Univerzita Hradec Králové

Přírodovědecká fakulta

BAKALÁŘSKÁ PRÁCE

2017 **Pavel Musílek**

UNIVERZITA HRADEC KRÁLOVÉ

Přírodovědecká fakulta

Katedra kybernetiky

Historie šifrování

Bakalářská práce

Autor:	Pavel Musílek
Studijní program:	B1801 - Informatika
Studijní obor:	Historie se zaměřením na vzdělávání
	Informatika se zaměřením na vzdělávání
Vedoucí práce:	doc. RNDr. Štěpán Hubálovský, Ph.D.

Hradec Králové **2017**

Univerzita Hradec Králové

Přírodovědecká fakulta

Zadání bakalářské práce

Autor:	Pavel Musílek
Studijní program:	B1801 - Informatika
Studijní obor:	Historie se zaměřením na vzdělávání
	Informatika se zaměřením na vzdělávání
Název práce:	Historie šifrování
Název práce v Aj:	History of cyphering
Cíl a metody práce:	Cílem teoretické práce bude podat ucelený přehled vývoje a základních typů klasických ručních šifer. Teoretická část práce bude zpracována formou literární rešerše a bude shrnovat vývoj klasických ručních šifer, jejich typologii, způsoby šifrování a dešifrování a u několika vybraných jednoduchých typů šifer i luštění. Shrne dosavadní dostupné informace o vztahu mezi kryptologií a výukou informatiky. Cílem praktické části práce bude vytvoření studijního materiálu podporujícího využití klasických ručních šifer ve výuce informatiky. Praktická část práce bude zpracována formou sady pracovních listů s úlohami různé obtížnosti. Významnou součástí pracovních listů bude u vybraných typů šifer historický kontext, ve kterém daný typ šifer vznikl, nebo byl používán, nebo měl výrazný vliv na konkrétní historické události. Tím budou akcentovány mezipředmětové vztahy mezi informatikou a dějepisem, což by mohlo pozitivně ovlivnit vztahy mezi přírodovědným a společenskovědním myšlením.
Garantující pracoviště:	Katedra kybernetiky, Přírodovědecká fakulta
Vedoucí práce:	doc. RNDr. Štěpán Hubálovský, Ph.D.
Oponent:	Mgr. et Bc. Radek Němec, Ph.D.
Datum zadání práce:	7. 10. 2016
Datum odevzdání práce:	28. 4. 2016

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně a že jsem v seznamu použité literatury uvedl všechny prameny, z kterých jsem vycházel.

V Hradci Králové dne 28. 4. 2017 Pavel Musílek

Poděkování

Rád bych poděkoval doc. RNDr. Štěpánu Hubálovskému, Ph.D. za užitečné rady a vstřícný přístup při vedení diplomové práce. Zároveň bych rád poděkoval mému otci, který mě k šifrování přivedl a byl mi vždy dobrým učitelem a rádcem.

Anotace

MUSÍLEK, P. *Historie šifrování*. Hradec Králové, 2017. Bakalářská práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí diplomové práce Štěpán Hubálovský. 30 s.

Cílem práce bylo stručně zmapovat historii šifrování s důrazem na klasické ruční substituční šifry od starověku po konec 20. století. Historii šifrování lze vnímat jako souboj mezi tvůrci šifrových systémů (kryptografy) a učenci, využívajícími znalosti z oblasti jazykovědy, matematiky a logiky k luštění šifrových textů bez znalosti použitého systému nebo hesla (kryptoanalytiky). Praktická část práce má formu sady pracovních listů s úlohami různé obtížnosti, které provedou žáky klíčovými okamžiky historie kryptologie a spojují na první pohled tak odlehlé oblasti lidské kultury, jakými jsou informatika a historie.

Klíčová slova: šifrování, kryptologie, kryptografie, kryptoanalýza, historie, pracovní listy

Annotation

MUSÍLEK, P. *Historie šifrování*. Hradec Králové, 2017. Bakalářská práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí diplomové práce Štěpán Hubálovský. 30 s.

The goal of the thesis was to map the history of cyphering with an emphasis on classical manual substitution codes from antiquity to the late 20th century. History of ciphering can be seen as a battle between creators of cipher systems and scholars who use knowledge of language, matematics and logic for deciphering ciphered texts without knowledge of used system or key. The practical part of the thesis is composed of set of worksheets with exercises of varying difficulty.

Key words: ciphering, cryptology, cryptography, cryptanalysis, history, worksheets

Obsah

ÚVOD

Téma historie šifrování jsem si vybral proto, že spojuje dvě zajímavé oblasti lidského poznání, historii a matematiku. Inspirovalo mě také poutavé líčení zajímavostí z historie šifrování a kódování v knize Pierra Berloquina. (Berloquin, 2011) Už ve starověku měli zejména politici a válečníci potřebu utajit některé důležité zprávy před svými soupeři a nepřáteli. Na utajení informací před nepovolanými osobami závisel často úspěch politické intriky, či strategie použité v důležité bitvě. Vznikly tak první dvě součásti vědy o utajování informací – ***kryptologie***, kterými jsou nauka o utajování samotné existence tajných zpráv – ***steganografie*** a nauka o různých metodách šifrování – ***kryptografie***.V této práci jsem se rozhodl, že se nebudu příliš zabývat ***steganografií***, přestože se jedná o velmi zajímavé téma, do kterého patří např. výroba a použití neviditelných inkoustů, ale soustředím se předně na šifrování.

Šifrovanou zprávu přes veškerou opatrnost poslů nepřítel zachytil, a tu pak příslušný velitel předložil nejchytřejším, ze svých poradců a žádal je o rozluštění zprávy. Tak vznikla třetí, nejspíš nejzajímavější součást vědy o utajování zpráv, a to nauka o luštění šifrových textů – ***kryptoanalýza***.

Výzvou je pro mne možnost pokusit se o akcentování mezioborových vztahů mezi na první pohled odtažitými předměty - společenskovědním dějepisem a přírodovědnou informatikou.

Literární oporou v mé práci se mi staly zejména knihy Skryté kódy a velkolepé projekty od Pierra Berloquina (2011), Kniha kódů a šifer od Simona Singha (2009) a Kryptologie, šifrování a tajná písma od Pavla Vondrušky (2006). Velmi mi v mé práci pomohly stránky: www.musilek.eu, (2010) jejichž autorem je Michal Musílek. Tyto i ostatní autory pro lepší přehlednost dále zmiňuji v závěrečném seznamu literatury.

CÍLE PRÁCE

Cílem teoretické práce bude podat ucelený přehled vývoje a základních typů klasických ručních šifer. Teoretická část práce bude zpracována formou literární rešerše a bude shrnovat vývoj klasických ručních šifer, jejich typologii, způsoby šifrování a dešifrování a u několika vybraných jednoduchých typů šifer i luštění. Shrne dosavadní dostupné informace o vztahu mezi kryptologií a výukou informatiky.

Cílem praktické části práce bude vytvoření studijního materiálu podporujícího využití klasických ručních šifer ve výuce informatiky. Praktická část práce bude zpracována formou sady pracovních listů s úlohami různé obtížnosti. Významnou součástí pracovních listů bude u vybraných typů šifer historický kontext, ve kterém daný typ šifer vznikl, nebo byl používán, nebo měl výrazný vliv na konkrétní historické události. Tím budou akcentovány mezipředmětové vztahy mezi informatikou a dějepisem, což by mohlo pozitivně ovlivnit vztahy mezi přírodovědným a společenskovědním myšlením.

1 ZÁKLADNÍ KRYPTOLOGICKÉ POJMY

1.1 Šifrování, dešifrování a luštění

Je zajímavé, jak často se chybuje v některých základních pojmech. Dobře je vysvětluje kryptolog Pavel Vondruška (2006):

Původní text zprávy, ještě předtím, než byl zašifrován, se nazývá ***otevřený text*** nebo otevřená zpráva. Zašifrované zprávě říkáme **šifrový text** nebo šifrová zpráva. Anglická literatura používá označení ***plain text*** a ***cipher text***.

Pro zápis otevřeného textu se běžně používá ***mezinárodní abeceda***, tj. 26 písmen bez diakritiky. Jsou to písmena A, B, D, E, F, G, H, I, J, K, L, M, N, O, P ,Q, R, S, T, U, V, W, X, Y, Z. V praxi to znamená, že z českého textu zpravidla před šifrováním odstraníme diakritiku (háčky a čárky nad písmeny) i interpunkci (čárky, tečky, středníky, vykřičníky, otazníky, dvojtečky a uvozovky). ***Šifrová abeceda*** může používat běžná písmena (latinku) nebo také docela jiné znaky (např. řeckou abecedu, či různé grafické značky, jako jsou křížky, šipky, hvězdičky apod.). Velmi často se ale používá i k zápisu šifrového textu mezinárodní abeceda, takže abeceda otevřeného textu a šifrová abeceda mohou být stejné.

Šifrování je postup, kterým z otevřeného textu vytvoříme šifrový text na základě známého ***algoritmu*** a ***klíče*** (hesla). Pokud je celé šifrování založeno pouze na algoritmu a neumožňuje obměnu změnou klíče, říkají kryptologové, že jde o ***omezený algoritmus***. ***Dešifrování*** je postup, kterým z šifrového textu na základě známého algoritmu a klíče získáme otevřený text. Naproti tomu ***luštění*** šifrové zprávy je postup, kterým se snažíme získat otevřený text, aniž bychom znali použitý klíč, nebo, v horším případě, aniž bychom znali použitý šifrovací systém. Pokud se nám taková činnost podaří, říkáme, že jsme šifru ***zlomili*** (prolomili, rozbili, anglicky ***break***).

Jiří Janeček věnuje celou jednu kapitolu své knihy (2008) upozornění na časté nesprávné používání pojmu dešifrování místo luštění a s tím úzce souvisejícího označení dešifranti místo luštitelé. Toto nedorozumění vzniká mimo jiné předkladem z angličtiny, kde se používají pojmy ***encrypting*** a ***decrypting*** pro šifrování a dešifrování, zatímco anglické ***deciphering*** znamená luštění, nikoliv dešifrování!

2 První starověké šifry a jejich luštění

2.1 Počátky šifrování

Historie šifrování se začala psát okolo roku 1500 př. n. l. ve staré Mezopotámii. Pavel Vondruška se ve své knize zmiňuje o neznámém mistrovi, který tehdy vyryl do destičky text obsahující skryté úřední tajemství. Použitá šifra, využívá jednoduchou záměnu klínopisných písmen za jiná klínopisná písmena, která mají stejnou zvukovou podobu (Vondruška, 2006). Takový systém se brzy ukázal jako ne příliš spolehlivý, proto se přestal používat a dal prostor novým a bezpečnějším.

2.2 Šifra, s níž se setkáme v Bibli – atbaš

Jedna z nejstarších substitučních šifer se vyskytuje v Bibli, konkrétně v knize Jeremiáš, kapitole 25, verš 26 a kapitole 51, verš 41. Namísto názvu města Babel, se tu objevuje jméno Šešak. Tato záměna vznikla už v hebrejském textu, okolo roku 500 př. n. l., kdy pisatel zaměnil druhé písmeno hebrejské abecedy bét, předposledním šin a dvanácté lamed jedenáctým kaf. Vezmeme-li to popořadě, zamění se první písmeno abecedy alef posledním tav, druhé bet předposledním šin, tedy A-T, B-Š a odtud název šifry atbaš. Koho to zajímá, může si hebrejskou abecedu, která má 22 písmen, vyhledat např. na Wikipedii. My ale převedeme systém ***atbaš*** na naši mezinárodní abecedu a znázorníme šifrování zkrácenou převodovou tabulkou:

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

Stejnou tabulku použijeme pro šifrování i dešifrování. Vždy vyhledáme dané písmeno a nahradíme ho písmenem ve stejném sloupci ale jiném řádku. Ukážu to stejně jako u předchozích šifer na příkladu. Zašifruji větu: Komu není shůry dáno, v apatyce nekoupí.

