: <http://www.volweb.cz/musicpra/autor/znalost_%20VM.htm> .

19) DUPUY, Paul. *Early cryptology* [online]. 1996-2002 , 9/30/02 [cit. 2008-04-28]. Dostupný z WWW: <http://home.hiwaay.net/~paul/cryptology/history.html> .

20) EMICK, Jennifer. *Atbash cipher* [online]. New York : About.com, c1996- , Updated: Mon May 5 17:25:24 2008 [cit. 2008-05-06]. Dostupný z WWW: <http://altreligion.about.com/library/glossary/bldefatbashcipher.htm> .

21) FOUSEK, Pavel. *Caesarova šifra : z historie šifrování 2/8* [online]. Praha : IABC, [2001] , 21. 6. 2005 [cit. 2008-04-06]. Dostupný z WWW: <http://www.iabc.cz/scripts/detail.php?id=7241> .

22) GADALLA, Moustafa. *The Egyptian Sacred Numerology* [online]. Greensboro (NC) : Tehuti Research Foundation, 2003 , Last Updated: 28-Mar-2003 [cit. 2008-04-11]. Dostupný z WWW: <http://www.egypt-tehuti.org/articles/sacred-numerology.html> .

23) GEBBIE, Stewart. *Survey of the Mathematics of Cryptology*. Johannesburg : University of Witwatersrand, 2002 [cit. 2008-04-28]. Dostupný z WWW: <http://crypto.cs.mcgill.ca/~gsavvi1/547/gebbie.ps> .

24) GOSLEE, Sarah. *Medieval Cryptography* [online]. [Pennsylvania] : Phiala\'s String Page, 1996-2006 [cit. 2008-05-02]. Dostupný z WWW: <http://www.stringpage.com/other/crypto.html> .

25) GRIFFITH , F.; THOMPSON, Herbert. *The Demotic Magical Papyrus of London and Leiden : introduction* [online]. Santa Cruz : Internet Sacred Text Archive, c2007 , 5/9/2008 [cit. 2008-05-08]. Dostupný z WWW: <http://www.sacred-texts.com/egy/dmp/dmp03.htm> .

26) HAYDEN, Lance, et al. *Cryptography* [online]. Austin : Network Security Resource, [2001] , Spring 2002 [cit. 2008-04-27]. Dostupný z WWW: <http://www.gslis.utexas.edu/~netsec/crypto.html> .

27) KAHN, David. *The Codebreakers : the story of secret writing*. 4. print. New York : Macmillan, 1968. 1164 s.

28) KALLIS, Stephen. *Captain Midnight and decoder rings* [online]. Washington : Metropolitan Washington Old Time Radio Club, c2005 , Modified 27. Febrary 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://www.mwotrc.com/rr2005_08/decoders.htm> .

29) KESSLER, Garry. *Steganography : hiding data within data* [online]. Burlington : Gary Kessler Associates, 2001 , September 2001 [cit. 2008-05-02]. Dostupný z WWW: <http://www.garykessler.net/library/steganography.html> .

30) KOMISARCZUK, Peter. *Data Communications : lecture 6 : cryptography*. Wellington : Victoria University of Wellington, 2006 [cit. 2008-04-25]. Dostupný z WWW: <http://www.mcs.vuw.ac.nz/courses/COMP306/2006T2/lectures/6.crypto.pdf> .

31) KRAJČOVIČ, Jozef. *Alberti, Leon Battista* [online]. 2002-2007 , Posledná aktualizácia: 25.4.2007 [cit. 2008-05-09]. Dostupný z WWW: <http://friedo.szm.sk/krypto/alberti.htm> .

32) KRAJČOVIČ, Jozef. *Dôležité medzníky v histórii kryptológie* [online]. 2002-2007 , Posledná aktualizácia: 25.4.2007 [cit. 2008-05-09]. Dostupný z WWW: <http://friedo.szm.sk/CryptoloHistory.htm> .

33) KRAJČOVIČ, Jozef. *Sprievodca dejinami kryptológie* [online]. 2002-2007 , Posledná aktualizácia: 25.4.2007 [cit. 2008-05-09]. Dostupný z WWW: <http://friedo.szm.sk/hist1.html> .

34) LEWANDOWSKI, Dean; PALMISANO, Mike. *Steganography*. Chicago (Illinois) : DePaul University, 2004 [cit. 2008-04-12]. Dostupný z WWW: <http://ovid.cs.depaul.edu/Classes/CS233-W04/Papers/Steganography.doc> .

35) MAT, Pavel. *Šifry v Bibli : Atbaš* [online]. [Praha] : Mýty a skutečnost, 2002 , Aktualizováno: 26.11.2007 [cit. 2008-05-02]. Dostupný z WWW: <http://www.myty.info/view.php?nazevclanku=sifry-v-bibli-atbas&cisloclanku=2007110003> .

