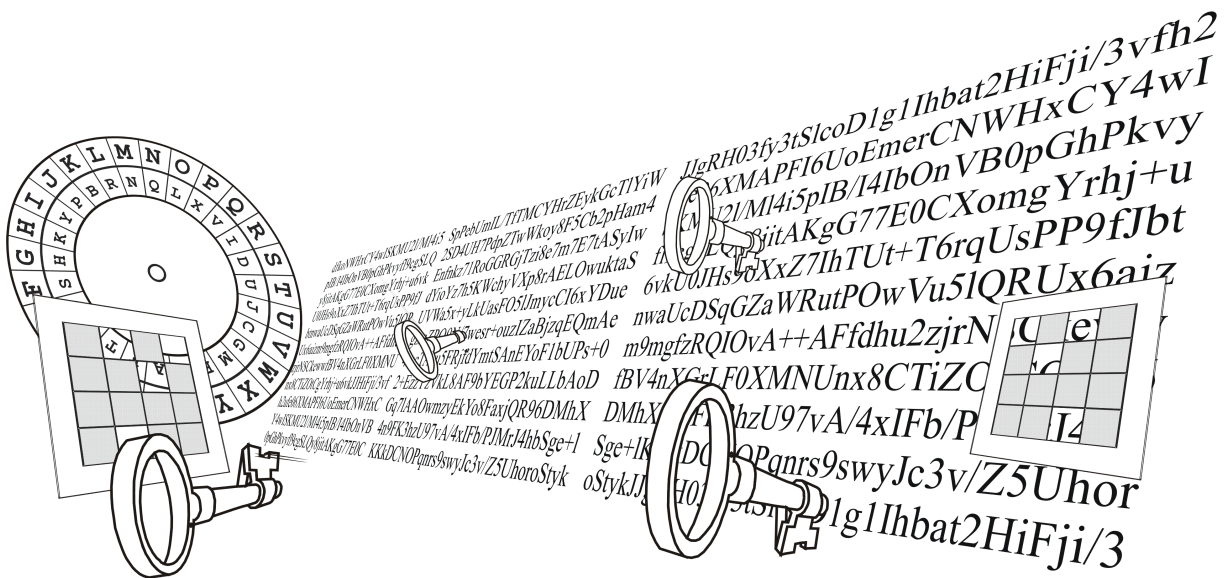


Ladislav Huraj

# NEBOJME SA ŠIFROVANIA



# Obsah

<b>1 Úvod.....</b>	<b>2</b>
<b>2 Fylogenéza kryptografie .....</b>	<b>4</b>
2.1 RANÁ ÉRA KRYPTOGRAFIE .....	4
2.2 MECHANICKÉ A ELEKTRONICKÉ ŠIFROVACIE STROJE .....	9
2.3 ÉRA POČÍTAČOV .....	13
2.4 OD ASYMETRICKEJ KRYPTOGRAFIE AŽ PODNES .....	13
2.5 ZHRNUTIE .....	14
<b>3 Ontogenéza kryptografie .....</b>	<b>15</b>
3.1 KRYPTOGRAFIA NA ZÁKLADNEJ ŠKOLE .....	15
3.1.1 Motivácia.....	15
3.1.2 Vlastné šifry .....	16
3.1.3 Mechanické šifrovacie pomôcky .....	18
3.1.4 Autokľúč.....	22
3.2 ŠTÚDIUM KRYPTOGRAFIE NA STREDNEJ ŠKOLE .....	23
3.2.1 Caesarova šifra .....	23
3.2.2 Bigramová šifra .....	24
3.2.3 Vigenerova šifra .....	25
3.2.4 Autokľúč.....	25
3.2.5 Fleissnerova otočná mriežka .....	26
3.2.6 Vernamova šifra .....	28
3.2.7 Šifrovacie zariadenie Enigma.....	28
3.2.8 DES .....	29
3.2.9 Asymetrické šifrovanie.....	32
3.3 ZÁVER .....	35
<b>4 Podporné programy .....</b>	<b>36</b>
4.1 PROSTREDIE PROGRAMOV .....	36
4.2 TECHNICKÁ REALIZÁCIA .....	39
<b>5 Záver.....</b>	<b>40</b>
<b>6 Slovník pojmov .....</b>	<b>42</b>
<b>Zoznam citovanej literatúry .....</b>	<b>45</b>
<b>Príloha I.....</b>	<b>47</b>

Ladislav Huraj

# NEBOJME SA ŠIFROVANIA

Metodicko-pedagogické centrum v Bratislave  
Bratislava 2002

# Kapitola 1

## Úvod

Šifrovanie bolo donedávna výsadou iba tajných služieb, armád, špionáže, príp. filmových hrdinov typu James Bond. V súčasnosti sa, hlavne vďaka rýchlemu rozvoju Internetu, stáva šifrovanie každodennou vecou účastníkov pri komunikácií. Ved' len v bankovníctve, napr. pri prezeraní účtov cez Internetbanking prebieha komunikácia šifrovane. Takisto komunikácia cez mobilné telefóny GSM využíva šifrované spojenie. Tento fakt si bežný používateľ vôbec neuvedomuje.

Šifrovanie, ako každý vedný odbor, má svoje históriu. História šifrovania sa môže človek zaoberať z viacerých dôvodov: pre potešenie zo štúdia, kvôli poznaniu, ktoré uľahčuje správne orientovať svoje bádanie v tejto oblasti, alebo kvôli poučeniu o zákonitostiach vývoja myslenia v tomto odvetví.

V tejto práci chceme poukázať na ďalší spôsob, prečo sa zaoberať históriou kryptografie. Sústreďujeme sa na poučenie, ktoré štúdium histórie kryptografie prináša učiteľovi. Východiskom našich úvah bola metóda *genetickej paralely* založená na predpoklade, že ontogenéza kryptografie v určitej miere opakuje históriu rozvoja tejto vedy – fylogenezu kryptografie. Problém hľadania analógií medzi fylogenezou a ontogenézou a zhôd v ich mechanizmoch poznania sa objavuje v mnohých dielach významných didaktikov, spomeňme napr. Jeana Piageta [1].

Proti myšlienke genetickej paralely bývajú uvádzané námietky poukazujúce na protiklad medzi kľukatou cestou histórie a snahou o priamosť cesty pri vyučovaní. Autori takýchto námietok, nechápu správne podstatu metódy genetickej paralely. Vývoj redukujú na chronologicky usporiadanú postupnosť udalostí. Toto je však iba východiskom. Jadrom metódy genetickej paralely je: 1. utriedenie jednotlivých javov z hľadiska ich významu pre rozvoj myslenia a 2. poznanie príčin, ktoré spôsobujú kvalitatívne zdvihy – zmeny vedúce od nižšej kvalitatívnej úrovne k vyššej úrovni. [2]

Snahou práce je zodpovedať dve základné otázky pri vyučovaní kryptológie: čo učiť a ako to učiť a rešpektovať skúsenosti, znalosti študentov, časové obmedzenia predmetu a teoretickú a praktickú stránku preberanej témy. [3]

*Kryptológia*, ako veda zaoberajúca sa šifrovaním a dešifrovaním, pozostáva z dvoch častí: *kryptografie* – časť študujúca teoretické aspekty navrhovania šifrovacích metód a *kryptoanalýzy* – časť zameraná na štúdium metód lúštenia šifier. Práca sa zámerne nezaobera implementáciou druhej časti – kryptoanalýzou do vyučovacieho procesu. Kryptoanalýzu ako oblasť, ktorá je špecifickejšia a náročnejšia oproti kryptografii, jednak nárokmi na vedomosti žiakov, jednak časovou dotáciou, je možné podľa potreby použiť ako

rozširujúce cvičenie pri preberaní určitého šifrovacieho algoritmu. V práci sme sa zamerali predovšetkým na celok kryptografia a na jeho zavedenie do vyučovania.

Snáď každé dieťa počas svojich hier použilo nejaký druh tajného písma, kódov ako napr. písmená zobrazované na rukách. Deti odjakživa priťahuje záhada, tajomstvo, tajné mapy a objavovanie pokladov. Túto skutočnosť sme brali do úvahy pri zavádzaní celku kryptografie do vyučovania.

Pripomeňme, že podľa osnov predmetu Informatika [4], cieľom vyučovania informatiky je sprístupniť základné pojmy a techniky používané pri práci s údajmi a pri tvorbe algoritmov a výpočtových procesov. Vyučovanie kryptológie tento cieľ dokonale napĺňa. Zostáva zodpovedať otázku, kam v osnovách kryptografiu zaradiť.

Na strednej škole je pre kryptografiu vytvorený priestor predovšetkým v štvorročnom voliteľnom predmete Informatika. V zameraní Informačné a komunikačné technológie v prostredí Internetu je jedna časť venovaná práve "Počítačovej bezpečnosti a ochrane údajov." Do tejto kapitoly spadá aj kryptografia.

Klasické kryptosystémy okrem iného predstavujú zaujímavú triedu algoritmov, ktorých naprogramovanie si vyžaduje zvládnuť prácu s textovými súbormi, viacrozmernými poliami a pod. [5] Preto je ich možné spracovávať aj v zameraní "Programovanie pre pokročilých."

V texte sa okrem kryptoanalýzy vedome nezaobráame *steganografiou*. Steganografia je oblasť, ktorá by bola istotne pre žiakov zaujímavá, jej vývoj má ale iné smerovanie ako kryptografia.

Okrem predostretia vzťahu ontogenézy a fylogenézy kryptografie sa snažíme v práci nájsť vhodný spôsob vyučovania tohto odvetvia, a tým vyplniť medzeru, týkajúcu sa vyučovania kryptografie, v predmete Informatika.

Prvá kapitola podáva obraz fylogenézy kryptografie prostredníctvom časovej osi. Uvádza predovšetkým zlomy, ktoré znamenali kvalitatívne zmeny pre rozvoj kryptológie.

Cieľom druhej kapitoly bolo vybudovať metodický systém výučby kryptografie na základnej a strednej škole. Navrhnuť aktivity a súbor pomôcok, ktoré by pomohli žiakom pochopiť princípy využívané v kryptografii.

Cieľom tretej časti bolo implementovať pomocné programy, ktoré pomôžu učiteľovi pri rýchlej kontrole správnosti algoritmu, ale taktiež môžu napomôcť pri programovaní samotných šifrovacích algoritmov.

Práca obsahuje aj výkladový slovník základných pojmov kryptografie a ďalších termínov v nej použitých.

Naším zámerom bolo sledovať maximálnu reálnosť a podnetnosť práce, t. j. aby sa v nej hovorilo o skutočnej škole, nesústredovala sa iba na výborných žiakov, a aby stimulovala učiteľa k podobným aktivitám.

Poznamenajme, že kryptológia je špecifická veda. Na rozdiel od iných oblastí informatiky, na dosiahnutie poznatkov, na ktorých by bolo možné stavať vlastné kryptografické aplikácie nestačí jedna prednáška, alebo prečítanie populárnej knihy. Zaujímavá história kryptológie a atraktívne aplikácie však môžu byť dobrou motiváciou pre štúdium aj tých teórií, ktoré majú študenti tendenciu považovať za príliš teoretické [5].

## Kapitola 2

### Fylogenéza kryptografie

Na znázornenie fylogény kryptografie použijeme časovú os, na ktorej vyznačíme dôležité medzníky v jej vývoji. Hoci sme sa zamerali predovšetkým na fylogézu kryptografie, uvádzame aj niektoré dôležité časové údaje z fylogény kryptoanalýzy. Toto je spôsobené bezprostrednou previazanosťou týchto dvoch disciplín.

#### 2.1 Raná éra kryptografie

- okolo r. 1900 p.n.l.

Egyptský pisár použil neštandardné hieroglyfické symboly namiesto obvyklých hieroglyfov, čím sa text pre bežného čitateľa stal zašifrovaným.



Obr. 2.1 Šifrované hieroglyfy (šifrované hieroglyfy sú vľavo, ich otvorené ekvivalenty vpravo) [6]

- okolo r. 1500 p.n.l.

Tabuľka z Mezopotámie obsahovala zašifrovanú formulu na výrobu glazúrovej keramiky. Použitá šifra využívala substitúciu písmen za písmená, ktoré majú rovnakú zvukovú hodnotu v rôznych slovách.

- roky 600-500 p.n.l.