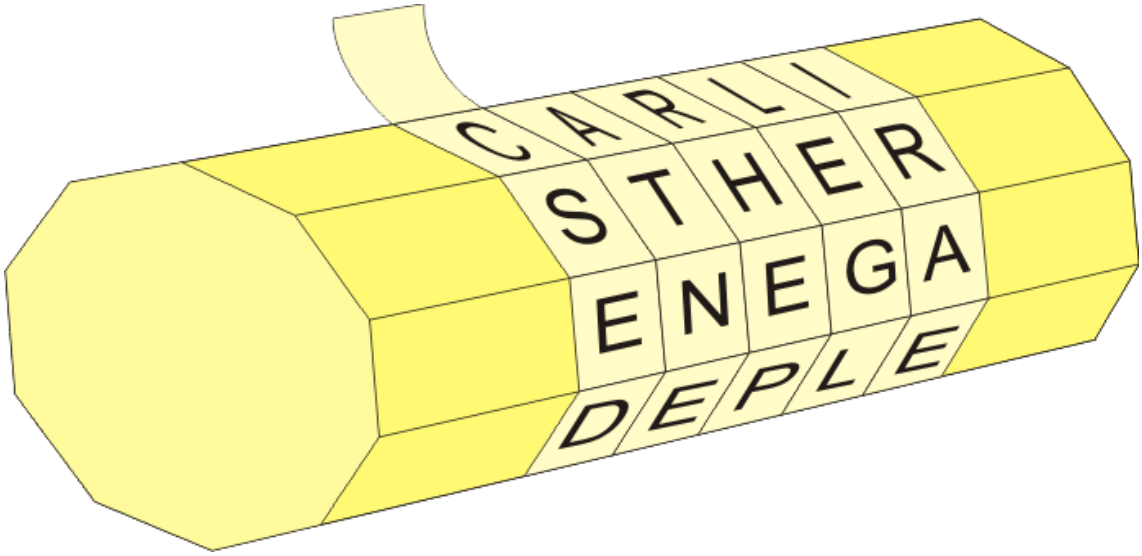
```
KOMUN ENISH URYDA NOVAP ATYCE NEKOU PI
PLNFM VMRHS FIBWZ MLEZK ZGBXV MVPLF KR
```

Samotná šifra atbaš neumožňuje obměnu pomocí klíče, jde o omezený algoritmus. Bylo by ale možné získat podobné šifry např. cyklickým posouváním písmen ve spodním řádku tabulky (cyklickým znamená, že vysunuté písmeno nevypadne z tabulky, ale

vrací se na její začátek), ale to už by byly jiné šifry typu jednoduchá záměna. Atbaš je jen jeden.

2.3 Řecké vynálezy

O pouhé století později přichází Sparťané, nejobávanější z Řeků, s prvním technickým zařízením na utajení tajných zpráv - skytalé. Ta funguje na principu ***transpozice***, která spočívá ve změně pořadí písmen ve zprávě. Odesílatel i příjemce zprávy museli mít silné dřevěné hole stejného tvaru a velikosti. Před psaním zprávy se na hůl navinul šroubovitě proužek papyru. Zpráva se pak psala napříč závity papyru, takže po odvinutí byla na proužku nesrozumitelná řada písmen. Příjemce potom proužek opět navinul, tentokrát na svou skytalé, a pohodlně přečetl.



Obr. 1 Skytalé – převzato z WikimediaCommons (licence CreativCommons BY-SA 3.0)

Nejčastěji uplatňovaným řeckým postupem pro utajení zprávy byla však steganografie. Konkrétní příklad popsal Herodotos ve svých Dějinách, viz (Vondruška, 2006). Histiaeus potřeboval nutně poslat zprávu svému příbuznému, tyranu Aristagorovi do Milétu, aby tak pomohl koordinaci povstání proti Peršanům. Aby zpráva dorazila v pořádku nedotčena, nechal svému poslu oholit hlavu, poté na jeho lebku napsal vzkaz, a když mu vlasy opět narostly, mohl jej vyslat na cestu.

2.4 Slavná Césarova šifra

Asi nejznámější šifrou starověké civilizace je tzv. Césarova šifra. Slavný římský vojevůdce používal několik různých šifer (Singh, 2009). Jedna z nich spočívala např.

v nahrazení římských písmen řeckými. Caesarovo jméno dodnes nese jednoduchý systém šifrování, který spočívá v nahrazení každého písmene písmenem, které stojí v abecedě o tři pozice dále. Jde tedy o substituční šifru. Jestliže nahrazujeme stejné písmeno vždy stejným znakem, mluvíme o ***jednoduché substituci***, anglicky ***monoalphabetical substitution***. Takový typ šifry můžeme znázornit tzv. ***převodovou tabulkou***:

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

Při šifrování najdeme písmeno v horním řádku a nahradíme ho písmenem, které je pod ním v dolním řádku. Při dešifrování vyhledáme písmeno v dolním řádku a nahrazujeme písmenem, které je nad ním. Ukážu to na příkladu šifrování věty: Dnes jsem překročil Rubikon.

```
DNES JSEM PREKROCIL RUBIKON
GQHV MVHP SUHNURFLO UXELNRQ
```

Pro znesnadnění luštění se šifrový text zpravidla ještě přeskupí do pětimístných skupin písmen, takže zašifrovaná věta bude vypadat takto:

```
GQHVM VHPSU HNURF LOUXE LNRQ
```

Přestože text působí na první pohled nečitelně, jde o poměrně slabý šifrový systém. I když ho můžeme obměňovat tím způsobem, že dolní řádek posuneme o jiný počet písmen, zjistíme, že možných posunů, tedy v tomto případě klíčů, je jen 25. Posun o 1, 2, 3, 4, …, 24, 25 znaků. Při posunutí o 26 znaků se budou písmena v horním a dolním řádku stejná, jako kdybychom je vůbec neposunuli, a pak se začnou opakovat už dříve použitá posunutí.

3 Středověká kryptografie

3.1 Luštění jednoduché záměny

Caesarova šifra i atbaš jsou jednoduchými příklady ***monoalfabetické substituční šifry***. Když je budeme všelijak obměňovat, nebo vytvoříme převodovou tabulku, v jejímž dolním řádku budou písmena nepravidelně zpřeházená, zkomplikujeme luštitelům práci, ale přesto nezabráníme, aby šifru zlomili. Jestliže totiž máme dostatečně dlouhý šifrový text, který byl získaný jednoduchou (neboli monoalfabetickou) substitucí, budou se v něm některé znaky vyskytovat mnohem častěji než jiné, stejně jako se v původním otevřeném testu vyskytují některá písmena mnohem častěji než jiná. V českém textu půjde například o písmena E (10,5 %), A (8,8 %), O (8,3 %), I (7,7 %), N (6,7 %), viz statistické údaje Centra zpracování přirozeného jazyka (kolektiv, 2008). Také v jiných jazycích jsou mezi nejčastějšími písmeny především samohlásky. Porovnáním zastoupení znaků v šifrovém textu se statistickými údaji daného jazyka je možné odhadnout části luštěné zprávy a dalším upřesňováním metodou pokus – omyl (otevřený text musí dávat smysl, musí vznikat srozumitelná slova) zprávu vyluštit.

Uvedená metoda se nazývá ***frekvenční analýza*** a jako první ji popsal Abú Júsuf Jaqúb ibn Isháq ibn as-Sabbáh ibn Omrán ibn Ismail al-Kindí (Singh, 2009). Tento arabský učenec, který se zabýval jazykovědou, matematikou, astronomií, hudbou a lékařstvím, ji popsal již v 9. století. Tak, jak k nám ve středověku pronikala prostřednictvím Arabů kultura a vzdělanost antických klasiků, či matematické poznatky, uvědomili si také středověcí politici a vojevůdci, že jednoduchá záměna není bezpečným způsobem šifrování. Proto začali vymýšlet dokonalejší šifrovací systémy.

3.2 Chemie v tajné korespondenci

Spolu s šifrovacími systémy se vyvíjela i steganografie. Okolo roku 1400 arabský učenec Egypťan Šiháb al-Qalqa-šandí ve svém díle podrobně popisuje několik typů neviditelných inkoustů, které jsou založeny na různých chemických reakcích. Neviditelným inkoustem se tajná zpráva většinou vepisovala mezi nedůležitou, klamavou zprávu, psanou obyčejným inkoustem.

3.3 Odbočka na cestě k polyalfabetické substituci – nomenklátory

Jednou z možných cest bylo nahrazovat nejčastější písmena několika různými znaky. Znaky vyjadřující jedno písmeno, nejčastěji samohlásku, se nazývají homofony, a odtud i název ***homofonní substituce***. Tyto šifry jsou ale komplikované, protože musí mít víc znaků, než má písmen abeceda. Navíc se jako další vylepšení začaly vkládat do textu znaky, které neznamenaly vůbec nic a měly jen oklamat luštitele, těm se říkalo klamače. Jiné vylepšení spočívalo v nahrazení celých, často používaných slov jedním znakem. Takové kombinaci homofonní šifry, klamačů a značek pro celá slova, případně dalších speciálních značek (např. v angličtině pro zdvojená písmena) se říká nomenklátor. První nomenklátory pravděpodobně vytvořil roku 1379 Ital Gabrieli di Lavinde pro vzdoro-papeže Klamenta VII. (Vondruška, 2006).

3.4 Polyalfabetická substituce s periodickým heslem

Nomenklátory byly velmi složité. Pro tajnou diplomatickou korespondenci se používal mnoho dalších století a rozrostly se na celé kódové knihy, které obsahovaly značky a kódy pro mnoho různých slov, či dokonce krátkých vět. Pro vojenské použití, případně pro šifrování obchodních sdělení však nebyly prakticky použitelné. Proto pokračovaly pokusy o vytvoření jednoduchého systému, který by odolával luštění lépe než obyčejná monoalfabetická substituce. První nápad v tomto směru měl renesanční polyhistor Leon Battista Alberti, který v 60. letech 15. století popsal šifru spočívající v pravidelném střídání dvou či více monoalfabetických substitucí. Jeho pokračovateli byli Johannes Tritheimus, Giambattista della Porta a nakonec Blaise de Vigenère. Po posledním z nich je pojmenována Vigenèrova šifra, kterou si nyní popíšeme. K šifrování a dešifrování nám tentokrát nebude stačit převodová tabulka, ale použijeme velkou čtvercovou tabulku, kterou publikoval již Johannes Tritheimus pod názvem ***tabula recta***, ale často se jí říká také Vigenèrův čtverec:

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

Šifrování se řídí ***periodickým heslem***, to znamená, že postupně střídáme jednotlivá písmena dohodnutého klíče. V průsečíku řádku začínajícího příslušným písmenem klíče a sloupce určeného nahrazovaným písmenem otevřeného textu najdeme písmeno, které zapíšeme do šifrového textu. Při dešifrování postupujeme opačně, to znamená, že v řádku určeném příslušným písmenem klíče najdeme dané písmeno šifrového textu a od něj jdeme svisle vzhůru do první řady. V první řadě pak najdeme odpovídající písmeno otevřeného textu. Ukažme si to opět na příkladu. Pomocí periodického hesla ALBERTI zašifruji větu: Studium historie šifrování je napínavé.

```
KLÍČ:   ALBER TIALB ERTIA LBERT IALBE RTIAL BERT
OT:     STUDI UMHIS TORIE SIFRO VANIJ ENAPI NAVE
ŠT:     SEVHZ NUHTT XFKQE DJJIH DAYJN VGIPT OEMX
```

Další dvě obměny polyalfabetických substitucí s periodickým heslem, které používají stejnou tabulku ***tabula recta*** jako Vigenèrova šifra, navrhli kolem roku 1710 italský kryptolog Giovanni Sestri a kolem roku 1850 anglický admirál sir Francis Beaufort, který je známý svou stupnicí síly větru. Výhoda posledně jmenovaného systému

spočívá v tom, že se stejným způsobem šifruje i dešifruje. Jiné šifrovací tabulky používá originální systém Giambattisty della Porta z roku 1563. Pokud si budeme chtít ušetřit práci, vyžadující soustředění při hledání v tabulce a neustálém střídání použitých řádků a sloupců, můžeme použít skripty dostupné na webu (Musílek, 2010), které šifrování i dešifrování provedou s počítači vlastní rychlostí a přesností. Polyalfabetické substituce byly považovány za nerozluštitelné až do druhé poloviny 19. století.

4 Novodobé dějiny šifrování

4.1 Nová doba si žádá nové služby

V roce 1500 vzniká v Benátské republice první šifrovací a luštitelská služba řízená Radou Deseti. Hlavou instituce se stal Giovani Soro, jeden z největších luštitelů západního světa. Je ovšem znám především jako autor nomenklátoru (všeobecné šifry), jejíž význam spočívá v umožnění velvyslancům vzájemný styk mezi sebou. Navíc měl pak každý vyslanec tzv. Speciální šifru, kterou používal pouze pro zasílání a dešifrování zpráv z a do Benátek. Nomenklátor použil například Hernando Cotéz v roce 1532, když měl odeslat dopis o dobytí Mexika. Zašifrovaná zpráva o jeho vítězství se dochovala. Zajímavé je, že luštitelé v státních službách tehdy patřili mezi vážené občany a dobře placené úředníky. Pokud by však vyzradili státní tajemství šifrovaných textů, hrozila jim smrt.