36) MISHRA, Sonu. *The Internet Security : network security : cryptography* [online]. 2007 , February 26, 2008 [cit. 2008-02-28]. Dostupný z WWW: <http://www.mynetsecurity.blogspot.com/2007/05/network-securitycryptography-i.html>.

37) *MR01001101 : early cryptography* [online]. c2004-2005 , 08/05/2005 [cit. 2008-02-28]. Dostupný z WWW: <http://www.mr01001101.co.uk/essays/caesar.html>.

38) *MR01001101 : kronos* [online]. c2004-2005 , 08/05/2005 [cit. 2008-02-28]. Dostupný z WWW: <http://www.mr01001101.co.uk/KRONOS/welcome.html>.

39) PELLING, Nick. *Voynich News : dots for vowels, revisited* [online]. 2007- , Saturday, 10 May 2008 [cit. 2008-04-22]. Dostupný z WWW: <http://voynichnews.blogspot.com/2008/02/dots-for-vowels-revisited.html> .

40) *Praktické základy kryptologie a steganografie* [online]. Security-Portal.cz, c2005-2008 , 08.04.2008 [cit. 2008-04-27]. Dostupný z WWW: <http://www.security-portal.cz/clanky/prakticke-zaklady-kryptologie-a-steganografie.html> .

41) PRATT, Fletcher. *Secret and Urgent : basic substitution ciphers*. Walnut Creek (California) : Aegean Park Press, 1996 [cit. 2008-04-01]. Dostupný z WWW: <http://cryptology.dod.net/uploads/documents/applied_cryptography/se01.pdf> .

42) SHAN. *Cryptology : middle ages timeline* [online]. Machinae, c2005-2007 , 26. 12. 2006 [cit. 2008-05-08]. Dostupný z WWW: <http://www.machinae.com/crypto/timelinemid.html> .

43) SINGH, Simon. *Caesar Shift Cipher* [online]. London : SimonSingh.net, [2007] , 22. April 2007 [cit. 2008-05-08]. Dostupný z WWW: <http://www.simonsingh.net/The_Black_Chamber/home.html> .

44) SINGH, Simon. *Kniha kódů a šifer : tajná komunikace od starého Egypta po kvantovou kryptografii*. Přeložili Petr Koubský a Dita Eckhardtová. 1. v českém jazyce vyd. Praha : Dokořán, 2003. 382 s. Aliter; sv. 9. ISBN 80-86569-18-7.

45) STWORA, Vladimír. *Steganografie : způsob komunikace zítřka* [online]. Toronto : Vladimír Stwora, c1999-2008 , Poslední aktualizace 09. 05. [cit. 2008-05-02]. Dostupný z WWW: <http://www.zvedavec.org/techpor/2001/11/216-steganografie-zpusob-komunikace-zitrka.htm?PHPSESSID> .

46) ŠTRÁFELDA, Jan. *Hebrejský atbash* [online]. Velvary : Shaman.cz, c2001-2008 , Aktualizováno 19. prosince 2005 [cit. 2008-05-01]. Dostupný z WWW: <http://www.shaman.cz/sifrovani/hebrejsky-atbash.htm> .

47) ŠTRÁFELDA, Jan. *Polybiův čtverec* [online]. Velvary : Shaman.cz, c2001-2008 , Aktualizováno 15. ledna 2006 [cit. 2008-05-01]. Dostupný z WWW: <http://www.shaman.cz/sifrovani/polybiuv-ctverec.htm> .

48) *The man who cracked the Kama Sutra code* [online]. London : Telegraph Media Group, c2000-2008 , ast Updated: 12:01am GMT /10/2000 [cit. 2008-04-29]. Dostupný z WWW: <http://www.telegraph.co.uk/connected/main.jhtml?xml=/connected/2000/10/05/ecfcode05.xml> .

49) *Timeline of cryptography development* [online]. Cary (NC) : Research Triangle Software, 2003-2007 [cit. 2008-04-11]. Dostupný z WWW: <http://www.cryptostick.com/cryptographytimeline.php> .

50) VONDRUŠKA, Pavel. *Cesta kryptografie do nového tisíciletí: od Kámasutry k osobním zápiskům K. H. Máchy* [online]. 2002 , 12.09.2000 [cit. 2008-05-09]. Dostupný z WWW: <http://friedo.szm.sk/krypto/CW/Cesta1.htm>.

51) VONDRUŠKA, Pavel. Cesta *kryptografie do nového tisíciletí: od Kámasutry k osobním zápiskům K. H. Máchy*. Praha : Crypto-World, 2000 [cit. 2008-04-24]. Dostupný z WWW: <http://www.math.muni.cz/~bulik/vyuka/aplikace/vondruska-cesta.pdf> .

52) VONDRUŠKA, Pavel. *Mikulášská kryptobesídka 2007*. Praha : Crypto-World, 2007 [cit. 2008-04-10]. Dostupný z WWW: <http://crypto-world.info/vondruska/prezentace/mkb_07.ppt> .