Hebrejci používali jednoduchú reverznú substitučnú šifru *atbaš*. V tejto šifrovacej metóde je prvé písmeno abecedy nahradené posledným, druhé predposledným atď. a naopak. Názov *atbaš* je odvodený od toho, že prvé písmeno hebrejskej abecedy alef je nahradené posledným písmenom tav, druhé bet je nahradené predposledným sin. Prejavy tohto šifrovania nájdeme aj v Starom zákone. V hebrejskej literatúre sú známe podobné ďalšie dve substitúcie: *albam* a *atbah*. [7, 8]

Atbaš:

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

Albam:

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

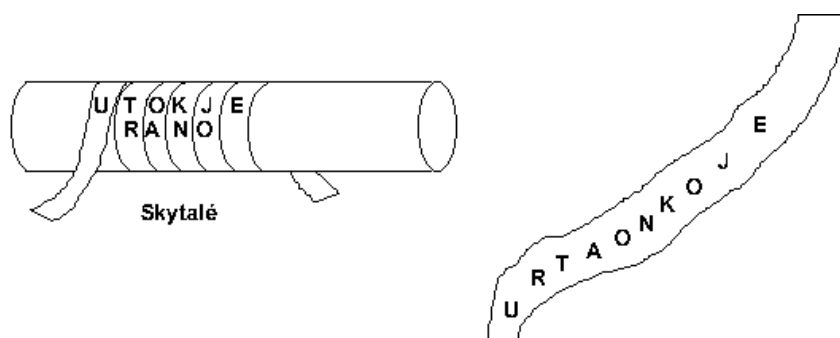
Atbah:

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

			Atbash	Albam	Atbah
Aleph 1	א	ל	ה	ש	ח
Beth 2	ב	ט	ו	ז	ט
Ghime1 3	ג	ד	ז	ח	ז
Daleth 4	ד	ה	ח	ט	ו
He 5	ה	ו	ט	ז	ו
Vau 6	ו	ז	ח	ט	ו
Zain 7	ז	ח	ט	ז	ו
Heth 8	ח	ט	ו	ז	ו
Teth 9	ט	ו	ז	ח	ו
Yod 10	י	ז	ח	ט	ו
Kaph 20	כ	פ	ק	צ	ח
Lamed 30	ל	מ	נ	ס	ע
Mem 40	מ	נ	ס	ע	ד
Nun 50	נ	ו	ז	ח	ו
Samekh 60	ס	ע	ד	ו	ו
Ayin 70	ע	ד	ו	ז	ו
Phe 80	פ	ק	צ	ח	ו
Tzaddi 90	צ	ח	ו	ז	ו
Quoph 100	ק	צ	ח	ט	ו
Resh 200	ר	ש	ז	ח	ו
Shin 300	ש	ז	ח	ט	ו
Taw 400	ת	א	ה	ש	ח

### • okolo r. 500 p.n.l.

V starom Grécku v Sparte používali prvú známu mechanickú pomôcku na šifrovanie – *skytalé*. Využívali ju spartskí stratégovia na vojenských výpravách. Tento šifrátor mal tvar dreveného valca, na ktorý sa prúžok za prúžkom tesne vedľa seba namotal pruh papyrusu, kože alebo pergamenu. Správa sa vypisovala smerom od jedného konca valca k druhému, až sa zaplnil celý papyrus. Potom sa pruh odmotal. Správa na ňom nedávala zmysel, pokiaľ sa u príjemcu nenamotala na rovnako hrubý valec, pretože písmena boli poprehadzované (transponované). [9]



Obr. 2.2 Šifrovacie abecedy používané antickými hebrejcami [8]

Obr. 2.3 Šifrovacia pomôcka v Sparte – skytalé. Otvorený text je "UTOKJE RANO", šifrovaný text "URTAONKOJE"

### • rok 360 p.n.l.

AINEIAS TAKTIKOS napísal dielo "Taktika" o vojenskom umení. V časti "Poliorketika" uvádza 16 rôznych šifrovacích metód. Jedna z nich je založená na rovnakom princípe ako morzeovka. Iná využíva nahradenie znakov gréckej abecedy číslami, čo je spôsob manipulácie s údajmi v dnešnej kryptografii. [7]

### • okolo r. 300 p.n.l.

V Indii sa používala substitúcia písmen za písmená, ktoré sú im foneticky príbuzné. [9]

- roky 60-50 p.n.l.

JULIUS CAESAR (100-44 p.n.l.) používal jednoduchú substitučnú šifru, ktorá nesie po ňom aj pomenovanie. Caesar používal niekoľko šifier, ale kniha, kde sa opisovali, sa nezachovala. V Caesarovej šifre sa každé písmeno nahradí písmenom, ktoré v abecednom poradí leží tri písmena za ním. Napr. výrok LIST ZNICIT by v Caesarovom liste nadobudol tvar OLVW CQLFLW. Na tú dobu to bola prakticky nerozlúštiteľná šifra, jednoduchá a účinná, až kým ju neprezradil Cicero, ktorý prešiel do tábora Caesarových protivníkov. [7]

- roky 0-400?

Klasické dielo "Kama Sutra" uvádza kryptografiu ako 44. a 45. zo 64 umení, ktoré majú muži a ženy poznať.

- roky 725-790?

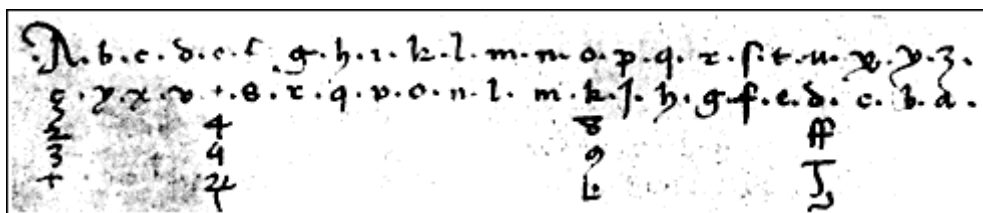
ABU `ABD AL-RAHMAN AL-KHALIL IBN AHMAD IBN `AMR IBN TAMMAM AL FARAHIDI AL-ZADI AL YAHMADI napísal knihu o kryptografií inšpirovanú jeho riešeniami kryptogramov pre Byzanského cisára. Jeho riešenie bolo založené na znalosti otvoreného textu, čo je štandardná kryptoanalytická metóda použitá napr. počas 2. svetovej vojny na správy Enigmy.

- rok 1379

Najstaršie zachované *nomenklátory* zostavil tajomník vzdor pápeža Klementa VII. GABRIELI DI LAVINDE na spojenie s jeho vyslancami. Nomenklátory obsahujú okrem úplnej substitučnej abecedy aj dvoj písmenové kódy pre jeden až dva tucty najfrekvencovanejších slov alebo mien, a navyše tiež tzv. klamače, nevýznamové skupiny písmen, ktoré mali sťažiť kryptoanalýzu zašifrovaných textov. Nomenklátory postupne rozširovali svoj slovník na stovky až tisíce kódových slov. Zaujímavé je, že sa používali dlho a masovo, a to aj napriek tomu, že boli známe oveľa dokonalejšie metódy šifrovania. Mali totiž jednu neprekonateľnú výhodu: ich použitie bolo jednoduché. Každý si mohol zložitost' nastaviť podľa svojho slovníka kódov. Je to prvé riešenie všeobecného rozporu medzi bezpečnosťou a rýchlosťou (praktickosťou) šifier. [10]

- rok 1401

Doposiaľ najstaršiu známu západnú *homofónnu šifru* zostavil vojvoda SIMEONE DE CREMA z Mantovy. [10, 11]



Obr. 2.4 Prvá známa homofónna šifra od Simeone de Crema z roku 1401 [11]

Príklad nomenklátora:

Pozostáva z homofónnej substitúcie hlások, klamačov a substitúcie pre vybrané slová a slabiky.



Homofónna substitúcia hlások:

OT: 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  
 ŠT: w ξ y s v d e t v x c r q j p o n l m k l a h g b f  
 2 4 7 8 H  
 3 u 5 9 τ  
 + ψ i z

(O niečo jednoduchšiu podobnú substitúciu zostavil vojvoda z Mantovy v roku 1401)

klamače: ss+t8j kionulls Hrtgf 25xrq lilsa

slabiky: OT: ne na no ni in en an pr st od do ja je my  
 ŠT: X T U V π 89 W S ρ φ A BB Ca μ

slová:

Pápež = pp, Napoleon = np, Florencia = flr, Benátky = bey, kráľ = ro,  
 Rím = rm, Francúzko = fr, mesto = tw, ulica = st.

Otvorený text: Pápež odišiel z Benátok do Ríma.

Šifrový text: kionulls pp φvm74r lilsa f bey A rm.

respektíve: kionullsppφvm74rlilsafbeyArm.  
 (do ŠT sú vložené dva klamače). [10]

## • rok 1412

Arabský učenec SHIHAB AL-DIN ABU `L-`ABBAS AHMAD BEN `ALI BEN AHMAD `ABD ALLAH AL-QALQASHANDI dokončil svoju 14 zväzkovú encyklopédiu, ktorá bola určená pre úradníkov ako systematický prehľad o všetkých dôležitých oblastiach ľudských vedomostí a obsahuje aj rozsiahle informácie o kryptológii. [7]

## • roky 1466-1467



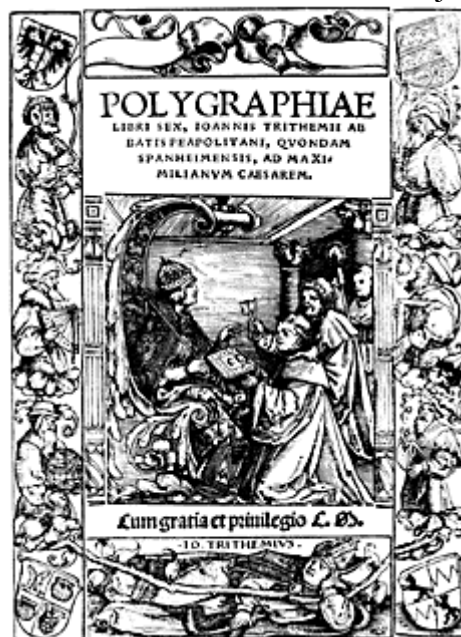
Obr. 2.5 Albertiho šifrovací disk [12]

LEON BATTISTA ALBERTI – nazývaný aj otcom západnej kryptológie. Bol všestranne vzdelaný človek, je známy ako autor prvej tlačenej knihy o stavitelstve. Albertiho 25 stranová práca je prvá práca napísaná v západnej Európe venovaná kryptoanalýze. Dielo obsahuje výklad lúštitel'ských postupov na základe jazykových znalostí, roztriedenie systémov šifrovania na substitúciu a transpozíciu, objav *polyalfabetickej substitúcie* a šifrovanie kódov. K substitúcií zostrojil Alberti *šifrovací disk* pozostávajúci z dvoch otáčavých kotúčov reprezentujúcich otvorené a zašifrované znaky, pričom ich otáčanie simulovalo polyalfabetickú substitúciu. [13]

## • rok 1518

Prvá tlačená kniha s kryptologickou náplňou bola kniha od známeho benediktínskeho mnícha JOHANNESA TRITHEMIUSA. V piatej knihe jeho súboru šiestich kníh "Polygraphiace libri sex" je zavedená tzv. "tabula recta", ktorá je základom pre polyalfabetické šifry. [7]

Obr. 2.6 Trithemiusove dielo "Polygraphiae libri sex" [12]



```

abcdefghijklmnopqrstuvwxyz
bcdefghijklmnopqrstuvwxyz
cdefghijklmnopqrstuvwxyzab
defghijklmnopqrstuvwxyzabc
efghijklmnopqrstuvwxyzabcd
...
zabcdefghijklmnopqrstuvwxyz

```

Obr. 2.7 Trithemiusova tabula recta (prepis v latinke)

### • rok 1553

Vyšla brožúra "La cifra" nenápadného talianskeho šľachtica GIOVANA BATISTU BELASA opisujúca kryptosystém, ktorého základom je tajný kľúč. Tajným kľúčom je tu slovo, príp. veta, ktorá sa opakovane píše nad otvorený text. Každé písmeno otvoreného textu je potom šifrované abecedou, ktorá je určená písmenom nad ním. Pri šifrovaní sa používala Trithemiusovu tabuľka. V tomto systéme už význam a úloha *kľúča* vystupujú do popredia. Jeho výhoda je zrejmá. Jeden a ten istý systém je možné podľa potreby variabilne meniť. To už nie je ďaleko od myšlienky, vytvoriť taký systém, v ktorom by bola kľúčom samotná správa. Takýto autokľúč navrhol v roku 1586 Vigenère. [7, 13]