O několik let později vznikají i první soutěže v šifrování. Jakákoliv novinka v oboru byla odměněna až 100 dukáty, což představuje roční plat tamního dvořana. Např. v roce 1525 zvítězil Marco Rafael (pozdější oblíbenec anglického krále Jinřicha VIII.) tím, že objevil a převedl nový způsob neviditelného psaní. (Vondruška, 2006)

4.2 Nomenklátor Marie Stuartovny

Vraťme se nyní na okamžik do roku 1586, kdy byla souzena skotská královna Marie Stuartovna. Marie byla obžalována pro velezradu, tedy údajné spiknutí, které pomáhala vést proti své sestřenici královně Alžbětě v touze po jejím trůnu. K doznání byli přivedeni všichni spiklenci, zejména angličtí katoličtí šlechtici vedeni proslaveným Mariiným obdivovatelem Anthony Babingtonem a následně byli také popraveni. Až na samotnou Stuartovnu. I přes všechna důvodná podezření, ji nebylo možné bez pádného a hmatatelného důkazu odsoudit. Sir Francis Walsingham – Alžbětin tajemník, měl být tím, komu se podaří prokázat její vinu.

Simon Singh (2009) se o tento případ velmi zajímal a zjistil k němu následující. Když ještě Babington a jeho společníci byli naživu, měli veliké plány. Osvobodit Stuartovnu, zavraždit protestantskou královnu Alžbětu a následně udělat vše pro to, aby v zemi proběhla rekatolizace. K tomu účelu neváhali ani vyzvat ostatní evropské katolické státy k útoku na Anglii.

K takovému počínání ovšem bylo zapotřebí získat Mariin souhlas. Dopis psaný Babingtonovou rukou, který ji byl tajně doručen, ji měl přesvědčit o jeho úmyslech v naději, že mu panovnice dá svolení. Doručil jej muž, který Babingtonovi nabídl své služby - Gilbert Gifford, katolík, který se z Marií znal, už dlouhý čas ji doručoval dopisy z francouzského vyslanectví, které tam posílali katoličtí přívrženci ze zahraničí. Pracoval jako dvojitý agent. Celou tu dobu, po kterou se zdál být Marii důvěrníkem, vyzrazoval informace a předával veškeré její dopisy již zmíněnému siru Walsinghamovi – šéfovi anglické špionáže.

Zprávu od Babingtona Gifford donesl Walsinghamovi. Ta však byla zašifrovaná pomocí nomenklátoru, který spiklenci vytvořili pro tento záměr ještě před Mariiným uvězněním. V tomto konkrétním nomenklátoru je 23 symbolů pro 23 písmen abecedy. Vynechána jsou písmena j, v a w. Dalších 35 symbolů vyjadřuje přesně stanovená slova a fráze, mimo jiné také určitý člen „the“, který je jinak velkou nápovědou pro zkušené luštitele. Také obsahuje čtyři nuly (tj. které nic neznamenají a jsou přidány pouze pro ztížení luštění šifrové ho textu) a speciální symbol, který znamenal, že následující znak je zdvojený. Šifrový text pak připomínal náhodné znaky vepsané těsně za sebou.

Pro vrchního představitele zemské špionáže to ovšem, jak lze očekávat, nebylo překážkou. Thomas Phelippes, jeho tajemník pro šifry, mu brzy předložil dešifrovaný text. Walsingham přesto vyčkával i přes vážnost situace. Usvědčit hrstku rebelů nebylo jeho hlavním cílem.

Marie v odpovědném dopisu s plány svého ochránce souhlasila, nevědomě tím proti sobě pomohla doplnit dostatek důkazů k jejímu odsouzení. Třešničkou na dortu Walsinghamova vítezství měla být jména všech spiklenců. Kryptoanalytik Phelippes, který byl i zdatným falzifikátorem, připsal do Mariina dopisu, ve kterém byla odpověď pro Babingtona text, ve kterém jej panovnice žádá o jména jejích podporovatelů. Když bez zaváhání uvedl seznam a popis daných pánů, vše se dalo do pohybu.

Spiklenci byli dopadeni, krutým způsobem ztrestáni a nakonec popraveni. Odsouzena k smrti byla nakonec po řádném soudním procesu i skotská královna. Soud ji seznal vinou z intrik a příprav, které měly za cíl zneškodnit její sokyni Alžbětu. *„V mém konci, je můj začátek.“* Tak zněla jedna z posledních slov před její proslavenou popravou. Příliš důvěrná konverzace mezi ní a rebelanty skutečně zapříčinila začátek jejího konce. Oba pisatelé příliš spoléhali na tajné kódování a šifrování v době, kdy frekvenční

analýza i kryptoanalýza obecně byly na vzestupu. Pokud by si dopisovali bez šifrování, dost možná by byli méně konkrétní a mnohem více diskrétní. Velmi pregnantně vyjádřil tuto skutečnost Simon Singh (2009): *„Šifra Marie Stuartovny jasně ukazuje, že špatné šifrování je horší než žádné.“*

4.3 Francouzská politika a šifry

Antoine Rossignol a jeho syn Binaventure patřili v sedmnáctém století k hlavním luštitelům francouzského dvora. Díky nim se začali o šifry zajímat i opravdu vlivní a význační lidé jako kardinál Richelieu, který sám je autorem jedné z nich – tzv. blokové transpozice. Král Ludvík XIV. však nebyl potěšen tím, že jeho ministr má po ruce lepšího šifrátora a luštitele, a tak ho převzal do svých služeb.

Rossignol byl mimo jiné tvůrcem tzv. Velké šifry, která byla po smrti Rossignolů dvě století považována za nerozluštitelnou. V roce 1890 objevil Victor Gendron - vojenský historik dopisy Ludvíka XIV. zašifrované právě touto šifrou. Po 3 letech usilovného snažení Étienna Bezeriese se podařilo systém prolomit. Díky tomu známe mimo jiné pravdu o muži se železnou maskou, jehož případ je popsán v jednom z dopisů. Řada odborníku se mylně domnívala, že se jednalo se o panovníkovo dvojče. Ve skutečnosti šlo o velitele Viviena de Bulonde, který ohrozil tažení francouzské armády do Itálie tím, že zbaběle uprchl z nechráněné pohraniční pevnosti Cuneo.

Ukažme si na příkladu, jak vypadá bloková transpozice, neboli Richelieova transpozice. Před šifrováním rozdělíme otevřený text na stejně dlouhé bloky (skupiny) písmen. Délka bloku je dána počtem písmen zvoleného hesla. Přeskupení písmen v každém bloku je také dáno heslem a je stejné jako přeskupení písmen hesla do pořadí podle abecedy. Pomocí hesla LUDVIK zašifrujeme zprávu: Zatkněte d’Artagnana a uvězněte ho v Bastile. Očíslujeme-li písmena hesla LUDVIK = 123456, pak seřazením písmen hesla podle abecedy dostaneme permutaci DIKLUV = 356124. Tuto permutaci následně použijeme pro šifrování:

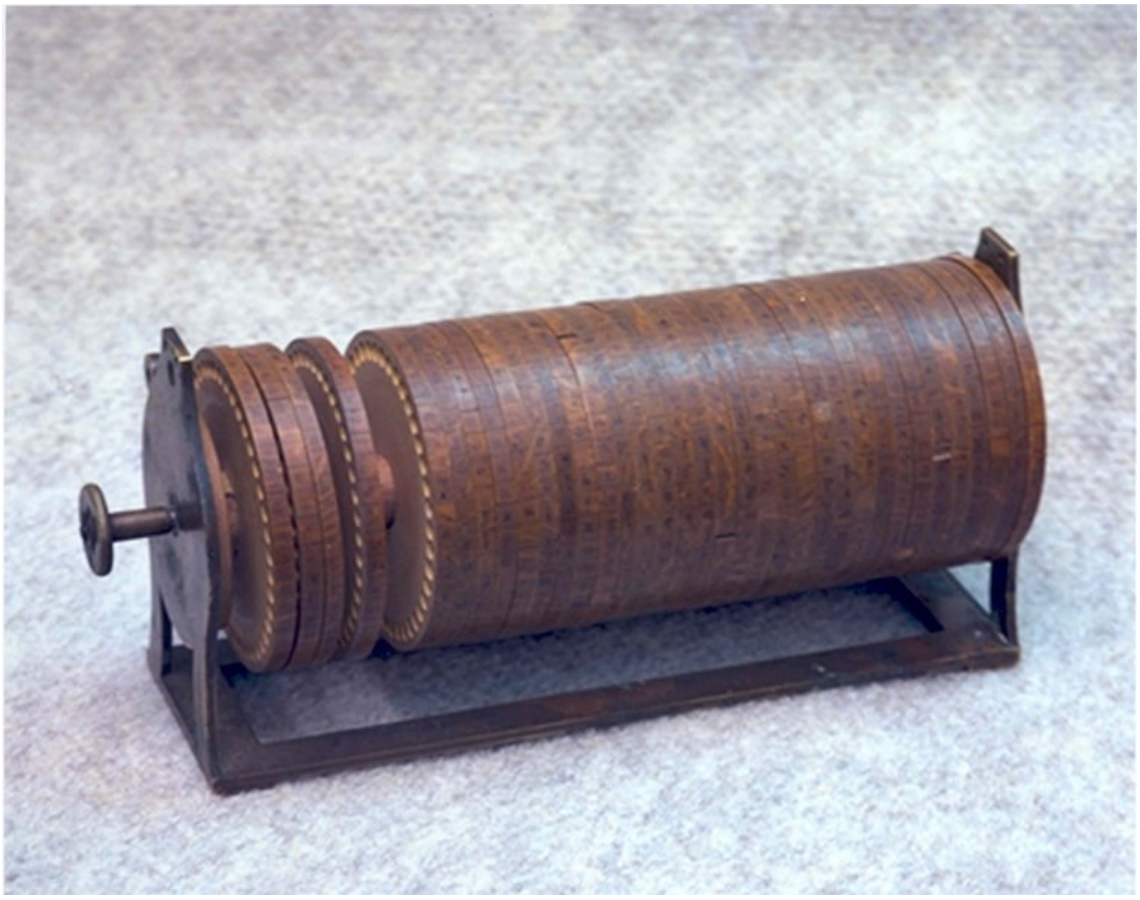
```
OT:   ZATKNE TEDART AGNANA AUVEZN ETEHOV BASTIL E
KLÍČ: 356124 356124 356124 356124 356124 356124
ŠT:   TNRZAK DRTTEA NNAAGA VZNAUE EOVETH SILBAT E
```

Celý text pak Richelieu přepsal jako dlouhý sled malých písmen bez mezer, aby nijak nenaznačil délku použitého hesla, tedy: *trnzakdrtteannaagavznaueeovethsilbate*.

4.4 Vynález prezidenta USA Thomase Jeffersona

Po kardinálu Richelieu byl dalším významným státníkem, který se zapsal do dějin tajné komunikace, třetí prezident USA a hlavní autor amerického prohlášení nezávislosti Thomas Jefferson. Spolu s Robertem Pattersonem z Pensylvánské univerzity sestrojili důmyslnou šifrovací pomůcku, nazývanou ***wheel cipher***. (Boone, 2005) Jedná se o soustavu 36 disků, na jejichž obvodu je vyryto 26 písmen anglické abecedy v náhodném pořadí, přičemž pořadí na každém z disku je jiné. Disky jsou očíslovány a mají uprostřed otvor, který umožňuje je navléknout na čep v různém pořadí. Toto pořadí disků vlastně představuje klíč (heslo) pro konkrétní použití této šifrovací pomůcky, tedy odesilatel a příjemce šifrové zprávy musí nejen mít k dispozici stejný systém disků, ale musí mít také dohodnuté klíče (pořadí kotoučů) a způsob jejich používání. Při vlastním šifrování sestaví šifrant z písmen na kotoučích úsek otevřeného textu a pak opíše jako šifrový text libovolný, náhodně zvolený řádek z obvodu válce. Postup opakuje tolikrát, na kolik úseků je třeba rozdělit celý text. Při dešifrování sestaví dešifrant z písmen na kotoučích příslušný úsek šifrového textu a pak pomalu otáčí celým válcem a hledá řádek, který dává smysluplný text. Je velmi nepravděpodobné, že by nahodile vznikl smysluplný text o délce 36 znaků ještě v nějakém jiném řádku, než v tom, který byl použit při šifrování.

Zajímavé je, že Jeffersonův vynález upadl v zapomnění, ačkoliv to byla na svou dobu velmi důmyslná pomůcka, ale ještě zajímavější je skutečnost, že s prakticky stejným vynálezem přišel zhruba o sto let později francouzský kryptolog Etienne Bazieres (ten, který prolomil velkou šifru Rossignolů).



Obr. 2 Jeffersonův disk – převzato z WikimediaCommons (public domain)

4.5 Luštění polyalfabetické substituce s periodickým heslem

Až do druhé poloviny 19. století, přesněji řečeno do roku 1963 byla Vigenèrova šifra nazývána ***le chifre indéchiffrable***, tedy nerozluštitelná šifra (používal se francouzský název, snad proto, že Blasie de Vigenère byl Francouz). V roce 1963 však vysloužilý důstojník pruské armády Friedrich Wilhelm Kasiski publikoval v knize *Die Geheimschriftenunddie Dechiffrirkunst* (Tajné šifry a uměni je dešifrovat) postup luštění polyalfabetické substituce s periodickým heslem, který je od té doby znám pod názvem ***Kasiského test***. Podle Simona Singha (2009) je pravděpodobné, že již v roce 1854 objevil stejný postup anglický matematik Charles Babbage, ale nepublikoval jej, nejspíš proto, že Anglie byla v té době ve válečném stavu s Ruskem. Angličané, kteří vstoupili do krymské války, se nechtěli připravit o výhodu luštit ruské šifry, které Rusové považovali za nerozluštitelné.