53) VONDRUŠKA, Pavel. Přehled a historie polyalfabetických šifer. *Crypto-World : informační sešit GCUCMP* [online]. 2007, roč. 9, č. 6 [cit. 2008-05-01], s. 2-11. Dostupný z WWW: <http://crypto-world.info/casop9/crypto06_07.pdf>. ISSN 1801-2140.

54) ZECHER, Henry. *The Papyrus Ipuwer, Egyptian Version of the Plagues : a new perspective* [online]. [Wisconsin] : Henry Zecher, c2006 , Last modified: 09/17/06 [cit. 2008-05-02]. Dostupný z WWW: <http://www.henryzecher.com/papyrus_ipuwer.htm> .

Hesla ve Wikipedii

55) Aelianus Tacticus. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Aelianus_Tacticus> .

56) Alberti Cipher Disk. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Alberti_Cipher_Disk> .

57) Astroláb. In *Wikipedie : otevřená encyclopedie* [online]. Praha : Wikimedia Česká republika, 2002- , nap. edit. 26. 2. 2008 [cit. 2008-05-06]. Dostupný na WWW: <http://cs.wikipedia.org/wiki/Astrol%C3%A1b> .

58) Caesar cipher. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Caesar_cipher> .

59) Cicco Simonetta. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Cicco_Simonetta> .

60) Cipher disk. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Cipher_disk> .

61) Cipher. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Cipher> .

62) Ciphering. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Ciphering> .

63) Code (cryptography). In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Code_%28cryptography%29> .

64) Code-O-Graph. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Code-O-Graph> .

65) Cryptography. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Cryptography> .

66) Egyptian hieroglyphs. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 3 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Egyptian_hieroglyphs> .

67) Frequency analysis. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Frequency_analysis> .

68) Geoffrey Chaucer. In *Wikipedie : otevřená encyclopedie* [online]. Praha : Wikimedia Česká republika, 2002- , nap. edit. 26. 2. 2008 [cit. 2008-05-06]. Dostupný na WWW: <http://cs.wikipedia.org/wiki/Geoffrey_Chaucer> .

69) History of cryptography. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/History_of_cryptography> .

70) Ibn Khaldun. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Ibn_Khaldun> .

71) Ibn Washiyya. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Ibn_Wahshiyya> .

72) Immanuel Velikovsky. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Immanuel_Velikovsky> .

73) Ipuwer papyrus. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Ipuwer_papyrus> .

74) Julius Caesar. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Julius_Caesar> .

75) Kamasutra. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Kamasutra> .

76) Klínové písmo. In *Wikipedie : otevřená encyclopedie* [online]. Praha : Wikimedia Česká republika, 2002- , nap. edit. 26. 2. 2008 [cit. 2008-05-06]. Dostupný na WWW: <http://cs.wikipedia.org/wiki/Kl%C3%ADnov%C3%A9_p%C3%ADsmo> .

77) Kryptografie. In *Wikipedie : otevřená encyclopedie* [online]. Praha : Wikimedia Česká republika, 2002- , nap. edit. 26. 2. 2008 [cit. 2008-05-06]. Dostupný na WWW: <http://cs.wikipedia.org/wiki/Kryptografie> .

78) Leone Battista Alberti. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Leone_Battista_Alberti> .

79) Muqaddimah. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Muqaddimah> .

80) Nomenclator. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Nomenclator> .

81) Pliny the Elder. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Pliny_the_Elder> .

82) Polyalphabetical cipher. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Polyalphabetic_cipher> .

83) Polybios square. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Polybius_square> .

84) Polybios. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Polybios> .

85) Roger Bacon. In *Wikipedie : otevřená encyclopedie* [online]. Praha : Wikimedia Česká republika, 2002- , nap. edit. 26. 2. 2008 [cit. 2008-05-06]. Dostupný na WWW: <http://cs.wikipedia.org/wiki/Roger_Bacon> .

86) ROT13. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/ROT13> .

87) Scytale. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Scytale> .

88) Secret decoder ring. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Secret_decoder_ring> .

89) Secret key. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: < http://en.wikipedia.org/wiki/Secret_key> .

90) Substitution cipher. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Substitution_cipher> .

91) Transposition cipher. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Transposition_cipher> .

92) Voynich manuscript. In *Wikipedia : the free encyclopedia* [online]. San Francisco (California) : Wikimedia Foundation, 2001- , last modif. 1 May 2008 [cit. 2008-05-08]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Voynich_manuscript> .

8. SEZNAM OBRÁZKŮ

Evidence výpůjček

Prohlášení:
Dávám svolení k půjčování této bakalářské práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

V Praze, 1. 5. 2005

David Prokopič

Jméno	Katedra / Pracoviště	Datum	Podpis