### • rok 1563

Talian GIOVANNI BATTISTA PORTA napísal niekoľko kníh. Jeho najslávnejšia kniha z oblasti kryptológie sa nazývala "De Furtivis Literarum Notis" vyšla v roku 1563 a "vládla" v kryptografii 300 rokov. Porta v knihe jasne a výstižne sústredil kryptologické poznatky vtedajšej doby, rozdelil šifry na substitučné a transpozičné, uviedol prvú digrafickú šifru. Ďalej zverejnil návod na lúštenie monoalfabetickej substitúcie a vypracoval aj niekoľko metód lúštenia polyalfabetických šifier. Portova digrafická šifra bola tvorená tabuľkou, kde riadky a stĺpce boli označené písmenami abecedy. Vo vnútri tabuľky boli symboly (značky), ktoré reprezentovali šifrové výrazy vždy namiesto dvojice písmen otvoreného textu, určených riadkom a stĺpcom tabuľky. Jeho najväčším prínosom bola malá poznámka, ktorá definovala *všeobecnú polyalfabetickú šifru*. Doporučil čo najdlhší kľúč v Belasovom systéme a potom poznamenal, že Trithemiusovu tabuľka nemusí obsahovať len vzájomne posunuté abecedy, ale abecedy úplne poprehadzované, nesúvisiace. Tým vznikla všeobecná polyalfabetická substitúcia, pretože jednotlivé písmená otvoreného textu sú šifrované rôznymi substitúciami, ktoré určuje kľúč. [13]

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	Z	
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	A
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	B
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	C
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	D
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	E
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	F
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	G
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	H
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	I
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	L
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	M
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	N
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	O
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	P
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	Q
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	R
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	S
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	T
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	V
⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	Z

Obr. 2.8 Portova digrafická šifra [14]

- rok 1585

Francúz BLAISE DE VIGENÈRE navrhol vo svojej knihe "Traicté des Chiffres" *autokľúč*, t. j. kľúč, ktorý sa sám reprodukuje. Belaso prv nechal opakujúci sa kľúč bežať nad otvoreným textom. Vigenère ako kľúč použil len jedno písmeno, zašifroval ním prvé písmeno otvoreného textu a výsledné písmeno šifrového textu použil ihneď ako nasledujúce písmeno kľúča. Kľúč sa teda vytváral automaticky. Jeho druhá metóda autokľúča bola podobná. Po zašifrovaní prvého písmena otvoreného textu (prvým a jediným písmenom kľúča), bolo ako nasledujúci kľúč použité práve toto písmeno otvoreného textu. Dnes je Vigenèrovo meno spojené (kryptologicky) s oveľa jednoduchšou šifrou, ktorá vznikne z Belasovho systému použitím jednoslovného kľúča. Žiaľ, tak ako Vigenèrov autokľúč, aj Belasova polyalfabetická šifra upadli, aspoň navonok, do zabudnutia na 300 rokov. Dôvodom bola pravdepodobne prachnosť pri šifrovaní a dešifrovaní.[7, 13]

- rok 1623

Sir FRANCIS BACON popísal vo svojom diele "De Augmentis Scientiarum" biliterálnu šifru, známu v dnešnej dobe ako 5-bitové binárne kódovanie.

Obr. 2.9 Baconové kódovanie, dnes sú znaky "a" a "b" nahradené znakmi "0" a "1"  
[15]

A	B	C	D	E	F
Aaaaa	aaaab.	aaaba.	aaabb.	aabaa.	aabab.
G	H	I	K	L	M
aabba	aabbb.	abaaa.	abaab.	ababa.	ababb.
N	O	P	Q	R	S
abbaa.	abbab.	abbba.	abbbb.	baaaa.	baaab.
T	V	W	X	Y	Z
baaba.	baabb.	babaa.	babab.	babba.	babbb.

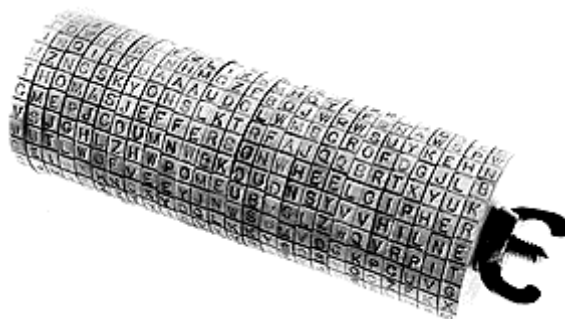
- rok 1685

JOHN FALCONER popísal vo svojom diele "Cryptomenytices Patefacta" *stĺpcovú transformáciu*. Otvorený text bol zapisovaný do obdĺžnika zľava doprava, ale vypisovaný bol po stĺpcoch, zhora nadol.

## 2.2 Mechanické a elektronické šifrovacie stroje

- rok 1790

Americký minister zahraničných vecí (neskôr prezident) THOMAS JEFFERSON vynášiel mechanický šifrátor, ktorému sa hovorí Jeffersenov valec. Pozostáva z 26 rovnakých koliesok, ktoré sú nasunuté na spoločnú os a tak vytvárajú valec. Na obode jednotlivých koliesok sú napísané všetky písmená abecedy v rozhádzanom poradí. Pri šifrovaní sa jednotlivé kolieska proti sebe otáčajú tak, že nakoniec dávajú vo zvolenom riadku na obode valca požadovanú správu. Šifrovaný text sa prečíta z riadku nasledujúceho, alebo z iného vybraného z 26 možných. Kolieska boli číslované a mohli byť menené alebo poprehadzované. [17]



Obr. 2.10 Jeffersenov mechanický šifrátor [16]

- **rok 1817**

Plukovník americkej armády COLONEL DECIUS WADSWORTH zostrojil mechanický šifrátor podobný Albertiho disku. Počet znakov na vonkajšom kotúči rozšíril na 33, na vnútornom na 26 písmen. Kotúče spojil pomocou ozubených kolies s 26 a 33 zubami. Pri šifrovaní otáčal vnútorným kotúčom, pokiaľ sa vo vodiacom okienku neukázalo požadované písmeno. Vo vonkajšom okienku potom vyčítal šifrovaný text. Ak mal znovu šifrovať rovnaké písmeno, musel vnútorný kotúč celý opäť otočiť (o 26 pozícií). Vo vonkajšom okienku sa ale objavilo iné písmeno ako v prvom prípade, pretože vonkajší kotúč sa otočil iba o 26/33 otáčky. Po Vigenèrovom autokľúči je to ďalší systém, kde je šifrovaný text závislý od všetkých znakov predchádzajúceho otvoreného textu. Wadsworthov šifrátor bol zabudnutý. [17]

- **rok 1843**

EDGAR ALAN POE vyslovil domnienku, že pokiaľ ľudský rozum dokáže nejakú šifru vymyslieť, dokáže ju aj rozlúštiť. Tím nastolil i jednu zo základných otázok kryptológie – otázku *bezpečnosti šifier*, ktorá je aktuálna dodnes. [9]

- **rok 1854**

Anglický fyzik CHARLES WHEATSTONE vynášiel tzv. Playfairovu šifru (publikoval ju jeho priateľ Lyon Playfair), ktorou sa šifrovali vždy dve písmená otvoreného textu na dve písmená šifrovaného textu. Bola to vôbec prvá písmenková digrafická šifra (znakovú vynášiel Porta). [17]

- **rok 1863**

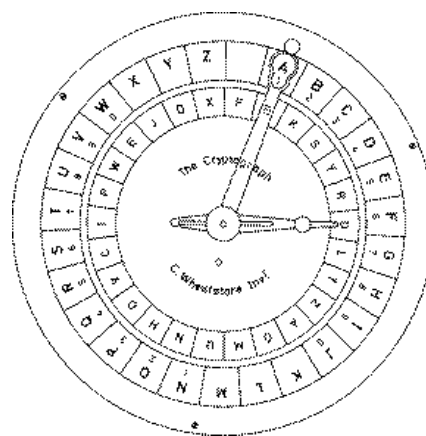
Dôstojník pruskej armády FRIEDRICH W. KASISKI uverejnil v knihe "Die Geheimschriften und die Dechiffirkunst" metódu na riešenie polyalfabetickej šifry prostredníctvom nájdenia jej periódy a následným zredukovaním na monoalfabetickú šifru. Tento objav znamenal obrat v kryptológii. Netrvalo dlho a kryptológovia vedeli, že ani polyalfabetická šifra s periodickým kľúčom nie je bezpečná, pokiaľ kľúč nie je zhruba taký dlhý ako samotná správa. [7]

- **rok 1867**

Nezávisle od Wadswortha (1817) vynášiel už spomínaný CHARLES WHEATSTONE zjednodušenú verziu šifrovacieho disku a predstavil ju na svetovej výstave v Paríži. Vonkajší kotúč mal iba 27 znakov. Princíp šifrovania bol rovnaký ako u Wadswortha, avšak bol použitý na ručičky narozdiel od okienok na kotúčoch. [17]

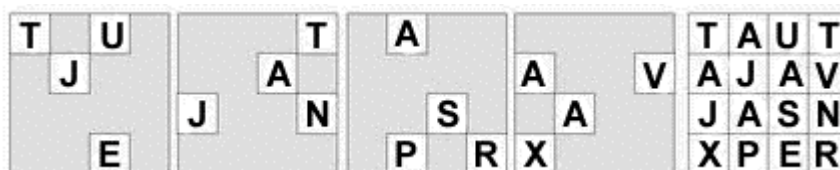
- **rok 1881**

Fleissnerova *otočná mriežka*, ktorú popísal ako prvý FLEISSNER VON WOSTROWITZ, je po spartánskom drevenom valci druhou známou mechanickou pomôckou realizujúcou transpozíciu. Princíp mriežky bol jednoduchý. V štvorci  $n \times n$  políčok je vystrihnutých  $n \times n/4$  políčok tak, aby pri postupnom otáčaní o 90 stupňov vzniknuté otvory ukazovali vždy na iné políčka. Takúto mriežka bola položená na papier a do jej okienok bol vpisovaný otvorený text.



Obr. 2.11 Wheatstonov šifrovací disk [6]

Po vyplnení všetkých okienok sa mriežka otočila o 90 stupňov. Nakoniec na papieri vznikol štvorec súvislo vyplnený písmenami. Šifrovaný text sa z neho vypisuje po riadkoch. Šifru použil Jules Verne v knihe "Nový Gróf Monte Christo", ale aj nemecká armáda, ktorá ju jeden čas používala v prvej svetovej vojne ako poľnú šifru. [17]



Obr. 2.12 Fleissnerova otočná mriežka OT: Tu je tajná správa x, ŠT: TAUTAJAVJASNXP

- **rok 1883**

AUGUSTE KERCKHOFFS vydal knihu "La Cryptographie Militaire". Kerckhoffs našiel metódu, ako rozlúštiť všeobecnú polyalfabetickú šifru s neperiodickým kľúčom, ak tento bol použitý niekoľkokrát. Portova kniha, ktorá bola po celých 300 rokov favoritom v kryptologickej literatúre, bola nahradená práve touto knihou. V praxi sa prestávajú používať nomenklátory. Široké uplatnenie, predovšetkým vďaka vynálezu telegrafu, nachádza Vigenèrova šifra. [7, 17]

- **roky 1914-1918**

Prvá svetová vojna znamenala značný rozmach v používaní známych šifier.

- **rok 1917**

WILLIAM FREDERICK FRIEDMAN, neskôr označovaný ako otec americkej kryptoanalýzy, bol zamestnaný ako kryptoanalytik v Rivenbank Laboratories a vykonával kryptoanalýzu a školenia pre americkú vládu [18]

- **rok 1917**

GILBERT S. VERNAM, zamestnanec americkej AT&T, vymyslel polyalfabetický šifrovací stroj schopný používať náhodný neopakujúci sa kód. Tento systém je dodnes známy ako jediný teoreticky *bezpečný kryptosystém*. Do stroja sa vkladala dierna páska s otvoreným textom spolu s diernou páskou, na ktorej bol náhodne vydierkovaný kľúč. Šifrogram vznikol sčítaním príslušných bitov oboch pásek modulo 2. Veľkou výhodou stroja bolo, že proces šifrovania aj dešifrovania prebiehal úplne rovnako. Tento systém ostáva bezpečným, ak náhodný kľúč je rovnako dlhý ako šifrovaná správa a používa sa iba raz (One Time Pad). [18]

- **rok 1918**

USA použilo osem amerických indiánov kmeňa Choctaw na posielanie súrnych správ nešifrovaným kanálom v ich rodnom jazyku.