Princip luštění spočívá v následující myšlence. V každém jazyce jsou nejen typické frekvence písmen, ale také frekvence bigramů. ***Bigram*** je dvojice po sobě jdoucích písmen. Občas se stane, že bigram připadne na stejnou dvojici písmen periodického hesla. Díky takové šťastné náhodě, která nastane tím pravděpodobněji, čím je určitý bigram v daném jazyce častější, heslo kratší a otevřený text delší, se dva stejné bigramy v otevřeném textu zašifrují do dvou shodných bigramů v šifrovém textu. Kasiského test spočívá v hledání dvojic shodných bigramů v šifrovém textu, určení vzdálenosti mezi členy dvojice a nakonec v hledání společného dělitele těchto vzdáleností. Společný dělitel bude odpovídat délce použitého hesla.

Když známe délku hesla, můžeme písmena šifrového textu rozpočítat do skupin připadajících na stejné písmeno hesla a na tyto skupiny pak použít frekvenční analýzu. Frekvenční analýzu lze navíc zjednodušit, jestliže víme, že jednotlivým písmenům hesla odpovídají pouze různé posuny abecedy – různé řádky tabulky ***tabula recta***.

Postup publikovaný ve druhé polovině 19. století (existují dohady, zda nebyl už dříve znám některým luštitelům, kteří ho pečlivě utajili), rázem změnil názor na Vigenèrovu šifru. Z nerozluštitelné šifry se stala šifra poměrně snadno luštitelná. To přimělo kryptology k přemýšlení o konstrukci nových šifrových systémů. Uvedeme si ještě několik komplikovanějších substitučních šifer. Postupy jejich luštění jsou složitější, než frekvenční analýza a Kasiského test. Proto už budu dále uvádět pouze postup šifrování a dešifrování, nikoliv princip luštění.

4.6 Šifra Playfair

Šifru Playfair navrhl v roce 1854 všestranný anglický vědec Charles Wheatstone. Jméno ale dostala po jeho příteli, nadšeném propagátorovi šifry, skotském baronovi a poslanci britského parlamentu Lyonu Playfairovi. K šifrování se používá čtvercová tabulka 5 x 5 polí, do které vyplníme nejprve písmen podle zvoleného hesla a pak doplníme zbylými písmeny abecedy. Mezinárodní abeceda má 26 písmen, ale my máme k dispozici jenom 25 polí. Proto musíme jedno písmeno vynechat, nebo do jedno z políček zapsat dvě písmena. Angličané nejčastěji spojí písmena I a J do jednoho políčka, my můžeme úplně vynechat písmeno Q, které se v českém textu téměř nevyskytuje (a pokud by se přece jen vyskytlo, nahradíme ho dvojicí písmen KV). Pokud zvolíme heslo Hradec Králové, bude výsledná tabulka vypadat takto:

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

Do prvních pěti polích doplníme H, R, A, D a E. Na druhém řádku pokračujeme C a K, písmena R a A už znova nepíšeme, protože už v tabulce jsou, pokračujeme L, O a V, písmeno E znovu nepíšeme. Pomocí hesla jsme zaplnili horní dva řádky, zatímco zbylá písmena vyplní zbývající tři řádky. Písmeno Q vynecháme.

Šifrování neprobíhá po jednotlivých písmenech, ale po bigramech. Šifra Playfair je tedy ***bigramová substituce***. Před vlastním šifrováním tedy rozdělíme text do dvojic, a pokud by někde náhodou vznikla dvojice dvou stejných písmen, vložíme do otevřeného textu navíc písmeno vzácné v českém textu (např. X, nebo W). Podobně doplníme písmeno na konec textu, pokud by poslední písmeno otevřeného textu bylo liché.

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

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

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

Máme-li připravené bigramy i tabulku, můžeme začít šifrovat. Při šifrování mohou nastat tři různé situace. Obě písmena bigramumohou být ve stejném řádku, ve stejném sloupci, nebo je každé z nich v jiném řádku i jiném sloupci. Podle toho, který z případů nastane, volíme konkrétní pravidlo:

1) Pokud leží obě písmena ve stejném řádku, je každé písmeno bigramu nahrazeno písmenem ležícím v tabulce vpravo od něj. Poslední písmeno v řádku se nahradí prvním písmenem téhož řádku.
2) Pokud leží obě písmena ve stejném sloupci, je každé písmeno bigramu nahrazeno písmenem pod ním. Je-li písmeno v posledním řádku je nahrazeno prvním písmenem téhož sloupce.
3) Pokud je každé z písmen v jiném řádku a sloupci, je každé písmeno bigramu nahrazeno písmenem nacházejícím se v průsečíku jeho vlastního řádku a sloupce obsahujícího druhé písmeno bigramu.

Dešifrování probíhá samozřejmě také po bigramech, pouze v prvním pravidle nahradíme slovo „vpravo“ slovem „vlevo“, slovo „první“ slovem „poslední“ a naopak.

Podobně se změní druhé pravidlo, zatímco třetí pravidlo zůstane zcela beze změn. Postup šifrování opět ukážu na příkladu. Zašifruji zprávu: Šifru Playfair používala britská armáda.

SI FR UP LA YF AI RP OU ZI VA LA BR IT SK AX AR MA DA
YS NK XM GL WI DG AN CY YJ LE GL FH JS NO LA DA PH ED

Jednotlivá písmena se šifrují různě podle toho, v jakém bigramu se vyskytnou. Vidíme, že např. písmeno A se v naší zprávě nahradilo postupně písmeny L, D, E, L, L, D, D, písmeno R písmeny K, A, H a A atd.

4.7 Šifra BIFID

Šifru BIFID publikoval Félix Marie Delastelle roku1895 v časopise *Revue du Génie civil*. Tento Francouz nebyl voják, diplomat, politik ani matematik či lingvista, pracoval jako účetní skladů v námořním přístavu, kryptologie byla jeho celoživotní zálibou. Šifra BIFID nešifruje po dvojicích jako šifra Playfair, ale zpravidla po pěticích znaků. Je to také první šifra, kde nešifrujeme přímo z otevřeného textu do šifrového textu, ale musíme použít také ***mezitext***. V tomto případě je mezitext dokonce dvouřádkový, zato si vystačí jen s pěti znaky – číslicemi od 1 do 5. Jako šifrovací tabulka slouží podobný čverec 5 x 5 políček jako u šifry Playfair, ale s tím rozdílem, že jej doplníme záhlaví, v němž očíslujeme řádky a sloupce. Zvolíme-li heslo KRYPTOLOGIE, bude čtverec vypadat takto:

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

Před šifrováním text rozdělíme do pětimístných skupin a šifrování provádíme postupně po těchto pěticích písmen. Pod každé písmeno pětice zapíšeme do prvního řádku číslo toho řádku, v němž najdeme písmeno v šifrovacím čtverci, a do druhého řádku číslo sloupce. Z tohoto dvouřádkového mezitextu pak získáme šifrový text tak, že bereme první a druhou číslici v horním řádku, pak třetí a čtvrtou číslici v horním řádku, potom poslední číslici v horním řádku a první číslici v dolním řádku, následuje druhá a třetí

číslice v dolním řádku a nakonec čtvrtá a pátá číslice v dolním řádku. V každé z těchto dvojic znamená první číslice číslo řádku v šifrovacím čtverci a druhá číslo sloupce. Nakonec tedy získáme pětici písmen, která tvoří příslušnou část šifrového textu. Pokud na konci textu vyjde kratší skupina než pětimístná, tak zde celý postup zkrátíme. Ukážu postup opět na příkladu. S použitím výše zobrazeného čtverce zašifruji citát: Moudrost je dcerou zkušenosti. Leonardo da Vinci.

```
MOUDR  OSTJE  DCERO  UZKUS  ENOST  ILEON  ARDOD  AVINC  I
42531241423321 2  55154  24241  22224  31323  35243  2
311421552543521   15115  54155  42514  12414  12443  4
JWYKJ IPOZE COIFO ZTHUT IITHZ LLNEP ABAIP FIAIM I
```

Při dešifrování pochopitelně vytváříme mezitext po řádcích a do otevřeného textu pak převádíme dvojice číslic stojících pod sebou v horním a dolním řádku mezitextu.

4.8 Šifra Fractionated Morse

Také šifra, kterou uvádím jako poslední, pracuje s mezitextem, kterým je v tomto případě otevřený text přepsaný pomocí Morseovy abecedy. Mezitext se potom rozdělí do skupin po třech znacích (abeceda se pro tyto účely skládá z teček, čárek a lomítek) a každá trojice se nahradí jedním písmenem abecedy. Bohužel se mi nepodařilo zjistit, kdo a kdy tento systém vymyslel, ale domnívám se, že je buď stejně starý, nebo novější než šifra BIFID. K této domněnce mě vede odhad, že systém vznikl až s rozvojem radiotelegrafie, kterou nezávisle na sobě vynalezli Rus Alexandr Štěpanovič Popov a Ital GuglielmoMarconi v roce 1895.

Mezitext zapisuje jednotlivá písmena pomocí teček a čárek, lomítko se uvede úplně na začátku zprávy a potom za každým písmenem, na konci slova jsou vždy dvě lomítka. Mimo to doplníme lomítka na konec zprávy tak, aby celkový počet znaků mezitextu byl dělitelný třemi. Z mezitextu vytvoříme šifrový text pomocí následující tabulky, kterou opět vytváříme na základě hesla. Protože tabulka má 27 pozic, využijeme celou abecedu a navíc jako 27. znak přidáme znaménko +. Zvolíme-li heslo MARCONI, bude tabulka vypadat následovně:

...	..-	../	.-.	.--	.-/	./.	./-	.//
M	A	R	C	O	N	I	B	D
-..	-.-	-./	--.	---	--/	-/.	-/-	-//
E	F	G	H	J	K	L	P	Q

/..	/.-	/./	/-.	/--	/-/	//.	//-	///
S	T	U	V	W	X	Y	Z	+

Protože písmena Morseovy abecedy se skládají z různého počtu teček a čárek, vytváří se šifrový text nepravidelně a počet písmen šifrového textu je vždy větší než počet písmen odpovídajícího otevřeného textu. Pro radiotelegrafistu, který dobře zná Morseův kód je šifrování poměrně snadné a výsledný šifrový text je přitom obtížné luštit.

Dešifrování se provádí tím způsobem, že ze šifrového textu získáme mezitext pomocí výše uvedené tabulky. Tento mezitext už je běžný zápis otevřeného textu v Morseově kódu, který převedeme do běžného zápisu pomocí písmen mezinárodní abecedy.

4.9 USA jde do války

Zimmermanův telegram. Příčina, kvůli níž USA v roce 1917 vstoupila do světové války. Německý ministr Arthur Zimmerman vyslal zašifrovaný telegram mexické vládě, v němž vyzývá Mexiko k válce proti USA. (Vondruška, 2006) Britové, naneštěstí pro Němce, telegram včas zachytili, rozluštili a předali Američanům. Tehdejší americký prezident Woodrow Wilson neotálel a svolal Kongres, jenž schválil vstup USA do války proti rozpínajícímu se Německu. Jak už víme, tato událost změnila poměr vojsk válčících stran. I během války obě strany bez ohledu na porážky či vítězství vyvíjejí další a dokonalejší šifrové systémy.

4.10 První počítačová šifra a zrození kvantové kryptografie

Po druhé světové válce přichází doba, kdy přebírají pomyslný štafetový kolík počítačové šifrové systémy. Některé z prvních elektronických počítačů byly určeny právě k luštění šifer. Michal Musílek (2011) k odlišnosti mezi klasickými ručními šiframi a jejich moderními nástupci uvádí: *„Rozdíl oproti ručním šifrám spočívá především v tom, že se zde nepracuje s jednotlivými znaky (písmeny), ale s jednotlivými bity jejich kódové reprezentace (ve smyslu kódů typu ASCII, ISO 8859-2, UNICODE), nebo bloky bitů určité délky.“* Jinak ovšem tyto systémy pracují na původních principech substituce, transpozice i připočtení hesla.

První z nich vytvořil Horst Feistel, vedoucí výzkumného projektu v IBM Watson Research Lab, který během šedesátých let dvacátého století vyvinul šifru Lucifer. Tato šifra se později stala základem amerického standardu DES a inspirovala i další blokové šifry.

Postupem času se stávaly počítačové šifrové systémy neodmyslitelným standardem nejrůznějších subjektů – bank a jejich klientů, obchodních firem apod. S tím se pochopitelně zvedala i poptávka po co nejbezpečnějším systému. Málokdo si zřejmě dokázal vůbec představit, že by existoval ideálně bezpečný šifrový systém. Přesto se to podařilo. Američan Gilbert S. Vernam již v roce 1917 přišel s šifrovacím systémem založeným na použití náhodně generovaného hesla, jednorázově užitého, jenž má stejnou délku jako samotný text. To, že tento systém je absolutně nerozluštitelný, dokázal matematickým metodami jeden ze zakladatelů teoretické informatiky Claude Elwood Shannon až v roce 1949. Dodržení podmínek takového systému je však velmi náročné, a právě generování a distribuce dokonale náhodných klíčů požadované délky se zdálo být velmi obtížné až nemožné. To změnil objev kvantové kryptografie.

Za prvním protokolem kvantové kryptografie nazvaným BB84 stojí dva informatici – Charles Bennett a Gilles Brassard. Tento protokol je založen na vysílání fotonů s různou polarizací, což umožňuje výměnu klíče. Síla tohoto protokolu spočívá v jednom z principů kvantové fyziky – každé měření v mikrosvětě ovlivní daný měřený objekt a díky tomu je možné odhalit každý pokus o odposlech. Pokud nedošlo k odposlechu, použije se část sekvence k přenosu klíče pro Vernamovu šifru. Také pro tvorbu klíče jsou využívány různé fyzikální jevy, které jsou dokonale náhodné. Absolutně bezpečný šifrový systém v kombinaci s kvantovým přenosem šifrovacího klíče je vrcholem moderní kryptografie. Pro běžné úrovně utajení a ochrany dat se i ve světě počítačů a počítačových sítí používají šifrové systémy, které jsou sice teoreticky luštitelné, ale při současném stavu techniky by průměrná doba luštění představovala roky, či desítky let a vyžadovala by velký výpočetní výkon. (Musílek, 2011)

5 Shrnutí vývoje substitučních šifer

Různé substituční šifry se používaly již ve starověku. V principu šlo vždy o nějakou podobu jednoduché záměny neboli monoalfabetické substituce. Že jednoduchou substituci lze také poměrně jednoduše luštit ukázali jako první Arabové, a to v 9. století našeho letopočtu. Ve středověku pak začínají pokusy o vytvoření složitějších šifrových systémů.

Jednou z cest je použití homofonů (více znaků šifrové abecedy pro často se vyskytující písmena, zejména samohlásky), klamačů (znaků, které nenesou žádnou informaci, mají jen zmást luštitele) a symbolů pro celá, často se opakující slova, či dokonce krátké věty. Tak vznikly nejprve nomenklátory a později rozsáhlé kódové knihy. Druhou cestou je vymýšlení důmyslných šifrovacích systémů, které vytváří šifrový text složitějším způsobem než jednoduchá záměna. Slavná Vigenèrova šifra, kterou publikoval v knize *Traicté des chiffres* (Pojednání o šifrách) v roce 1586, byla až do roku 1863 považována za nerozluštitelnou. Poté co vešel ve známost Kasiského test, vymýšleli kryptologové šifry, v nichž se nešifruje po jednotlivých písmenech, ale buď po dvojicích písmen (bigramech), nebo skupinách více písmen, případně se vytvořený mezitext „rozláme“ na malé úseky vůbec neodpovídající písmenům. Typické představitele tohoto vývoje jsme si uvedli v přechozích podkapitolách. Shrnu je pomocí tabulky:

Název šifry	***Šifrovací tabulka***	***Publikována***	***Mezitext***	***Heslo***	***Šifruje se po***
Atbaš (jednoduchá záměna)	převodová tabulka	okolo roku 500 př. n. l.	Ne	Ne	1
Vigenèrova šifra	tabula recta	1586	Ne	Ano	1
Playfair	čtverec 5 x 5 polí	1854	Ne	Ano	2
BIFID	čtverec 5 x 5 polí s čísly řádků a sloupců	1895	Ano	Ano	5
Fractionated Morse	Morseův kód, tabulka pro převod mezitextu na šifru	začátkem 20. století	Ano	Ano	nelze předem říct

6 Úvod k praktické části práce

V rámci praktické části práce jsem si stanovil dva následující cíle. Pokusit se dát podnět k zařazení nauky o kryptografii do výuky informatiky na středních školách a pomoct prohloubit mezioborové vztahy mezi informatikou a dějepisem. První cíl z toho důvodu, že historii šifrování považuji za zajímavou a velmi zásadní kapitolu informatiky, jakožto oboru o informacích. Jistě je třeba přihlédnout k tomu, že ony šifry, které popisuji v teoretické části práce, jsou opravdu vzdálené dnešním velmi sofistikovaným šifrovacím systémům, založeným na ohromujícím výpočetním výkonu soudobých informačních technologií, a proto by jistě nebylo vhodné se jim ve výuce věnovat více než záležitostem jistého aktuálního trendu, jako např. grafice, webovým technologiím či zejména algoritmizaci. Přesto se domnívám, že by se s nimi žák měl v hodinách informačních technologií přinejmenším seznámit. Zároveň jsem přesvědčen, že tímto exkurzem budou akcentovány mezipředmětové vztahy mezi informatikou a dějepisem. To může dle mého názoru velmi pozitivně ovlivnit vztah žáka k dosud méně preferovanému předmětu, bez ohledu na to, zdali je spíše přírodovědného či společenskovědního zaměření a dát mu zajímavý příklad provázanosti jednotlivých oborů lidské činnosti. K řešení stanovených cílů bylo pro mě relevantní ujasnit si pomocí odborné literatury přidružené pedagogické pojmy. Za klíčové považuji metody a formy výuky.

„Metoda jako cesta k cíli je rozhodujícím prostředkem k dosahování cílů v každé uvědomělé činnosti; proto záleží na výběru vhodných metod a na jejich dokonalém ovládání. Nové vědecké poznatky jsou téměř vždy vázány na nové metody bádání, zkoumání a také vynikající výsledky praxe jsou vždy spojeny s aplikací vhodných metod.“ uvádí Josef Maňák (2003).

Inspirací při výběru efektivní metody se mi stalo dělení výukových metod podle Průchy (2009). Ten dělí metody na klasické, mezi něž řadí metody slovní, názorně demonstrační a dovednostně-praktické, samostatně vyčleňuje metody aktivizující a komplexní. Nejinak tomu bylo i při výběru forem výuky. Průcha je v základu dělí na organizační formy výuky podle vztahu k osobnosti žáka, organizační formy výuky podle charakteru výukového prostředí a organizační formy výuky podle délky trvání.

Na základě mých subjektivních dosavadních zkušeností z praxe jsem vybíral mezi jednotlivými metodami ty, které se mi zdály pro danou oblast vhodné. Hned v úvodu bych ovšem rád ozřejmil, že se nedomnívám, že existuje jedna nebo více ideálních metod a že je v pedagogické praxi velmi potřebné metody kombinovat a zkoušet nové a nové. Při výuce dějepisu se mi vždy osvědčila převážně frontální, hromadná výuka, při uplatnění slovní metody (vyprávění, práce s textem). Vhodná se mi taky zdá aktivizující metoda v podobě diskuse či inscenace. Žáci tak jen pasivně nepřijímají encyklopedické znalosti, ale mají prostor se k problémům vyjádřit a některé významné dějinné události si zinscenovat. Tak lépe zafixují získané vědomosti.

Výuka informatiky je téměř vždy podporována počítačem, jako nástrojem k názorně-demonstračním metodám (předvádění a pozorování, instruktáž) a metodám dovednostně-praktickým (napodobování, nácvik dovedností). Vůbec pro výuku tohoto předmětu je velmi zásadní názornost. Pochopitelně nesmí chybět ani slovní metody.

Z výše uvedeného je patrné, že běžná výuka humanitního předmětu, jako je dějepis, a přírodovědného, jakým je informatika, se do jisté míry liší. Na základě tohoto uvědomění jsem se rozhodl vytvořit pracovní listy určené žákům, jež umožňují práci s textem, která je společná výuce obou předmětů. Pracovní listy podporují také individuální práci žáků a tím posilují obecné kompetence k učení. Pracovní listy jsem zaměřil na tři historická období: starověk, středověk a raný novověk a přelom 19. a 20. století. Jedná se celkem o 8 pracovních listů, které mají následující strukturu: úvod, obecný princip a konkrétní příklad. Žák se vždy v úvodu seznámí s historickými událostmi, které souvisí s danou šifrou, jejím původem a uplatněním. Obecný princip použití šifry je vysvětlován co nejjednodušším způsobem. Poslední část každého pracovního listu tvoří jeden nebo více příkladů, na kterých žák může procvičit aplikaci nabitých poznatků. Příklady jsou buď jednoduché, nebo strukturované úlohy s, nebo bez historického kontextu. Např. u Caesarovy šifry jsem jako modelový příklad uvedl bitvu u Alessie. Žák má možnost se na krátký okamžik přenést do dávno minulé doby, vžít se do role vojevůdce a kryptografa, který rozhoduje o výsledku bitvy, čímž jej podněcuji k vyššímu úsilí o zdolání problému.

V samotných pracovních listech již pro přehlednost necituji, z kterých děl bylo čerpáno, protože tato informace je pro žáky nadbytečná a mohla by rozptylovat jejich pozornost. Mohu zde souhrnně uvést, že jsem čerpal zejména, podobně jako v teoretické části

práce, z knih *Skryté kódy a velkolepé projekty* Pierra Berloquina (2011), *Kniha kódů a šifer* Simona Singha (2009) a *Kryptologie, šifrování a tajná písma* Pavla Vondrušky (2006). Velikou oporou se mi staly také stránky *www.musilek.eu* jejichž autorem je Michal Musílek (2010). Jejich součástí jsou velmi kvalitně zpracované programy určené k šifrování či dešifrování řady historických šifer.

CAESAROVA ŠIFRA

Úvod a princip

Julius Caesar. Jedno z nejproslulejších jmen starověké historie. Jméno, se kterým jste se jistě již setkali a pokud ne, tak zcela určitě ještě setkáte při hodinách dějepisu. Dozvíte se, že šlo o vynikajícího politika a vojevůdce starověkého Říma. Muže, který sehrál klíčovou roli v přeměně římské republiky v monarchii.

Pravděpodobně se ale nedozvíte, že využíval substituční šifru, dnes známou jako Caesarova. Tu popisuje ve svém slavném díle *Zápisky o válce Galské*. Není tedy divu, že ji využíval právě pro vojenskou komunikaci. V historii kryptografie se jedná o běžnou praxi. Nepřítel sice dokázal silou získat odeslanou zprávu, ale nebyl schopen ji rozluštit.

Princip této šifry je přitom z dnešního pohledu triviální. Odborně hovoříme o jednoduché záměně neboli monoalfabetické substituci. Spočívá v nahrazení každého písmene písmenem, které stojí v abecedě o tři pozice dále. Tedy písmeno A z otevřeného textu je v šifrovém textu nahrazeno písmenem D. Nejlépe to demonstruje převodová tabulka:

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

PŘÍKLAD

Přenesme se nyní v čase do roku 52. př. n. l. Je to již pět let, co vyrazil Gaius Julius Caesar na jedno z nejslavnějších tažení jeho vojenské kariéry. Podmanil si bezpočet barbarských kmenů, pokusil se dokonce dobýt Germánii a Británii, ale to mu v té době ještě nebylo souzeno. Jeho zrak se však začal upínat k jinému místu, k zemi zvané Gálie. Zde zpočátku úspěšně slavil jeden triumf za druhým, tedy do doby, kdy se na scéně objevil náčelník Arvernů, obávaný Vercingetorix. Ten sjednotil tamní kmeny v boji proti římskému uchvatiteli a Caesar byl nucen čelit největšímu galskému povstání.

Rozhodující střetnutí jej čekalo u galské pevnosti Allessie, kam se rozhodl Vercingetorix společně se svými spolubojovníky stáhnout. Ta byla na perfektní strategické pozici. Co však obráncům sházelo, byly potraviny, zásobování bylo vzhledem k obležení římskými legiemi prakticky nemožné. Proto, byli z pevnosti vysláni jezdci, jejichž úkolem bylo přivést pomoc. A tak se i stalo. Galové vytvořili armádu čítající přes 250 000 bojovníků.