- **rok 1918**

Pred koncom prvej svetovej vojny začali Nemci používať ADFGVX systém. Bola to šifra, ktorá vykonávala substitúciu aj transpozíciu. Rozlúštil ju francúzsky kryptoanalytik LIEUTENANT GEORGES PAINVIN.

- **rok 1919**

HUGO ALEXANDER KOCH zapísal svoj patent šifrovacieho stroja založeného na *rotoroch*. O štyri roky neskôr predal patent Arthurovi Scherbiusovi, nemeckému inžinierovi, ktorý ho vylepšil a nazval Enigma.

- **rok 1923**

Najznámejšia z elektromechanických rotorových strojov je nemecká *Enigma*. Je založená na vynálezoch Hugo Kocha a Arthura Scherbiusa a má mnoho variant. Vo variante A bola predstavená už v r. 1923 ako komerčné zariadenie na medzinárodnom poštovom kongrese v Berne. Počas 2. svetovej vojny bola používaná v rôznych variáciách predovšetkým nemeckou armádou. [19]

- **roky 1927-1933**

Prohibícia vyvolala počiatok tzv. *kriminálnej kryptológie*. V týchto rokoch FBI zakladá kryptografické oddelenie venované zločineckej kryptológii. Aj v súčasnosti sa kryptológia zneužíva aj na ilegálne účely.

- **rok 1929**

Najznámejšie použitie algebry v kryptológii pochádza od LESTER S. HILLA. V roku 1929 totiž navrhol polygramovu šifru, v ktorej  $n$ -gram otvoreného textu (napr.  $n$ -tica písmen) je prevedená na  $n$ -gram šifrovaného textu. Písmená sú očíslované od 0 po 25 a  $n$ -gram je číselný vektor. Kľúčom je invertibilná matica  $A$  o rozmeroch  $n \times n$  a šifrovanie prebieha podľa vzťahu  $ŠT = A * OT$ . [18]

- **roky 1933-45**

Šifrovací stroj Enigma nemal komerčný úspech, ale bol odkúpený, vylepšený a používaný nacistickým Nemeckom. Spôsob jeho šifrovania bol rozlúštený Marianom Rejewskim, Alanom Turingom a Gordonom Welchmanom.

- **rok 1937**

Japonská vláda začala používať šifrovací stroj *PURPLE*. Jeho šifra bola rozlúštená americkým tímom na čele s Williamom F. Friedmanom. Princíp Purple bol odlišný od nemeckej Enigmy, nebol založený na rotoroch, ale využíval telefonické súčiastky. [19]

- **roky 1945-1970**

Po druhej svetovej vojne nastáva obdobie, kedy vznikajú desiatky najrôznejších mechanických a neskôr elektromechanických šifrovacích strojov. Tie sa používajú až do 70. rokov (niektoré aj dlhšie). [18]



Obr. 2.13 Nemecký šifrovací stroj Enigma [20]

## 2.3 Éra počítačov

- rok 1970

HORST FEISTEL viedol výskumný projekt v IBM Watson Research Lab, ktorý počas šesťdesiatych rokov vyvíjal šifru LUCIFER. Táto šifra neskôr inšpirovala americký štandard DES a ďalšie šifry označované ako šifry *Feistelovského typu*.

- rok 1976

Návrh firmy IBM, založený na šifre Lucifer a upravený (zmenené S-boxy a zredukovaná dĺžka kľúča) americkou bezpečnostnou agentúrou NSA, bol prijatý ako americký národný štandard U.S. Data Encryption Standard, skrátene *DES*. Algoritmus si získal celosvetové uplatnenie až do konca 90. rokov. [21]

## 2.4 Od asymetrickej kryptografie až podnes

- rok 1976

WHITFIELD DIFFIE a MARTIN HELLMAN publikujú "New Directions in Cryptography", zahŕňajúcu myšlienku kryptosystému verejného kľúča (nazývanou aj *asymetrická kryptografia*). Toto dielo znamenalo revolúciu v kryptografii. Prínosom bola myšlienka, že kľúče môžu existovať v pároch – jeden šifrovací a jeden dešifrovací kľúč – a že nie je možné jeden kľúč odvodiť z druhého. [22]

- rok 1977

Inšpirovaní Diffie-Hellmanovou štúdiou oznámili RONALD L. RIVEST, ADI SHAMIR a LEONARD M. ADLEMAN (z počítačového laboratória Massachusetts Institute of Technology) objav prvého konkrétného kryptosystému s verejným kľúčom. Bol pomenovaný *RSA* podľa počiatkových písmen autorov. Systém je založený na probléme faktorizácie veľkých čísel a dodnes je neoficiálnym svetovým priemyselným štandardom. [23]

- rok 1990

XUEJIA LAI a JAMES MASSEY zo Švajčiarska vydali článok "A Proposal for a New Block Encryption Standard", ktorý obsahoval návrh šifrovacieho algoritmu – International Data Encryption Algorithm (IDEA) a mal nahradiť DES. Algoritmus používa 128-bitový kľúč a využíva operácie, ktoré podporujú architektúru počítača, a preto je jeho softvérová implementácia efektívnejšia.

- rok 1990

CHARLES H. BENNETT, GILLES BRASSARD A KOL. publikovali ich experimentálny výsledok z *kvantovej kryptografie*, ktorá využíva fotóny na prenos bitov kľúča Vermanovho šifrovania. Zo zákonitostí kvantovej mechaniky vyplýva, že kvantová kryptológia umožňuje nielen bezpečný prenos dát, ale aj indikuje pasívne monitorovanie správ. Ak niekto monitoruje viac bitov ako je dovolené, komunikáciu nutne preruší.

- rok 1991

PHIL ZIMMERMANN zverejnil jeho prvú verziu *PGP* (Pretty Good Privacy). PGP je šifrovací program, ktorým sa dá zabezpečiť bezpečný prenos e-pošty, ale taktiež telefonovanie cez Internet. Využíva algoritmy RSA a IDEA. Aj v súčasnosti tento program na Internetu používa

značné množstvo používateľov, čo je umocnené skutočnosťou, že pre súkromné účely je zadarmo. [24]

- **rok 1994**

Bolo roznásobené 129-ciferné číslo RSA-129. Podľa profesora Rivesta, jedného z tvorcov RSA, mala táto činnosť trvať  $4.10^{16}$  rokov. Proces faktorizácie prebiehal za pomoci *Internetu*. Do experimentu bolo zapojených 600 ľudí z 20 zemí zo všetkých kontinentov. Podstata experimentu spočívala v tom, že každý počítač zapojený do experimentu vykonával oddelené výpočty, a potom ich výsledky zasielal na súborový server umiestnený na MIT. Zber dát pre finálny výpočet trval osem mesiacov. Fenomén *Internetu* bol po prvý krát využitý na kryptoanalýzu (na útok hrubou silou). [25]

- **rok 1997**

Bol rozlúštený 56-bitový kľúč k DES pomocou *Internetu*, podobne ako v roku 1994 u RSA. [26]

- **rok 2000**

Šifrovací štandard DES bol, po takmer štvorročnej verejnej súťaži, nahradený belgickou šifrou *Rijndael*. Blokovoú šifru Rijndael prihlásili do súťaže známi kryptológovia JOAN DAEMEN a VINCENT RIJMEN. Hoci ich šifra podporuje aj väčšie bloky pre AES (Advanced Encryption Standard) je dĺžka vstupného a výstupného bloku definovaná ako 128 bitov. Dĺžka kľúča je voliteľná 128, 192 a 256 bitov. Šifra sa stane na najbližších 20 až 30 rokov najpoužívanejšou šifrou na svete. [27, 28]

## 2.5 Zhrnutie

Pre ontogenézu z fylogenetického rozboru kryptografie je dôležitá myšlienka štyroch etáp, v ktorých sa disciplína vyvíjala. *Prvá etapa, raná*, využíva predovšetkým manipuláciu s metódami substitúcie a transpozície na intuitívnej úrovni. *Druhá etapa, mechanické a elektronické šifrovacie stroje*, využíva zákonitosti kryptografie v mechanických strojoch, objavujú sa prvé matematické popisy. *Tretia etapa, éra počítačov*, priniesla hlavne šifry Feistelovského typu. *Štvrtá etapa, od asymetrickej kryptografie až podnes*, priniesla prevratný objav asymetrickej kryptológie, využívajúci princípy teórie čísel.

Z metodického hľadiska je dôležitý najmä prechod medzi prvou a druhou etapou, teda uvedomenie si určitých zákonitostí a princípov šifrovania a prechod od intuitívneho používania substitúcie a transpozície k matematickému pozadiu kryptografie.



## Kapitola 3

### Ontogenéza kryptografie

Vyučovanie kryptografie ako oblasti, s ktorou sa navonok nestretávame v bežnom živote, zvädza preferovať demonštratívny prístup ako prístup objavovaním. Jednotlivé pojmy učiteľ predkladá, definuje, ilustruje. Od študentov sa očakáva viac-menej pasívne akceptovanie a reprodukovanie. Pritom práve problematika substitučných a transpozičných šifrier je veľmi vhodná na samostatnú a tvorivú prácu.

#### 3.1 Kryptografia na základnej škole

Na základnej škole pri narábaní s kryptografiou úplne vystačíme iba s papierom a perom, tak ako to bolo aj v počiatočkoch tohto odvetvia.

##### 3.1.1 Motivácia

Ako motiváciu použijeme aktivitu Špióni, ktorú podrobne aj s hracími plánmi opisujeme v [29]. Aktivita využíva posielanie správ prostredníctvom elektronickej pošty a žiaci navzájom komunikujú iba týmto spôsobom.

Postup pri aktivite: Žiakov rozdelíme do troch až štyroch skupín po štyroch, bez toho, aby navzájom poznali svoje priradenie.

Porozprávame im motivačný príbeh:

“Každý z vás je špiónom nejakej veľmoci, snažia sa získať utajenú správu. Ste po štyroch v skupine patriacej k tej istej veľmoci, ale nepoznáte sa navzájom. Správa sa skladá zo 4 viet, pričom každý zo skupiny má rozdielnú vetu. Všetky tri skupiny majú rovnakú správu!

Úlohou každej skupiny je získať celú správu a vyriešiť jej obsah. Aby nepriatelia nezistili obsah vašej správy, treba ju šifrovať. Každá skupina má vlastný spôsob šifrovania, ktorému rozumejú iba členovia tej skupiny. Pozor, môže sa stať, že ak vašu správu dostane nepriateľ, je schopný ju po čase rozlúštiť.

Možný spôsob šifrovania, napr. pre skupinu Rýchla rota:

OTALZDANEOS

SOENADZLATO

Tu šifrovanie spočíva v napísaní písmen v opačnom poradí. Šifry skupín nie sú až také ťažké, dá sa prísť na každú z nich. Hráme na dve víťazné kolá, t.j. ktorá skupina bude mať ako prvá celú správu a ktorá skupina ako prvá vylúšti jej obsah.”

Odporúčime žiakom, aby sa v prípade, že im dlho nik neodpovedá, snažili rozlúštiť súperovu šifru (Príloha I.).

### 3.1.2 Vlastné šifry

Žiaci dostanú zoznam zašifrovaných viet. Ich úlohou je rozšifrovať utajený text a popísať spôsob šifrovania a dešifrovania. Úlohu majú uľahčenú tým, že text je písaný s diakritikou a každý obsahuje jedno slovenské príslovie.

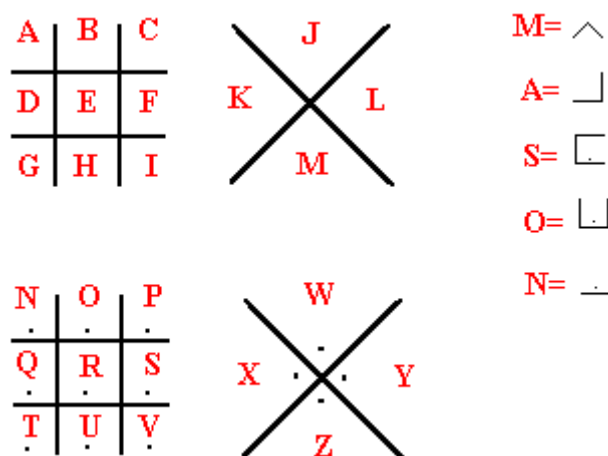
Šifrovaný text:

1. ÍBORENOTELAKČIVOTSALANDEJ
2. JUKOJUMUJUSAJUNEJULEJUNÍJUTOJUMUJUSAJUZEJULEJUNÍJU
3. KRMPMED  
TUUEDJÁ  
OHJKSOP  
DÉAOÁNA
4. MA PO ĎA LY ZÁJ LEJ DEŠ
5. AGO ZI UZDELIEŽ, DAG PUDEŽ ZBAĎ
6. KIŠTDŤOÍAHŽSLERAFJDMOÁZUNINÁLTJSEDHVEGJ
7. AÁAK,TKKTA  
KMTA AÁAK  
AÝTCTKSN  
KOE,AÝY.
8. KEĎ JE ŠŤASTIE UNAVENÉ, SADNE AJ NA VOLA.

Vo vetách 1, 3, 4 a 7 bola použitá metóda transpozície, vo vetách 2 a 6 boli použité klamače a vo vete 5 jednoduchá substitúcia foneticky znejúcich hlások.

Ďalej výučbový proces nasleduje metódou *brainstormingu* [30]. Poslednú vetu dostanú žiaci, aby ju zašifrovali vlastným spôsobom. Je potrebné klásť dôraz na spätné rozšifrovanie textu. Žiaci svoje výsledky ihneď prezentujú na tabuli.

Ďalšou etapou je oboznámenie žiakov z dvoma substitučnými šiframi. Caesarovou a Freemasonovou šifrou. Prvú sme podrobne opísali v kapitole 2.1. Druhá bola využívaná počas Americkej občianskej vojny a má nasledovný tvar:



Obr. 3.1 Freemasonova šifra. Uvedené sú aj šifrované tvary písmen M, A, S, O a N.[31]

Opäť ponecháme čas na nápady žiakov.

Na záver aktivity vyberieme dve najlepšie šifry. Kritériami sú schopnosť jednoznačného dešifrovania, obtiažnosť dešifrovania, rýchlosť šifrovania a dešifrovania správy, množstvo požadovaných tabuliek.

Uvádzame niekoľko ďalších zaujímavých metód transpozície a substitúcie, viac ich je možné nájsť v [32], príp. v [33]:

#### Písanie do niekoľkých riadkov po písmenách sprava zhora:

1234567890AB

B 9 8 5 4 1  
A 0 7 6 3 2

#### Zápis zhora nadol do dvoch riadkov:

1234567890

0 8 6 4 2  
9 7 5 3 1

#### Zápis do štvorcovej špirály

1234567890ABCDEFGHIJ

G F E D C  
H 5 4 3 B  
I 6 1 2 A  
J 7 8 9 0

#### Zápis raz spredu raz zozadu

1234567890

1357908642

#### Polybiov štvorec:

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

POLYBIUS

3534315412244543

#### Veľký poľský kľúč

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

° = M

Na mnohé z uvedených spôsobov šifrovania textu prídu žiaci samostatne.

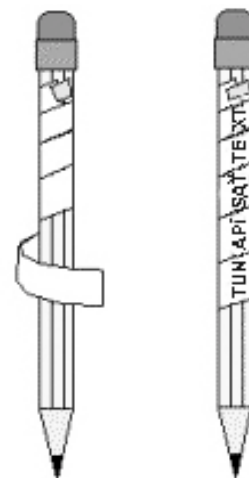
### 3.1.3 Mechanické šifrovacie pomôcky

V nasledujúcich aktivitách sme sa zamerali na predvedenie niektorých mechanických pomôcok na šifrovanie. Budeme k nim potrebovať papier, nožnice a lepiacu pásku.

#### Skytalé

Žiakov požiadame, aby si na hodinu doniesli dve rovnaké ceruzky, príp. dve rovnaké perá, rúrky, alebo malé valčeky. Z papiera vystrihneme tenký prúžok, ktorý obmotáme okolo ceruzky. Koniec papiera zalepíme lepiacou páskou.

Na papier po celom obvode ceruzky napíšeme text, ktorý má byť zašifrovaný. Text by mal byť dostatočne dlhý, aby dôsledok použitej transpozície bol očividný. Príklad textu "PRIKAZUJEM OMILOSTIT NIE POPRAVIT CISAR". Po rozvinutí prúžku papiera získame zašifrovanú správu, ktorá vznikla transpozíciou otvoreného textu. Otvorený text získame opätovným namotaním papiera na rovnakú ceruzku. Je vhodné predviesť prípad, keď je papier namotaný na ceruzku, príp. valec, s väčším (iným) polomerom a tým demonštrovať neschopnosť odhalenia správy takýmto spôsobom.

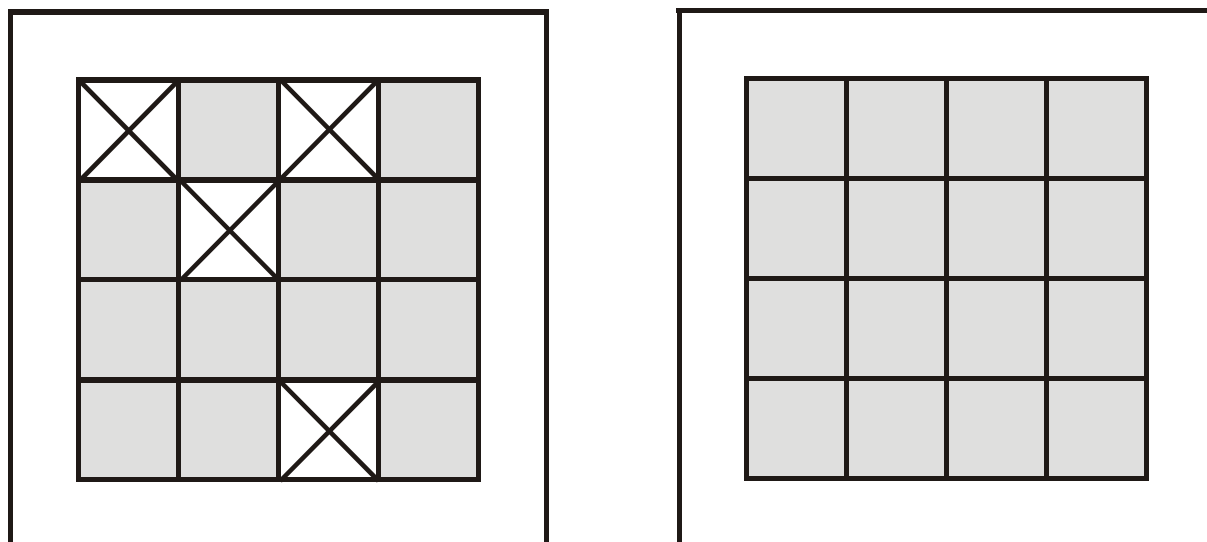


Obr. 3.2 Spôsob šifrovania metódou skytalé

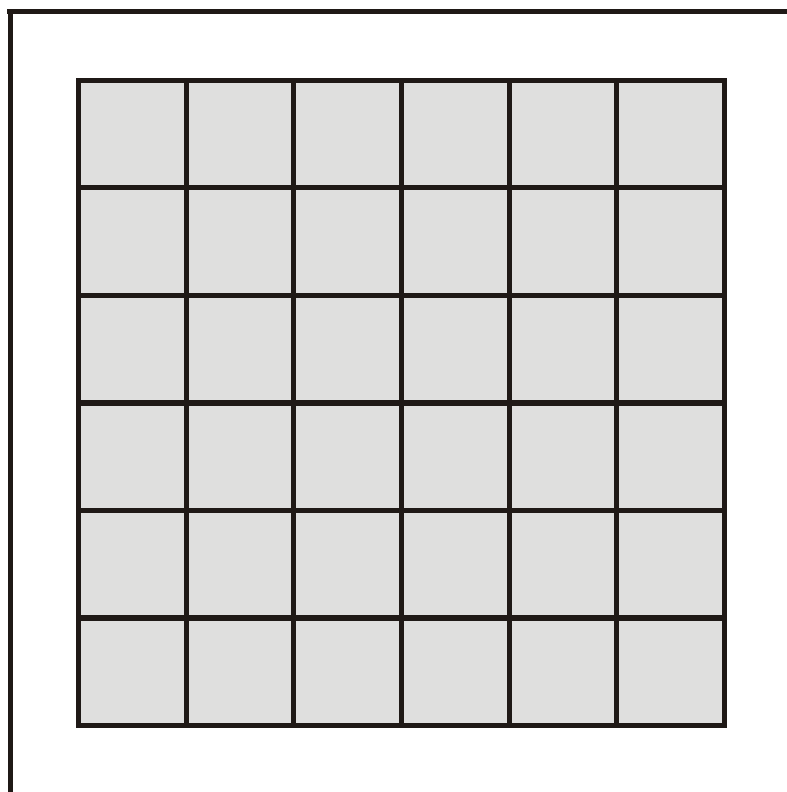
#### Fleissnerova otočná mriežka

Princíp Fleissnerovej otočnej mriežky sme popísali v kapitole 2.1. Jej opis uvádza aj kapitola 3.2.1 v zadaní úlohy.

Žiakom dáme mriežku z obrázku 3.3.a) so štyrmi vystrihnutými otvormi a necháme ich zašifrovať text, napr. vlastné meno, priezvisko a mesto narodenia. Ďalej im dáme mriežku z obrázku 3.3.b) a vyzveme ich, aby našli ďalšie možné štvorice otvorov v mriežke a aj zdôvodnili ich správnosť.



Obr. 3.3 Fleissnerova otočná mriežka a) s vyznačenými otvormi b) s nevyznačenými otvormi



Obr. 3.4 Fleissnerova otočná mriežka s nevyznačenými otvorami rozmerov 6x6

Nakoniec im dáme mriežku z obrázku 3.4, aby postup aplikovali aj na mriežku s väčším počtom otvorov. V našom prípade je počet požadovaných otvorov deväť.

## Šifrovací disk

– *monoalfabetická (jednoduchá) substitučná šifra*

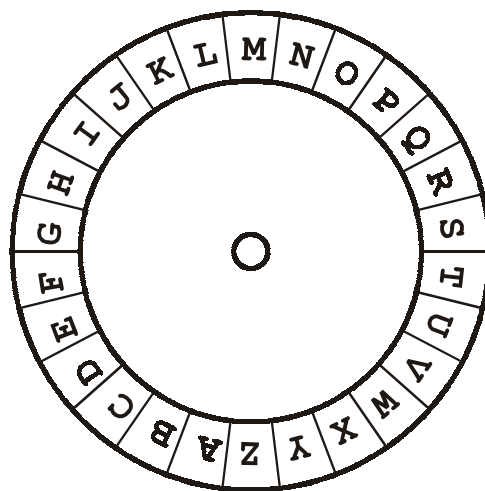
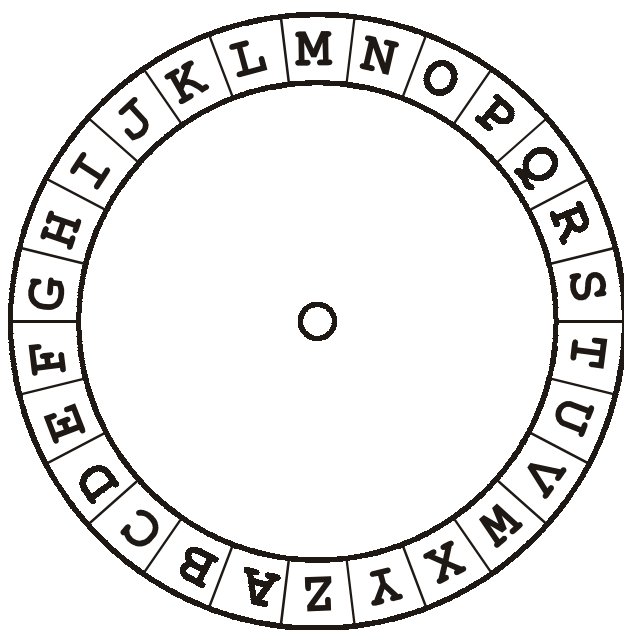
Najznámejšou monoalfabetickou šifrou je Caesarova šifra, ktorú sme so žiakmi robili už v aktivite vlastné šifry. Prechod z konca abecedy na začiatok tam bol vysvetlený tak, že po písmene Z znovu nasleduje písmeno A, atď. Teraz tento prechod objasníme aj po vizuálnej stránke. Žiakom dáme vystrihnúť a spojiť prvé dva kruhy z obrázku 3.5.a) a 3.5.b). Kruhy je možné spojiť napr. patentkou, alebo ich jednoducho v strede napichnúť na ceruzku.

Pootočením vnútorného kruhu o 3 políčka je možné vizuálne demonštrovať Caesarovú šifru.