Caesar byl tedy nucen čelit galskému vzdoru ze dvou stran, a proto zahájil výstavbu dvojitého opevnění kolem Allessie. Pokuste se nyní dešifrovat na základě nabitých vědomostí, jaké nástrahy tvořily vnější část opevnění: (*pozn.: písmeno CH se v dané šifrové abecedě nenachází, CH tedy bude kombinací písmen C a H; dešifrování vám usnadní převodová tabulka)*

UDGB RVHNDQBFK YHWYL VWURPX, MDPB CDNRQFHQH VSLFDWBPB NXOB, CHOHCQH KDNB, WUL SULNRSB, REUDQQH YDOB, REUDQQH YHCH, OHJLRQDUVNH WDERUB

Galové na sebe nenechali dlouho čekat. Byli však zaskočeni dokonalým obranným systémem římských jednotek a došlo na jejich straně k nemalým ztrátám. Po dni odpočinku a vyčkávání na vhodný okamžik opět vyrazili do útoku. Tentokrát ovšem připraveni. Vžijte se nyní do role velitele předsunutých jednotek. Je teď na Vás, abyste splnili Caesarovy rozkazy a útok barbarů odrazili.: (*pozn.: Vzhledem k důležitosti zprávy se Caesar rozhodl text rozdělit do skupin po pěti znacích, aby zpráva byla náročnější na luštění.)*

PHMWH VHQDS RCRUX SLGOH QDVLF KCYHG XQHSU LWHOS ULFKB VWDOR WHSBD EBMLP LYBVW ODOSU LNRSB DGRVW DOVHW DNQDV LPSRC LFLPQ HQHFK URMLW GDOSD OWHGR QLFKS UDNBD VDPRV WULOB DEXGH OLWUH EDYBV OHWHO HJLHD VPHWW HMHMH GQRXS URYCG BCSRY UFKXC HPH

Výborně! Galy se Vám podařilo zahnat. Ale ne na dlouho. Barbaři později zaútočili na více míst současně a tentokráte vyrazil do boje i Vercingerix, takže Římané byli nuceni čelit nepřátelům z obou stran. Nejkritičtějším místem byl tábor ležící na severu pod pahorkem. Caesar tam postupem času soustřeďoval více a více jednotek. Zde provedl rozhodující úder a plně zde zúročil svého strategického génia. Vydejte, jako slavný vojevůdce, rozkazy, které mají přinést vítězství. Pošlete veliteli jízdy zašifrovaný vzkaz následujícího znění. Pro opatrnost rozčleňte text do skupin o pěti znacích:

JÍZDU ROZDĚLTE NA DVĚ POLOVINY. PRVNÍ POLOVINA JÍZDY NECHŤ ZÚSTANE A BOJUJE. DRUHÁ AŤ PAK OBJEDE PAHOREK A VPADNE SPOLU SE MNOU A KOHORTAMI DO TÝLA NAPŘÍTELE.

Boj mezi legionáři a galskými válečníky byl urputný. Juliova taktika se však vyplatila. Obklíčení Galové se dali na útěk a obránci se k dalšímu útoku sami již neodvážili. Naděje na jejich záchranu se rozpadly.

Následujícího dne Vercingetorix přiznal bezpodmínečnou kapitulaci a římskému vojevůdci se vzdal. Přesto, že boje v Galii ještě nějaký čas pokračovaly, Caesar ji de facto ovládl celou. Nedlouho poté v roce 49. př. n. l. ho čeká rozhodnutí, zda překročit či nepřekročit řeku Rubikon, aby táhl na Řím jako dobyvatel proti jeho soku Pompeiovi a stal se diktátorem. Z tohoto významného mezníku historie pochází onen slavný výrok: „Alea acta est“ neboli „Kostky jsou vrženy“. Nebo snad „Nrvwnb mvrx yuchqb“? Ale k tomu více v hodinách dějepisu.

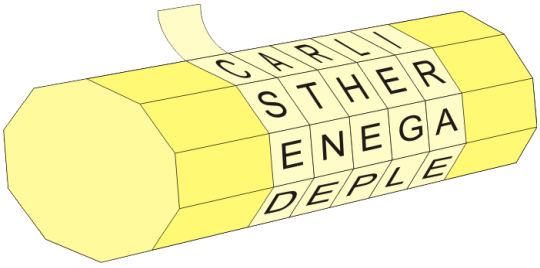
SKYTALÉ

Úvod a princip

V Řecku byla nejčastěji uplatňovaným postupem pro utajení zprávy steganografie. Tímto termínem se myslí utajení existence zprávy jako takové. Konkrétní příklad popsal Herodotos, významný antický historik, ve svých Dějinách. Uvádí zde, že tyran Histiaeus, který se odmítal podvolit vládě Dareia I., perského vládce, se odhodlal poslat zprávu svému příbuznému, tyranu Aristagorovi do Milétu, aby tak pomohl koordinaci povstání proti Peršanům. Aby zpráva dorazila v pořádku nedotčena, nechal svému nejvěrnějšímu otrokovi oholit hlavu, poté na jeho lebku napsal vzkaz, a když mu vlasy opět narostly, mohl jej vyslat na cestu. Díky Histieusovi a jeho originálnímu nápadu můžeme hovořit o počátcích steganografie již ve starověku.

Nás však bude nyní zajímat jiný způsob šifrování. Přesto zůstaneme v Řecku, a to konkrétně v jistém městském státě. I dnes, téměř tři tisíce let od počátku jeho existence, jsou nám známa slavná vítezství i hrdinné prohry z bitev u Thermopyl, Salamíny či Marathónu, kde bojovali jeho obávaní válečníci, stejně tak jako tvrdý přístup k dospívajícím chlapcům, který se stal pojmem.

Ano, byli to právě Sparťané, kdo plně využíval první technické zařízení na utajení tajných zpráv. Tzv. skytalé umožňuje provádět transpozici. Principem transpoziční šifry je změna pořadí písmen ve zprávě. Odesílatel i příjemce museli být vybaveni holemi stejného tvaru a velikosti. Před psaním zprávy se na hůl navinul šroubovitě proužek papyru. (viz obrázek) Zpráva se pak psala napříč závity papyru, takže po odvinutí byla na proužku nesrozumitelná řada písmen. Příjemce potom proužek opět navinul, tentokrát na svou skytalé, a pohodlně přečetl.



Skytalé – převzato z WikimediaCommons

PŘÍKLAD 1

Sparťané byli především válečníci a skytalé plně využívali při vojenských operacích. My se již nebudeme zabývat konkrétními historickými událostmi, pouze zkusíme aplikovat onen princip a dešifrovat následující text, napsaný na kousku papíru. Vytvořte k tomuto účelu svou vlastní skytalé, nebo použijte z vašeho pohledu již existující. Fantazii se meze nekladou!

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

PŘÍKLAD 2

Na pruh papíru, látky, kůže, či jiného materiálu, navinutého na skytalé napište vlastní zprávu. Po rozvinutí vypište do následující tabulky jak otevřenou, tak zašifrovanou podobu textu.

PŘÍKLAD 3

Zkuste se zamyslet nad tím, jak dešifrovat následující text bez pomocí skytalé. Své tvrzení zdůvodněte.

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

POLYBIŮV ČTVEREC

Úvod a princip

Před námi je poslední příklad starověké šifry. Zůstaneme i nadále v Řecku, ovšem v době pozdější, a to zhruba ve druhém století př. n. l. Šifra, o které budeme hovořit, nese název podle jména jejího autora. Nebyl jím nikdo jiný než slavný řecký historik Polybios. Ten se proslavil zejména svým dílem *Historiai* (Dějiny). Jeho práce je dodnes považována za jednu z nejvýznamnějších v oboru kritiky a studia historických pramenů.

Polybius byl ovšem také politikem a politická zkušenost jej nepochybně přivedla k šifrování, jako nástroji, který utají a předá důležité informace pouze do povolaných rukou. Ve svém, již výše zmíněném, díle popisuje šifrovací systém. Jedná se o čtverec, jehož obsahem je pět a dvacet znaků abecedy. Do řádků postupně vypisujeme vždy pětici znaků. V případě české abecedy, vynecháme jeden z nich, obvykle tak činíme s písmenem, které se v ní vyskytuje nejméně často, tedy písmenem Q či W. Vznikne nám tak tabulka 5 x 5 znaků, viz:

	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**	**R**	**S**	**T**	**U**
5	**V**	**W**	**X**	**Y**	**Z**

Každému znaku přiřadíme dvojici čísel, přičemž dodržíme pravidlo: první je číslo řádku a druhé sloupce. Tedy např. písmeno U bude mít souřadnici: 45.

PŘÍKLAD 1

Pokuste se pomocí Polybiova čtverce zašifrovat následující zprávu:

„Polybiovu šifru dnes nazýváme Polybiův čtverec.“

PŘÍKLAD 2

Pokuste se dešifrovat pomocí Polybiova čtverce následující zprávu:

4135325412244543 552432 51 351214351224
2315321534244333345

PŘEDMLUVA K PŘÍKLADU 3

Modernější šifry často pracují s tzv. klíčem, díky kterému se luštění stává obtížnějším. Klíčem obvykle může být kterékoliv slovo. V případě Polybiova čtverce je dané slovo (klíč), vepisováno postupně do řádků s tím, že žádné písmeno slova se neopakuje. Jako příklad si uvedeme Polybiův čtverec pracující s klíčem – ČTVEREC.

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

PŘÍKLAD 3

Pokuste se dešifrovat následující text pomocí Polybiova čtverce. Tento je ovšem vybaven klíčem. Indicie k odhalení klíče zní: **Dějiny**. Pokuste se odhalit klíč a úspěšně

dešifrovat následující zprávu. K postupu využijte vpisování do prázdného čtverce: *(Pozn.: Vzpomínáte na Caesarovu šifru? Pro obtížnější luštění byl text nějakým způsobem dělen. K správnému dešifrování využijte všechny své dosavadní zkušenosti.)*

35411 22435 14311 41513 12322 13155 43121 11213 14152 11222 12

	1	2	3	4	5
1					
2					
3					
4					
5					

STŘEDOVĚKÉ ŠIFROVÁNÍ

Úvod a princip

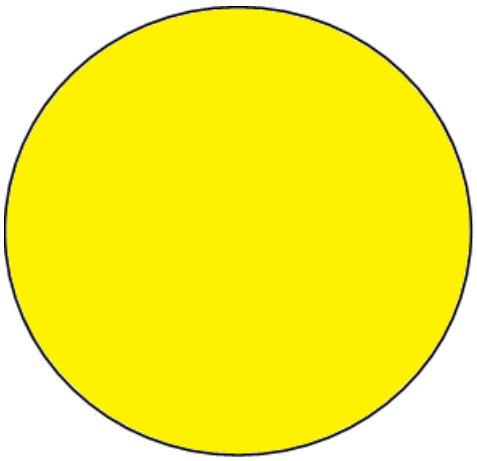
Po éře starověkých šifer se v době středověku rozvíjí kryptografie zejména ve východních oblastech. Arabští učenci přicházeli s novými a novými šifrovacími systémy, s významným počinem v historii šifrování – frekvenční analýzou a mnohým dalším. Neznamená to však, že by se v Evropě i nadále nešifrovalo. Jako příklad si lze uvést šifru mistra Jana Husa. Jeho zašifrované dopisy z Kostnice jsou však ukázkou pro tu dobu již zastaralé a snadno prolomitelné jednoduché substituce.

Evropa začala dohánět své orientální sousedy teprve v druhé polovině patnáctého století. Dalo by se říci, že čekání se vyplatilo. V této době se totiž o šifry začal zajímat muž, který je dodnes právem zván otcem západní kryptografie. Leon Battista Alberti – italský filozof, básník, stavitel a kryptograf. Jeho dílo obsahovalo tří zásadní počiny v historii posledního uvedeného oboru. Jako první Evropan představil ucelený výklad dešifrování na základě frekvenční analýzy (s tímto principem již dříve operovali arabští učenci) dále užití zašifrovaných kódů a v neposlední řadě nový šifrovací systém.

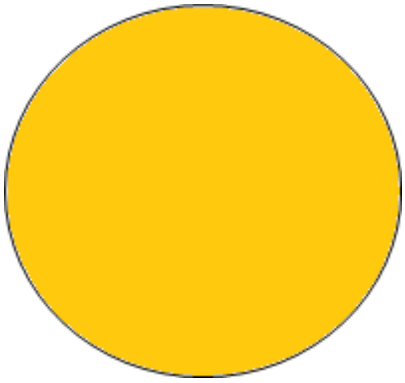
Tím byla polyalfabetická substituce. Její princip spočívá, jak název napovídá, v užití více šifrovacích abeced. Taková šifra lépe odolává frekvenční analýze. Alberti přišel s nápadem, jak rychle a efektivně šifrovat pomocí polyalfabetické substituce a k tomu účelu vytvořil šifrovací disk, který se skládá ze dvou otočných kotoučů. Oba kotouče mají identické počty segmentů, tvoří je kompletní abeceda, rozdíl je ve způsobu užití. Jednomu kotouči, lhostejno zda vnitřnímu či vnějšímu se druhý stává šifrovým textem. Po libovolném počtu slov lze kotouč pootočit, a tak změnit šifrovou abecedu na jinou.