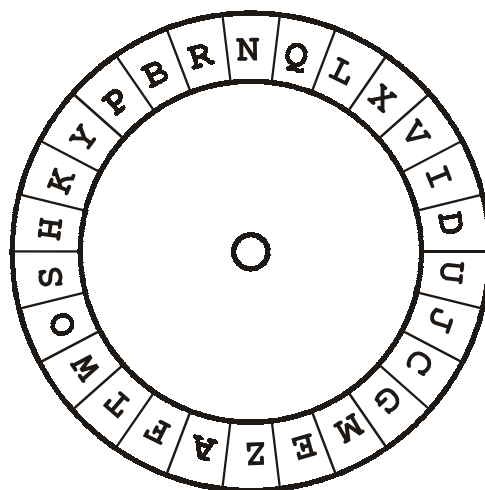
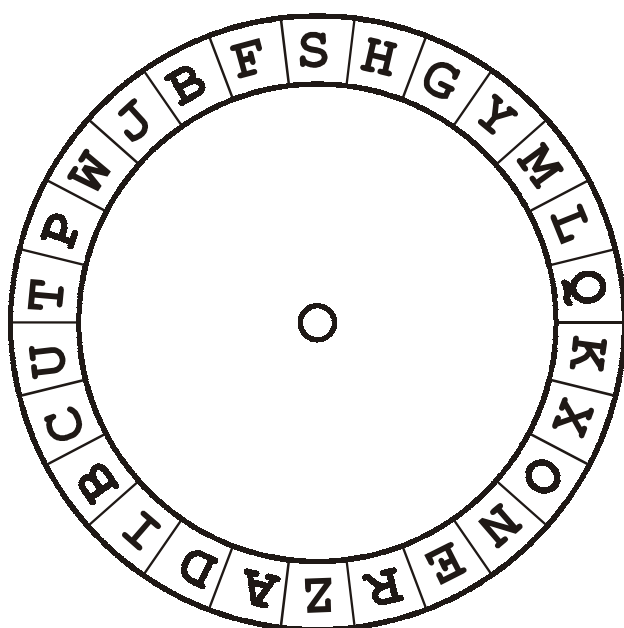
Navyše je možné posun tejto jednoduchej substitučnej šifry meniť. Napr. ak posun je len o jedno políčko získame šifru, ktorú používal Caesarov nasledovník Augustus, t.j. každé písmeno je nahradené písmenom bezprostredne za ním idúcim v abecede [7]. Ak je posun o 26 políčok, jedná sa o identitu. Na tento fakt je žiakov vhodné upozorniť.

Vďaka tejto pomôcke je proces šifrovania, ale hlavne dešifrovania oveľa rýchlejší a názornejší.

Šifrovací kruh nemusí vždy obsahovať štandardú abecedu, abeceda môže byť poprehadzovaná ako je to vidieť na šifrovacích kruhoch 3.6.a) a 3.6.b). Prvé a druhé šifrovacie disky môžeme navzájom kombinovať.



Obr. 3.5 Šifrovací disk substituční šifry a) vonkajší kruh b) vnitřní kruh



Obr. 3.6 Šifrovací disk substituční šifry s přeházanou abecedou a) vonkajší kruh b) vnitřní kruh

– polyalfabetická substitučná šifra

Najznámejšou polyalfabetickou šifrou je Vigenerova šifra. Na substitúciu využíva kľúč a 26 abecied. Abecedy sú uvedené vo Vigenerovej tabuľke na obrázku 3.7.

Vigenerovú tabuľku získame, ak necháme žiakov pod seba vypísať všetky možné posunutia Caesarovej šifry. Využitie tabuľky navedieme otázkou, ako by sme postupovali, keby sme chceli každé písmeno textu šifrovať iným posunutím (inou abecedou). Jednou z možných odpovedí je šifrovať text postupne po abecedách, ale toto riešenie je pre nepovolené dešifrovanie príliš jednoduché. Ak chceme používať abecedy prehádzané, vznikne potreba zapamätať si poradie jednotlivých abecied a teda využívať kľúč.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Obr. 3.7 Vigenerova tabuľka

Postup šifrovania je nasledovný: Otvorený text podpisujeme heslom až do konca textu. V stĺpci Vigenerovej tabuľky nájdeme písmeno otvoreného textu, v riadku písmeno hesla. V priesečníku riadku a stĺpca nájdeme zašifrovaný znak správy.

Napr. OT: TOTOJESIFRA

Heslo: KLUCKLUCKLU

ŠT: DZNQTPMKPCU

Každý žiak si zašifruje svoje meno so zvoleným heslom. Ďalej ich vyzveme, aby sa pokúsili nájsť tento systém na šifrovacom disku. Je nasledovný: Na spodnom disku si nastavíme prvé písmeno kľúča (K) pod písmeno A. Zobrazenie písmena A na prvé písmeno kľúča zabezpečí, že sa celá abeceda zobrazí na posunutú abecedu začínajúcu prvým písmenom kľúča. Zašifrovaný znak (D) nájdeme na vnútornom kotúči pod písmeno otvoreného textu (T). Postup zopakujeme pre všetky písmená.

V našom príklade sme na šifrovanie použili štyri posunuté abecedy:

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

### 3.1.4 Autokľúč

Autokľúč je špeciálny druh substitučnej šifry, kde nový šifrovaný znak je závislý od predchádzajúceho znaku.

Aby mohli žiaci narábať s týmto šifrovacím systémom, musia najprv zvládnuť "sčítavanie" písmen, t. j. prepis písmen na čísla a ich sčítanie v modulárnej aritmetike modulo 26. K intuitívnemu narábaniu s týmito operáciami využijeme tabuľky uvedené na obrázku 3.8, kde sú uvedené číselné hodnoty písmen.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

Obr. 3.8 Prevod písmen na čísla a naopak

Po rozdání tabuliek zadáme žiakom, aby vyriešili nasledovné rovnice:

$A+B=$   
 $J+E=$   
 $K+P=$   
 $K+Q=$   
 $J+X=$   
 $Z+Z=$

Žiaci by mali sami prísť na to, že ak je číslo väčšie ako 25, treba od neho odrátať hodnotu 26 a dostaneme opäť číslo písmena abecedy. Pri odčítavaní treba hodnotu 26 pričítať.

Po tomto úvode je možné začať so simuláciou autokľúča. Ako heslo nám stačí jedno písmeno abecedy, ktoré sa sčíta s prvým písmenom otvoreného textu. Ďalej sa sčítavajú buď znaky otvoreného, alebo šifrovaného textu.

Napr. pri sčítavaní znakov šifrovaného textu, kľúčom je písmeno C

OT: TAJNASPRAVA

kľúč: CVVERRJYPPK

ŠT: VVERRJYPPKK

Napr. pri sčítavaní znakov otvoreného textu, kľúčom je písmeno C

OT: TAJNASPRAVA

kľúč: CTAJNASPRAV

ŠT: VTJWNSHGRVV

Po predvedení prvého spôsobu šifrovania a po zašifrovaní svojho mena žiakmi, vyzveme žiakov, aby druhý spôsob, t. j. čo by sa dalo ešte použiť ako kľúč, objavili sami. Takisto, aby prišli na spôsob dešifrovania správy.



Vhodné je na konkrétnych príkladoch predviesť, že ak nastane zmena v jednom písmene otvoreného textu napr. v Caesarovej šifre, zmení sa iba jedno písmeno v šifrovanom texte. V šifrovaní autokľúčom však nastane zmena textu od pozície zmeneného písmena, až do konca textu.

Napr. pri Caesarovej šifre pri zmene písmena B na A

OT: PLAN**B**NEPOUZIT

OT: PLAN**A**NEPOUZIT

ŠT: SODQ**E**QHSRXCLW

ŠT: SODQ**D**QHSRXCLW

pri použití autokľúča (sčítavanie znakov šifrovaného textu) pri zmene písmena B na A

OT: PLAN**B**NEPOUZIT

OT: PLAN**A**NEPOUZIT

kl'úč: DSDDQREIXLFEM

kl'úč: DSDDQQDHWKEDL

ŠT: SDDQ**R**EIXL**F**E**M**F

ŠT: SDDQ**Q**DHWKED**L**E

### 3.2 Štúdium kryptografie na strednej škole

Štúdium kryptografie na strednej škole sme prepojili s programovaním. Zastávame totiž názor, že ak študent zvládne samostatne naprogramovať šifrovací algoritmus, pochopí aj jeho činnosť. Taktiež z pohľadu stredoškolského študenta, je prepojenie tejto oblasti s počítačom a následné využívanie napríklad v elektronickej pošte, oveľa atraktívnejšie ako preberanie týchto systémov iba na papieri. Pochopiteľne pred tým, ako začneme so študentami šifru programovať, podrobne ju vysvetlíme a uvedieme konkrétny príklad, ktorý bude slúžiť študentom ako kontrola správnosti ich programu.

Samozrejme aj na strednej škole je možné začať vyučovanie s úlohami uvedenými v predošlej kapitole. V týchto prípadoch je vhodné k opisu jednotlivých algoritmov písať aj matematický zápis.

V použitých príkladoch uvádzame relevantnú časť programového kódu napísaného v prostredí Delphi. Ak nie je uvedené inak, programy využívajú premenné `otvtext`, `siftext`, `kluc` typu `string`, `otvzn`, `sifzn`, `kluczn` typu `char` a `i` typu `integer`.

#### 3.2.1 Caesarova šifra

Pri Ceasarovej šifre, kde je písmeno otvoreného textu  $p_i$  posunuté o hodnotu 3 v abecede na písmeno  $c_i$ , je vzorec šifrovania znaku nasledovný:  $c_i = E(p_i) = p_i + 3$ .

Programový kód je jednoduchý, stačí k ordinálnej hodnote každého znaku otvoreného textu prirábať hodnotu tri.

```
posun:=3;
for i:=1 to Length(otvtext)do
begin
    otvzn:=otvtext[i];
    sifzn:=chr((ord(otvzn)-65+posun) mod 26 +65);
    siftext:=siftext+sifzn;
end;
```

Pred samotným programovaním by sme mali študentom objasniť princíp modulárnej aritmetiky. Úplne však vystačíme s pojmom zvyšku po celočíselnom delení.

### 3.2.2 Bigramová šifra

Základom šifry je tabuľka, ktorej riadky a stĺpce sú označené písmenami abecedy. Šifrovanie spočíva v nahradení dvoch znakov otvoreného textu inými dvoma znakmi. Prvé písmeno otvoreného textu určuje riadok tabuľky, druhé stĺpec tabuľky. Na ich priesečníku sa nachádza príslušná dvojica znakov šifrovaného textu.

Študentom dáme vopred časť kódu obsahujúci tabuľku, čím sa vyhneme pracnému prepisovaniu údajov.

```
const tab:array['A'..'Z','A'..'Z'] of str2=
  (( 'QP','WB','EA','RV','TQ','YV','UC','IW','OT','PH','AO','SD','DN','FD',
    'GX','HR','JY','KC','LO','ZQ','XG','CH','VG','BF','NF','MM'),
    ('ZA','AN','QZ','XF','SG','WS','CR','DW','EQ','VC','FY','RU','BG','GN',
    'TW','NY','HL','YK','MG','JZ','UK','KJ','IA','LH','OO','PD'),
    ('PG','OK','IR','UH','YX','TI','RY','EL','WR','QK','LZ','KK','JS','HF',
    'GE','FA','DL','SE','AQ','MW','NP','BN','VW','CD','XT','ZP'),
    ('PK','LJ','OA','KH','MV','IS','JR','NQ','UM','HM','BM','YG','GR','VL',
    'TV','FP','CB','RE','DJ','XP','EE','SL','ZC','WU','AS','QJ'),
    ('TB','FG','BY','NU','JN','WF','SU','KW','MP','OJ','PF','QR','AW','IP',
    'VF','LN','UJ','DB','HP','YA','GG','CT','RB','EU','XX','ZU'),
    ('GO','ID','VE','KZ','PM','ZO','DC','YF','TO','FJ','NH','EO','CV','OC',
    'WX','QT','RF','XA','HX','LY','AC','JM','MH','SO','UG','BR'),
    ('ZZ','OF','BX','WH','KS','FZ','TD','NK','RQ','JV','HB','QU','IH','DA',
    'GP','LK','AK','MY','EB','XU','SH','YR','PR','UO','VU','CI'),
    ('ZG','BL','KT','YZ','AU','RI','ND','WD','PP','IF','OE','FI','JA','LC',
    'GQ','EW','DQ','QA','XM','MD','CS','TS','VQ','UN','SK','HY'),
    ('OX','PI','WK','DS','AE','YM','CL','BA','MR','RK','JB','FF','QO','GW',
    'XQ','ED','VJ','US','TC','KV','LD','SP','IM','ZM','NG','HH'),
    ('VD','KE','QV','IN','GV','CM','OL','MS','EK','SF','DP','TM','YP','FK',
    'BT','UF','JH','WI','AA','PA','LA','NC','XZ','RJ','HW','ZW'),
    ('DI','AV','FM','LS','YU','NA','KN','TH','ZK','JL','RN','EM','MK','OM',
    'WV','PU','CQ','QW','GU','VS','UZ','HN','XY','BV','SB','IG'),
    ('WQ','AX','JQ','SJ','PW','BC','EV','OH','IB','QI','VO','DX','HT','UU',
    'ZI','CY','TR','NN','LQ','KQ','RD','FB','GK','YB','MZ','XK'),
    ('QY','ZT','GF','EZ','KG','IO','PN','HO','UR','DF','OQ','NR','AR','TF',
    'WT','SS','BP','VI','RZ','LU','CF','FO','YW','MU','XL','JE'),
    ('MT','CP','PB','JW','KF','LG','ZF','RX','FU','TY','UY','NE','SR','GI',
    'HA','AB','XS','EY','IC','VH','DZ','YJ','BZ','QH','WA','OR'),
    ('OG','HD','IQ','ZV','FV','ER','NL','MQ','BW','PZ','RM','AJ','GC','YE',
    'LT','UX','VA','KO','XI','JX','WZ','DM','SC','CJ','TZ','QS'),
    ('UI','TP','MN','OU','WN','GA','ZD','EF','BE','SM','VX','AM','DO','IJ',
    'FT','NB','LX','QE','HE','PE','KB','JJ','XB','CG','YC','RO'),
    ('PL','SI','OP','YY','IY','VR','JC','ZL','DG','GH','KP','LL','BB','FL',
    'NZ','HS','WM','XN','QC','MJ','UA','CN','EC','RW','TJ','AF'),
    ('QX','TN','KM','GT','AD','FX','PQ','CW','WP','YH','ML','EG','RC','NJ',
    'JF','LE','HU','VZ','IL','ZR','DD','OZ','XC','BH','ST','UT'),
    ('ES','PJ','AI','TK','VB','RG','BI','NX','IK','SV','ZS','QM','FN','HI',
    'UV','JI','OB','WC','KL','ME','DK','YO','CU','XE','GY','LI'),
    ('GS','JT','XO','BS','LV','NM','YI','FE','MA','PY','WY','KI','HC','ZJ',
    'VV','EN','SW','AG','UP','RP','ON','CX','IX','DE','TA','QB'),
    ('RH','PS','WE','HJ','IZ','EI','GL','MB','JP','DR','AY','YD','LM','XW',
    'KX','TE','UB','QL','NS','SZ','ZB','FS','CZ','BK','OS','VY'),
    ('AP','OV','TL','LW','MX','WJ','QQ','XD','EP','PT','NO','IV','VK','CA',
    'ZX','BO','GJ','SA','DU','JU','UW','RA','FQ','YT','KA','HZ'),
    ('BD','VN','IT','CC','NT','FC','UD','QN','KD','YS','RL','TG','GZ','XV',
    'AH','LP','PX','HV','WL','EJ','DV','MC','ZH','SN','OI','JD'),
    ('HG','JO','WO','EX','MO','OY','IE','DT','GM','ZY','AT','LR','FR','TX',
    'YL','UQ','VP','XR','BJ','CK','SY','PV','KU','RT','QD','NV'),
    ('JG','GD','TT','YQ','UE','ZN','MF','QF','WW','SX','AL','OD','CE','FW',
    'BQ','IU','KR','EH','NW','LF','PC','RR','HK','DH','VT','XH'),
    ('YN','NI','JK','VM','II','WG','OW','CO','AZ','HQ','PO','ZE','RS','ET',
    'SQ','BU','QG','LB','UL','XJ','MI','FH','DY','KY','GB','TU'));
```

Pred samotným šifrovaním je potrebné zistiť, či otvorený text je párný, a ak nie je doplniť ho o ľubovoľný znak, napr. X.

```
if odd(Length(otvtext)) then ovtvtext:=otvtext+'X';
```

V procese šifrovania sa z tabuľky tab vyberie reťazec dĺžky dva a pridá sa k šifrovanému textu.

```
i:=1;
While i<Length(otvtext) do
begin
    siftext:=siftext+tab[otvtext[i],otvtext[i+1]];
    inc(i,2);
end;
```

### 3.2.3 Vigenerova šifra

Základom tejto šifry je Vigenerova tabuľka uvedená v kapitole 3.1.3.

Ak otvorený text pozostáva zo znakov

$$M_e = a_1, a_2, \dots, a_t, a_{t+1}, \dots, a_{2t}, \dots, a_n$$

šifrovaný text môžeme zapísať ako n-ticu monoalfabetických transformácií

$$M_e = f_1(a_1), f_2(a_2), \dots, f_t(a_t), f_{t+1}(a_{t+1}), \dots$$

Pri programovaní nemusíme využívať, a teda ani napĺňať, Vigenerovu tabuľku. Stačí zväčšiť ordinálnu hodnotu znaku otvoreného textu o ordinálnu hodnotu znaku kľúča, čím nájdeme príslušný znak ku znaku otvoreného textu v posunutej abecede.

```
for i:=1 to Length(otvtext)do
begin
    ovtzn:=otvtext[i];
    kluczn:=kluc[i];
    sifzn:=chr((ord(otvzn)-65+ord(kluczn)-65) mod 26 +65);
    siftext:=siftext+sifzn;
end;
```

Najskôr však musíme upraviť dĺžku kľúča na dĺžku otvoreného textu.

```
klucpom:=kluc;
while Length(kluc)<Length(otvtext) do
    kluc:=kluc+klucpom;
```

### 3.2.4 Autokľúč

Spôsob a príklady šifrovania s autokľúčom sme uviedli v kapitole 3.1.4. Rovnice v zápise modulárnej aritmetike by mali vyzeráť nasledovne:

$$\begin{aligned} A+B \bmod 26 &= B \\ J+E \bmod 26 &= N \\ K+P \bmod 26 &= Z \\ K+Q \bmod 26 &= A \\ J+X \bmod 26 &= G \\ Z+Z \bmod 26 &= Y \end{aligned}$$

Pri programovaní môžeme v jednom cykle naraz vytvárať obidve varianty šifrovania autokľúčom, v hesle sa sčítavajú buď znaky otvoreného, alebo šifrovaného textu.

```

for i:=1 to Length(otvtext)do
begin
  {Prvý variant: pričítanie šifrovaného textu}
  otvzn:=otvtext[i];
  sifzn:=chr((ord(otvzn)-65+ord(kluczn1)-65) mod 26 +65);
  kluczn1:=sifzn;
  siftext1:=siftext1+sifzn;

  {Druhý variant: pričítanie otvoreného textu}
  sifzn:=chr((ord(otvzn)-65+ord(kluczn2)-65) mod 26 +65);
  kluczn2:=otvzn;
  siftext2:=siftext2+sifzn;
end;

```

### 3.2.5 Fleissnerova otočná mriežka

Zadanie tejto úlohy sme si prepožičali z Matematickej olympiády kategória Programovanie, čo len upevňuje fakt, že na strednej škole je adekvátne prepojiť kryptografiu s programovaním.

#### P-I-1- MOP-48. ročník, 1998/99

Jednou z metód šifrovania správ je použitie šifrovacej mriežky. Šifrovacia mriežka je štvorec rozdelený na  $2N \times 2N$  štvorcových políčok, pričom dohodnutých  $N^2$  políčok je vyrezaných. Mriežka sa položí na štvorcovú tabuľku rovnakých rozmerov ( $2N \times 2N$  políčok) a do každého výrezu vpíšeme jeden znak správy, pričom postupujeme po riadkoch zhora nadol a v každom riadku zľava doprava. Tento postup ešte trikrát zopakujeme s mriežkou otočenou o  $90^\circ$ ,  $180^\circ$  a  $270^\circ$  stupňov v smere hodinových ručičiek. Zašifrovaná sprava sa získa prečítaním tabuľky po riadkoch. Aby sa daná mriežka dala použiť na šifrovanie, každá pozícia v tabuľke musí byť odkrytá popísaným spôsobom práve raz.

Napište program, ktorý čo najrýchlejšie zisti, či sa dá daná mriežka použiť ako šifrovacia mriežka. Vstupný súbor *MRIEZKA.IN* obsahuje  $2N+1$  riadkov. Na prvom riadku je celé kladné číslo  $N$ , ( $N \leq 100$ ). Každý z nasledujúcich  $2N$  riadkov obsahuje presne  $2N$  znakov  $0$  (nie je výrez) alebo  $1$  (je výrez) oddelených jednou medzerou. Výstupný súbor *MRIEZKA.OUT* bude obsahovať jediný riadok, na ktorom bude napísané *ANO*, ak predstavuje vstupný súbor šifrovaciu mriežku, v opačnom prípade na ňom bude napísané *NIE*.

*Príklad:*

MRIEZKA.IN	MRIEZKA.OUT
2	ANO
0 0 1 0	
0 1 0 0	
0 0 0 0	
1 0 1 0	

Myšlienka riešenia: Na políčko papiera so súradnicami  $[x, y]$  sa môžu dostať tie isté políčka mriežky ako nad políčka so súradnicami  $[2N - y + 1, x]$ ,  $[2N - x + 1, 2N - y + 1]$ ,  $[y, 2N - x + 1]$ . Keď si rozdelíme papier na štyri štvorce rozmerov  $N \times N$ , každé z týchto

štyroch políčok bude v inom štvorci. Teda nám stačí skontrolovať iba jeden takýto štvorec (napr. ľavý horný).

V programe je štvrtina papiera reprezentovaná maticou  $a$ . Pred načítaním údajov sa celá vymaže (nastaví na false). Pri načítaní každej diery sa zistí, aká bude jej poloha, keď sa mriežka natočí tak, aby táto diera bola v ľavom hornom štvorci. Na tieto súradnice sa do poľa  $a$  zapíše true. Ak tam už predtým bolo true, mriežka je nekorektná, lebo sa dá dvakrát zapisovať na to isté miesto. Nakoniec treba ešte skontrolovať, či sa dalo písať na každé miesto. To sa v programe realizuje počítadlom dier, ktoré sa zvýši s každou dierou. Ak je mriežka korektná a dier je  $N^2$ , je aj úplná. Tento algoritmus má tú výhodu, že netreba ukladať do pamäti celú mriežku, ale iba jej štvrtinu.

```
procedure pis(i, j : integer);
begin
    {skontroluje, či na súradniciach
     i, j nebola diera a zapíše ju tam}
    if a[i,j] then korektna := false
    else begin
        a[i,j] := true;
    end;
end;

...
for i:=1 to n do
    for j := 1 to n do
        a[i, j] := false;
dier := 0;
korektna := true;

{spracovanie mriežky}
for i := 1 to 2 * n do begin
    for j := 1 to 2 * n do begin
        read(fin, y);
        {ak je to diera...}
        if y = 1 then begin
            inc(dier);
            {treba otočiť dieru do ľavej hornej časti papiera
             a poznačiť si to do poľa}
            if i <= n then
                if j <= n then
                    pis(i, j) {ľavá horná časť mriežky}
                else
                    pis(2*n+1-j, i) {pravá horná časť mriežky}
            else if j <= n then {ľavá dolná časť mriežky}
                pis(j, 2*n+1-i)
            else
                pis(2*n+1-i, 2*n+1-j) {pravá dolná časť mriežky}
            end
        end;
    end;
    readln(fin)
end;

if korektna and (dier = n * n) then
    writeln(fout, 'ANO')
else writeln(fout, 'NIE');
...

```

### 3.2.6 Vernamova šifra

Vernamova šifra je klasickým príkladom substitučnej šifry s heslárom pre jedno použitie. Vernamova šifra je odolná proti kryptoanalytickým spôsobom lúštenia. Šifrovací algoritmus využíva pre šifrovanie otvoreného textu dlhú neopakujúcu sa postupnosť čísel reprezentujúcu heslár pre jedno použitie.