Návod k vyrobení

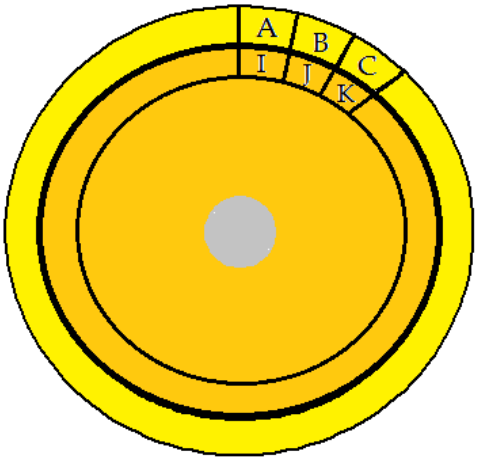
Přesto, že se jedná o velmi úspěšné zařízení, není výroba šifrovacího kotouče zdaleka náročná a zvládnete to i vy! Pokuste se o ni, abyste mohli dešifrovat/zašifrovat následující příklady. Návod k výrobě:



1. Ze čtvrtky vystřihneme jeden větší kruh.



2. Ze čtvrtky vystřihneme jeden menší kruh.



3. Podél okrajů obou kruhů vypíšeme jednotlivé znaky abecedy. Uprostřed oba kruhy spojíme připínáčkem či nýtkem, aby při sobě držely a zároveň bylo možné s oběma libovolně pootáčet.

PŘÍKLAD 1

Pokuste se pomocí vyhotoveného šifrovacího kotouče dešifrovat následující zprávu, když víte, že v každém prvním slově je písmeno A nahrazeno písmenem I a v každém

druhém nahrazeno písmenem F. *(pozn.: Povšimněte si, že text připomíná jen dlouhý sled písmen, je tedy na vás a vašich schopnostech, abyste správně určili, kdy se jedná o další slovo a systém případně pozměnili.)*

„itjmzbqgdqzmvmavkvquhqtajpjr.“

PŘÍKLAD 2

Pokuste se pomocí vyhotoveného šifrovacího kotouče zašifrovat následující zprávu. Zprávu zašifrujte dle libovolného klíče. Tedy vytvořte si vlastní postup, který by však měl splňovat určitý systém. Porovnejte pak se spolužáky svůj a jejich šifrový text a popište svými slovy, v čem vidíte přednosti a v čem úskalí polyalfabetického substitučního systému.

„Alberti byl především významným italským architektem.“

NOMENKLÁTOR MARIE STUARTOVNY

Úvod

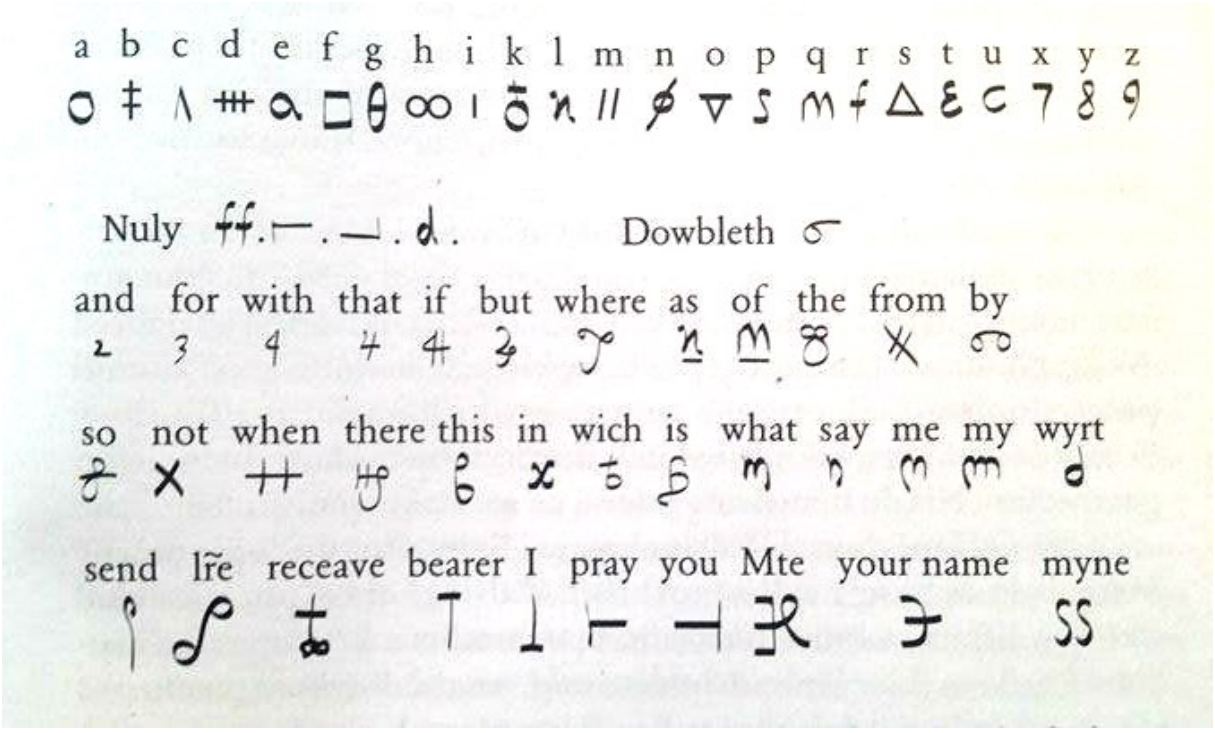
Intriky a spiknutí – nelibé činnosti, které jsou lidstvu vlastní od nepaměti. Obvykle byly a jsou konány tak, aby se dotyčný, proti němuž se osnují, do poslední chvíle neměl šanci dozvědět, co se chystá. Nejinak tomu bylo i v následujícím případu. Případu, který měl rozhodnout o životě či smrti.

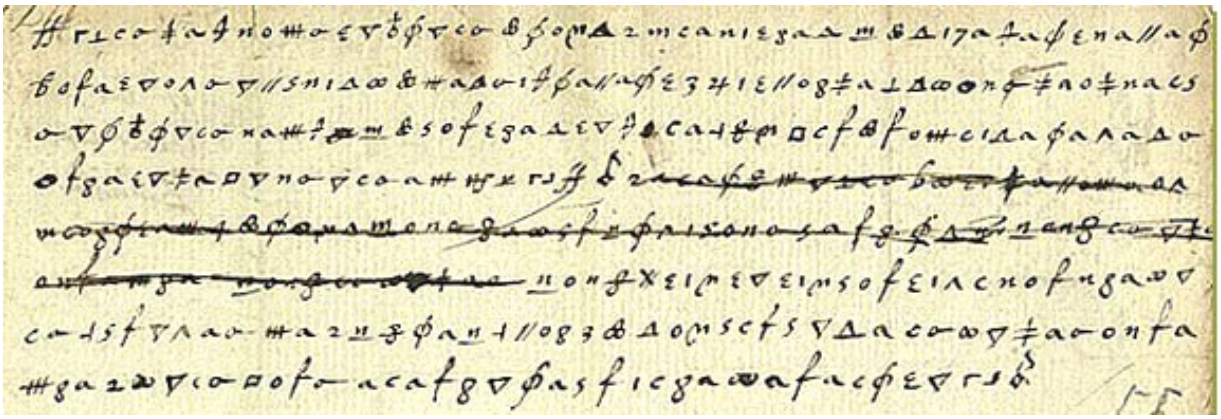
Několik let byla vězněna Marie Stuartovna, královna Skotska, pod dohledem její královské sestřenice Alžběty I. Anglická královna se totiž obávala možného nebezpečí, které by jí od Marie mohlo hrozit. Až se roku 1586 objevil jistý Anthony Babington, který přišel namísto prince, aby ji z věže vysvobodil. Nebyl to však zdaleka pohádkový čin, který Babington zamýšlel. Jednalo se o katolického šlechtice, který usiloval o záchranu své paní pro jejich společné katolické vyznání. Marie totiž byla katoličkou, kdežto Alžběta I. byla protestantskou královnou, což se pochopitelně odráželo v poměrech v zemi. Babington usiloval o Alžbětinu smrt a doufal ve vpád zahraničních katolických států do Británie a nástup Marie na anglický trůn. Pro své kruté záměry však potřeboval svolení a požehnání královny. Ale jak jej získat? Tuto otázku si jistě kladl do doby, dokud za ním nepřišel Gilbert Gifford, rovněž katolík, který mu nabídl své služby. Gifford již delší čas Marii sloužil. Pašoval k ní dopisy od jejích přívrženců ze zahraničí a ven propašovával odpovědi. To díky důmyslnému nápadu. Dopisy umisťoval do koženého obalu, který pak uložil do duté zátky, kterým se uzavřel soudek piva. Z něj pak Mariini sloužící zátku vyndali, z ní pak dopis a ten ji také předložili. Můžeme v tomto případě hovořit o tzv. Steganografii. Tento pojem si zapamatujte jako pojem, který také patří k dějinám šifrování a znamená systém utajení existence zpráv jako takových.

Babington si byl vědom ohromného rizika, které tím podstupoval. V případě, že by zprávu získala nepovolaná osoba, hrozila by jemu i jeho společníkům smrt. Rozhodl se proto text zašifrovat v naději, že přesto, že zprávu někdo získá, nebude schopen ji přečíst. Šifrování provedl pomocí nomenklátoru.

Princip a příklad

Co je to vlastně ten nomenklátor? Jedná se o kódovou knihu, kde má každý znak svůj symbol. V tomto konkrétním nomenklátoru je 23 symbolů pro 23 písmen abecedy, vynechána jsou písmena j, v a w. A 35 symbolů pro přesně stanovená slova a fráze. Také obsahovala čtyři nuly a speciální symbol, který znamenal, že následující znak je zdvojený. Šifrový text pak připomínal náhodné znaky těsně za sebou, které nedávají smysl. To ovšem pouze laikovi. Vy už jste zkušení kryptoanalytici. Pokuste se na základě následující kódové knihy dešifrovat následující text. Když budete úspěšní, zjistíte, zdali Marie Stuartovna souhlasila s osvobozením sebe sama a vraždou její sestřenice královny Alžběty, či nikoliv. *(pozn.: Přesto, že máte k dispozici kódovou knihu, jedná se o poměrně náročnou úlohu, jelikož text je psán starou angličtinou. Požádejte vyučujícího o možnost používat při dešifrování anglicko-českého slovníku, ať už v písemné, či elektronické podobě. Pokud Vám bude zpočátku připadat, že text nedává smysl, nenechte se odradit, nezapomeňte, že text je psán dobovým jazykem.)*





BLOKOVÁ TRANSPOZICE

Úvod a princip

Armand Jean du Plessiss, vévoda de Richelieu. Tento muž se bezpochyby proslavil díky románu Alexandra Duma, Tři Mušketýři. Skutečné dějiny o něm však nehovoří jako o prohnaném kardinálovi, či soku udatného D´artagnana, ale především jako o velmi významném státníkovi, prvním ministrovi francouzského krále Ludvíka XIII. a dalo by se bez nadsázky tvrdit, jako o druhém nemocnějším muži v zemi.

Pravdou však zůstává, že i přes jeho zbožnost a diplomatické schopnosti šlo o mstivého, velmi ambiciózního a nelítostného muže. K uskutečňování svých záměrů užíval i šifer. Zpočátku využíval služeb významných francouzských luštitelů, později vytvořil šifru vlastní. Tzv. blokovou, chceme-li Richelieho transpozici.

Proč blokovou? Před šifrováním se text rozdělí na stejně dlouhé skupiny, tedy bloky znaků. Délka bloku je dána počtem písmen zvoleného hesla. Ono heslo může být jakékoliv slovo. Písmenům hesla přiřadíme čísla, tak jak jdou za sebou. Poté je seřadíme tak, jak za sebou stojí v abecedě. Dojde k prohození znaků daného hesla, čímž dostaneme tzv. permutaci a s touto permutací dále šifrujeme.

Tedy pro příklad. Určíme si heslo: LUDVIK. Očíslujeme písmena hesla LUDVIK = 123456, získáme permutaci DIKLUV = 356124. Tuto permutaci následně použijeme pro šifrování textu: Zatkněte d´Artagnana a uvězněte ho v Bastile.

```
OT:   ZATKNE TEDART AGNANA AUVEZN ETEHOV BASTIL E
KLÍČ: 356124 356124 356124 356124 356124 356124
ŠT:   TNRZAK DRTTEA NNAAGA VZNAUE EOVETH SILBAT E
```

Richelieu následně celý text přepsal jako dlouhý sled malých písmen bez mezer, aby nijak nenaznačil délku použitého hesla, tedy: *trnzakdrtteannaagavznaueeovethsilbate*.

PŘÍKLAD

Téměř po celé druhé půlstoletí 16. věku byly vedeny náboženské války ve Francii. V boji proti sobě stanuli katolíci a francouzští protestanti – hugenoti. Ten však neměl jasného vítěze ani poraženého. Roku 1598 byl totiž vydán edikt Nantský, který zaručoval rovnost obou náboženství. Zdánlivě smířlivý akt však nepřinesl trvalý mír. Tam, kde edikt nebyl dodržován, neváhal Ludvík XIII. povstání potlačit vojenskou silou.

Panovník vojensky či diplomaticky porazil jednotlivé odbojné regiony a města, až na jedno. Tím byla proslavená pevnost La Rochelle, která poskytla útočiště hugenotům a její obyvatelé, usilující o co největší možnou míru nezávislosti na panovníkově vládě, se připojili k hugenotskému povstání. Ani podpora larochellských ovšem nepřinesla protestantům úspěch, byli poraženi a na ostrovy kolem pevnosti byla umístěna královská vojska. Obyvatelé La Rochelle byli ovšem příliš hrdí, než aby se vzdali svých privilegií. Jenže, kde hledat spojence, když protestanti utržili již tolik porážek. Naděje ležela na druhé straně kanálu La Manche. Naděje jménem Anglie.

Angličané se vylodili a začali s napadáním francouzských pozic. Když se o tom Ludvík dozvěděl, rozhodl se pro radikální krok, v říjnu roku 1627 započal s obléháním města. No a konečně v únoru příštího roku panovník svěřil velení obléhání do rukou svého pobočníka – kardinála Richelieu. Zdání, že muž víry byl špatnou a mírnou volbou pro takovou povinnost je přinejmenším úsměvné. Ihned po přidělení pravomocí započal s plánováním útoku.

Představte si, že jste jedním z vrchních velitelů katolického vojska a přišla Vám zpráva přímo od kardinála. Posel, který zprávu doručil, vás obeznámil s tím, že indicií k heslu je: „Pobočníkův zbraň královského mušketýra.“ Pokuste se na základě svých dosavadních znalostí zprávu dešifrovat, abyste splnili Richelieův rozkaz.

TZAUMOCIDEJECENAOTEHZBREBNAOCRANBINEUUDOKUTOAKECT

Kardinálův plán naneštěstí pro oblehatele ztroskotal. I nadále však zůstal Richelieu královým zástupcem ve vedeném boji. Ještě několikrát společně čelili anglické ofenzivě. Až do 26. října 1628, kdy se hladem, nemocemi a bojem vysílení obránci slavné La Rochelle uchýlili ke kapitulaci. Den na to bylo město obsazeno královským vojskem. V následujících několika letech město prošlo rekatolizací a počet katolíků ve městě časem převýšil počet hugenotů. Taková byla neúprosná, leč úspěšná politika slavného kardinála Richelieu – zástupce polické scény, duchovenstva a kryptografie.

ŠIFRA PLAYFAIR

Úvod a princip

Šifra Playfair je první z těch, které nás budou zajímat v rámci moderních dějin šifrování. Snad by se mohlo zdát, že během starověku, středověku a novověku byly všechny šifry již dávno vymyšleny. Lidská tvořivost je však neomezená a co víc, tvořili se naopak stále dokonalejší a propracovanější šifrovací systémy. Jeden takový byl sestrojen věhlasným britským vědcem Charlesem Wheastonem roku 1854. Onen kryptografický počin však nedostal jméno, jak tomu obvykle bývá, po svém autorovi, nýbrž po jeho příteli, nadšeném propagátorovi šifry, skotském baronovi a poslanci britského parlamentu Lyonu Playfairovi. Diplomacie si vždy žádala kvalitní šifrovací systémy.

Playfairova šifra pracuje s čtvercovou tabulkou o 5 x 5 polích, dalo by se říci, že s Polybiovým čtvercem, se kterým jsme se již v minulosti setkali. Zde ovšem, na rozdíl od starověkého modelu, Playfairova šifra pracuje výlučně s heslem. Do tabulky nejprve vypíšeme znaky hesla a ostatní pole doplníme o zbývající znaky abecedy. Tedy pro příklad, když zvolíme heslo Wheastone, tabulka bude vypadat následovně.

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

Ještě předtím než začněme šifrovat, je zapotřebí upravit otevřený text. Nešifrujeme zde jednotlivé znaky, ale dvojice znaků, tedy bigramy. Proto v souvislosti s Playfairovou šifrou hovoříme o bigramové substituci.

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

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

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

Obě písmena bigramu mohou být ve stejném řádku, ve stejném sloupci, nebo je každé z nich v jiném řádku i jiném sloupci. Podle toho, který z případů nastane, volíme konkrétní pravidlo:

1) Pokud leží obě písmena ve stejném řádku, je každé písmeno bigramu nahrazeno písmenem ležícím v tabulce vpravo od něj. Poslední písmeno v řádku se nahradí prvním písmenem téhož řádku.
2) Pokud leží obě písmena ve stejném sloupci, je každé písmeno bigramu nahrazeno písmenem pod ním. Je-li písmeno v posledním řádku je nahrazeno prvním písmenem téhož sloupce.
3) Pokud je každé z písmen v jiném řádku a sloupci, je každé písmeno bigramu nahrazeno písmenem nacházejícím se v průsečíku jeho vlastního řádku a sloupce obsahujícího druhé písmeno bigramu.

Dešifrování probíhá samozřejmě také po bigramech, pouze v prvním pravidle nahradíme slovo „vpravo“ slovem „vlevo“, slovo „první“ slovem „poslední“ a naopak. Podobně se změní druhé pravidlo, zatímco třetí pravidlo zůstane zcela beze změn.

PŘÍKLAD 1

Pokuste se na základě získaných znalostí dešifrovat následující zprávu. Heslo tabulky zní: ***„TABULA“***

„OM KY BR TB UK DO SR RA WM WT TB UP HA RM BW UO IL ID“

PŘÍKLAD 2

Pokuste se na základě získaných znalostí zašifrovat libovolný text s libovolným heslem. Porovnejte pak se spolužáky svůj a jejich šifrový text.

ŠIFRA BIFID

Úvod a princip

Fakt, že šifry se vždy týkaly především vojenských a politických záležitostí, už snad není třeba zdůrazňovat. Možná vás ale překvapí, že na přelomu 19. a 20. století přechází do soukromé sféry zájmu. Felix Marie Delastelle – jméno, které nebylo jménem diplomata, vojáka ani politika, ale co víc, dokonce ani matematika, či lingvisty, či znalce jiného příbuzného oboru kryptografie. Našli bychom ho v námořním přístavu ve Francii jako účetního skladů a jako vášnivého kryptografa - amatéra.

Čím je jeho dílo tolik významné? V čem je jeho prvenství? Inu, napadlo vás někdy, pokud jste sami někdy šifrovali, jaké by to bylo nešifrovat pouze z otevřeného do šifrového textu? Pak jste byli o více než století předběhnuti tímto pánem. Ten přišel se šifrou Bifid, která pracuje s tzv. „mezitextem“, tedy nástrojem, který stojí mezi otevřeným a šifrovým textem.

Jak vypadá „mezitext“. „Mezitext“ je podle Delastelle dvouřádkový text o pěti znacích. Jako šifrovací tabulka slouží podobný čverec 5 x 5 políček jako u šifry Playfair, ale s tím rozdílem, že jej doplníme záhlaví, v němž očíslujeme řádky a sloupce. Zvolíme-li heslo KRYPTOLOGIE, bude čtverec vypadat takto:

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

Před šifrováním text rozdělíme do skupin o pěti znacích. Pro každé písmeno pětice, pod něj zapíšeme, do prvního řádku číslo řádku, do druhého řádku číslo sloupce. Z tohoto dvouřádkového „mezitextu“ pak získáme šifrový text tak, že bereme první a druhou číslici v horním řádku, pak třetí a čtvrtou číslici v témže řádku, potom poslední číslici

v horním řádku a první číslici v dolním řádku, následuje druhá a třetí číslice v dolním řádku a nakonec čtvrtá a pátá číslice v dolním řádku. V každé z těchto dvojic znamená první číslice číslo řádku v šifrovacím čtverci a druhá číslo sloupce. Nakonec tedy získáme pětici písmen, která tvoří příslušnou část šifrového textu. Pokud na konci textu vyjde kratší skupina než pětimístná, tak zde celý postup. Pro ukázku zašifruji citát: Moudrost je dcerou zkušenosti. Leonardo da Vinci, s použitím výše zobrazeného čtverce

```
MOUDR  OSTJE  DCERO  UZKUS  ENOST  ILEON  ARDOD  AVINC  I
42531  24142  33212  55154  24241  22224  31323  35243  2
31142  15525  43521  15115  54155  42514  12414  12443  4
JWYKJ  IPOZE  COIFO  ZTHUT  IITHZ  LLNEP  ABAIP  FIAIM  I
```

Při dešifrování pochopitelně vytváříme „mezitext“ po řádcích a do otevřeného textu pak převádíme dvojice číslic stojících pod sebou v horním a dolním řádku „mezitextu.“

PŘÍKLAD

Pokuste se dešifrovat následující text pomocí následujícího čtverce:

LLUAL ZNJTC BREVI JXU

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

ZÁVĚR

Zpracováním tohoto textu jsem se mnohému naučil. Pochopil jsem, že historie šifrování je natolik rozsáhlé téma, že z něj musím vybrat jen relativně malou část. Rozhodl jsem se prozkoumat vývoj substitučních šifrových systémů od jejich vzniku ve starověku po komplikované šifry z počátku 20. století. Podrobně jsem popsal několik šifrových systémů. U jednodušších z nich jsem popsal také způsoby jejich luštění, u všech postupy použité při šifrování a při dešifrování. Tím jsem splnil cíl, který jsem si předsevzal pro zpracování teoretické části práce.

Cílem praktické části bylo navázat na toto stručné shrnutí poznatků získaných studiem odborné literatury a vhodným způsobem zařadit kryptologii do výuky informatiky na středních školách. Dílčím cílem praktické části práce pak bylo najít způsob, který se bude jevit k dosažení hlavního cíle jako nejvhodnější. Na základě získaných teoretických znalostí i vlastních praktických zkušeností v didaktice informatiky a v didaktice dějepisu jsem shledal jako nejvhodnější nástroj pracovní listy. Ty jsou koncipovány tak, aby měl žák možnost dozvědět se něco z dobového kontextu dané šifry, pochopit její princip a prakticky aplikovat, co se naučil. Věřím, že takto zpracované pracovní listy mohou akcentovat mezioborové vztahy mezi dějepisem a informatikou. Rád bych později v rámci souvislé pedagogické praxe tyto listy ve výuce použil a měl tak možnost potvrdit či vyvrátit mé předpoklady. Praktické provedení výuky s využitím pracovních bych pravděpodobně doplnil dotazníkovým šetřením, cíleným na vzdělávané subjekty.

LITERATURA

BERLOQUIN, Pierre. *Skryté kódy a velkolepé projekty.* 1. vyd. Praha: Knižní klub, 2011. 384 s. ISBN 978-80-242-2847-1.

BOONE, J. V. *Brief History of Cryptology.* 1st ed. Annapolis: Naval Institute Press, 2005. 192 s. ISBN 1-59114-084-6.

JANEČEK, Jiří. *Rozluštěná tajemství.* 2. vyd. Praha: Petr Tychtl - Nakladatelství XYZ, 2008. 268 s. ISBN 978-80-86864-96-9.

Kolektiv. *Frekvence písmen, bigramů, trigramů, délka slov* [online]. Brno: Centrum zpracování přirozeného jazyka Fakulty informatiky Masarykovy univerzity, 2008. [cit. 2012-01-10] Dostupné z: <http://nlp.fi.muni.cz/cs/Frekvence_pismen_bigramu_trigramu_delka_slov>

MAŇÁK, Josef. *Nárys didaktiky*. 3. vyd. Brno: Masarykova univerzita, 2003. 104 s. ISBN 80-210-3123-9.

MUSÍLEK, Michal. *Kapitoly z dějin informatiky.* 1. vyd. Univerzity Hradec Králové: Gaudeamus, 2011. 193 s. ISBN 978-80-7435-129-7.

MUSÍLEK, Michal. *Šifry a kódy* [online]. 2010 [cit. 2012-01-10] Dostupné z: <http://www.musilek.eu/michal/sifry.html?menu=mat>

PRŮCHA, Jan (ed.). *Pedagogická encyklopedie*. Vyd. 1. Praha: Portál, 2009. 936 s. ISBN 978-80-7367-546-2.

SINGH, Simon. *Kniha kódů a šifer.* 2. vyd. Praha: Argo a Dokořán, 2009. 384 s. ISBN 978-80-7363-268-7 (Dokořán), ISBN 987-80-257-0144-7 (Argo).

VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma.* 1. vyd. Praha: Albatros, 2006. 400 s. ISBN 80-00-01888-8.

VORLÍČEK, Jaroslav. Řešení úloh č. 7-9.*Crypto-World, informační sešit GCUCMP,* prosinec 2003, ročník 5, číslo 12, s. 9 – 20. ISSN 1801-2140.