Ako príklad nám poslúži spôsob Vernamovho šifrovania v dekadickom zápise. Predpokladajme, že písmená abecedy resp. ich číselné ekvivalenty budeme sčítavať v aritmetike mod 26 s postupnosťou náhodných dvojmiestnych čísel reprezentovaných ekvivalentnými znakmi. [22]

OT: VERNAMOVASIFRA

kl'úč: KVVAOJFRFWXBDS

ŠT: FZMNOVTMFOFGUS

Pri programovaní postupujeme podobne ako pri Caesarovej šifre, ale namiesto posunu pripočítavame k otvorenému textu náhodne vygenerovaný kl'úč.

```
for i:=1 to Length(otvtext)do
begin
    otvzn:=otvtext[i];
    kluczn:=kluc[i];
    sifzn:=chr((ord(otvzn)-65 + ord(kluczn)-65) mod 26 +65);
    siftext:=siftext+sifzn;
end;
```

Tento kryptosystém pracuje rovnako dobre s abecedou ľubovoľného základu. Pri šifrovaní dvojkovej postupnosti kombinujeme dvojkovú postupnosť s náhodnými bytmi (náhodnou postupnosťou núl a jednotiek) operáciou *xor*. Výsledkom produktu bude iná dvojková postupnosť [22].

Napr.

OT: 10111 10111 01010

kl'úč: 01111 11111 11001

ŠT: 11000 01000 10011

### 3.2.7 Šifrovacie zariadenie Enigma

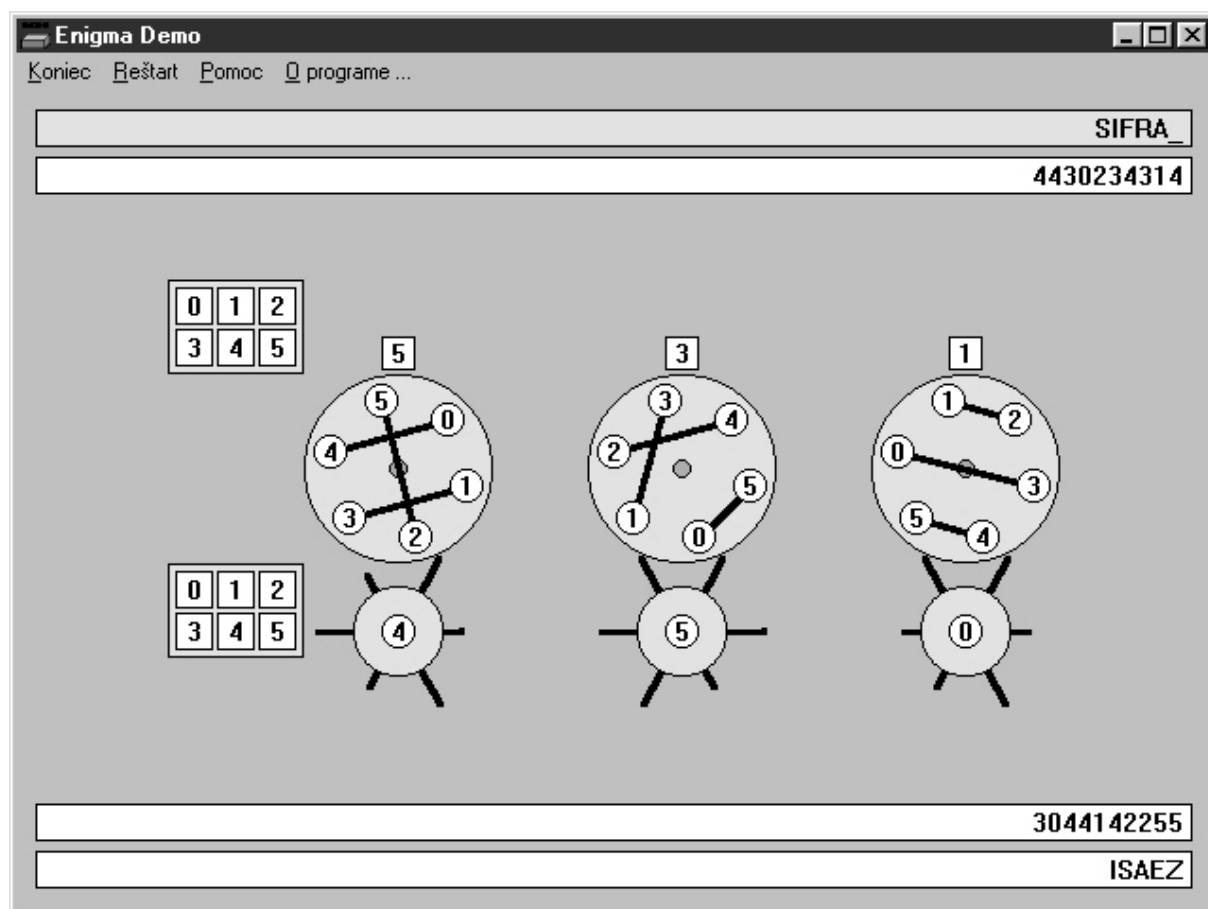
Rotorový stroj má klávesnicu a niekoľko rotorov, z ktorých každý realizuje určitú Vigenrovú šifru. Každý rotor reprezentuje ľubovoľnú permutáciu abecedy, má 26 pozícií a realizuje jednoduchú substitúciu. Rotor môže byť napríklad prepojený tak, že nahradí znak A znakom F, znak B znakom U, znak C znakom L, atď. Výstupné kontakty jedného rotoru sa potom spoja so vstupnými kontaktmi ďalšieho rotoru.

Napríklad pri štvor-rotorovom stroji môže prvý rotor nahradit' znak A znakom F, druhý rotor znak F nahradit' znakom Y, tretí znak Y znakom E a posledný rotor znak E znakom C. Znak C je výstupným znakom zašifrovanej správy. Potom sa niektoré rotory posunú, aby sa v ďalšom kroku realizovali iné substitúcie. Bezpečnosť tohoto stroja zaisťuje kombinácia a otáčanie niekoľkých rotorov. [22]

Na hodine použijeme metodický program autorov Lenky Fibíkovej a Richarda Ostertága, ktorý podrobne a interaktívne opisuje činnosť najznámejšieho šifrovacieho rotorového stroja

Enigmy. Program okrem vizuálnej simulácie obsahuje aj materiál zahŕňajúci princíp činnosti, matematický opis Enigmy a vývojové klony Enigmy v histórii. Program je možné pre vyučovacie aktivity stiahnuť bezplatne na adrese:

<http://www.edi.fmph.uniba.sk/slo/pedsof/ponuka.htm#INFORMATIKA>



Obr. 3.9 Vizualizácia činnosti šifrovacieho stroja Enigma v metodickom programe

### 3.2.8 DES

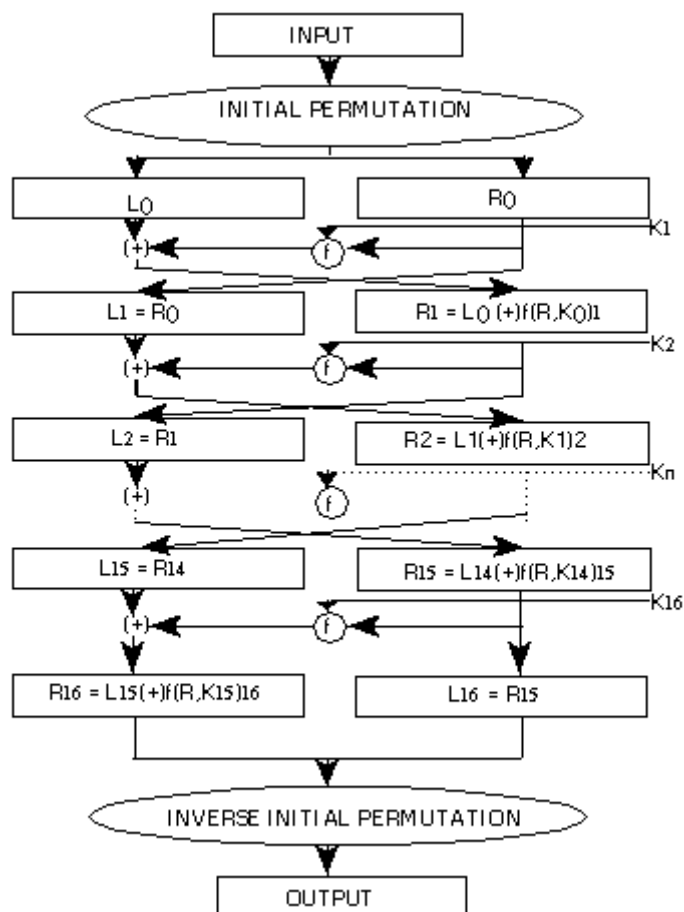
Šifra DES (Data Encryption Standard) slúži ako vhodná ukážková vzorka pre ďalšie systémy založené na princípe Feistelovho kryptosystému.

Princíp algoritmu je uvedený na obrázku 3.10 a 3.11, bližšie informácie je možné nájsť v [22] a [34].

DES je bloková šifra, šifruje dáta po blokoch veľkosti 64 bitov. Dĺžka kľúča je 56 bitov a závisí od neho celá bezpečnosť algoritmu. Algoritmus DES kombinuje metódy substitúcie a permutáciu jednotlivých bitov otvoreného textu v 16 cykloch tzv. rundách.

#### Stručný popis algoritmu:

DES pracuje so 64-bitovými blokmi otvoreného textu. Blok je po počiatočnej permutácii rozdelený na dve polovice, ľavú a pravú, každá má dĺžku 32 bitov. Ďalej nasleduje 16 rúnd identických operácií, označených v obrázku 3.10 ako funkcia  $f$ , v ktorých prichádza ku kombinácii dát a kľúča. Po šestnástej runde sa ľavá a pravá polovica spoja a vykoná sa konečná permutácia (inverzná k počiatočnej permutácii), čím sa algoritmus zakončí.



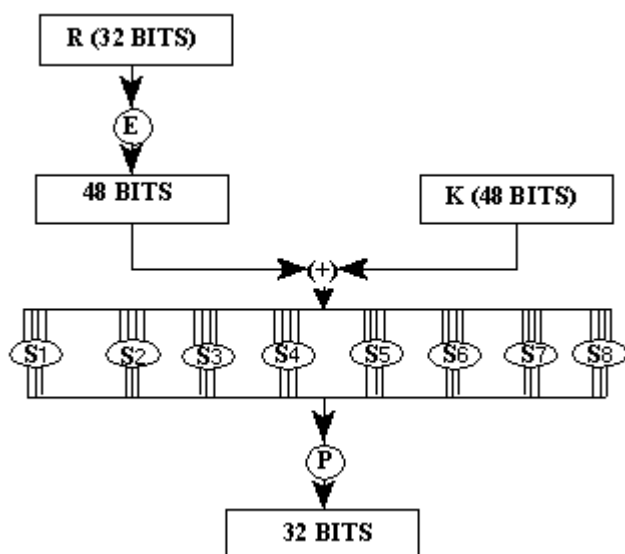
Obr. 3.10 Popis algoritmu DES

V každej runde sa bity kľúča posunú a potom sa z 56 bitov kľúča vyberie 48 bitov. Tento krok je možné algoritmicky pripraviť vopred.

Potom sa v runde pravá polovica dát rozšíri expanznou permutáciou na 48 bitov a skombinuje sa so 48 bitmi posunutého a permutovaného kľúča v sčítateľke mod 2. Ďalej je spracovaná pomocou ôsmich S-boxov (viď nižšie) na 32 nových bitov a znovu spermutovaná. Tieto štyri operácie predstavujú funkciu  $f$  a sú znázornené na obrázku 3.11.

Výstup funkcie  $f$  sa v ďalšej sčítateľke mod 2 skombinuje s ľavou polovicou. Výsledok týchto operácií sa stáva novou pravou polovicou; stará pravá polovica sa stáva novou ľavou polovicou. Tieto operácie sa opakujú 16 krát a vytvárajú 16 rund DESu. [22]

**S-boxy** sú nelineárne funkcie. Každý takýto substitučný S-blok má 6 vstupov a 4 výstupy. 48 bitov, ktoré vchádzajú do S-boxov, je rozdelených na osem 6-bitových podblokov. Každý podblok je



Obr.3.11 Popis funkcie  $f$



spracovaný samostatným S-boxom. Prvý podblok prvým S-boxom, druhý druhým, atď.

Nech je 6 vstupných bitov S-boxu  $b_1, b_2, b_3, b_4, b_5, b_6$ . Kombinácia bitov  $b_1$  a  $b_6$  vytvára číslo medzi 0 a 3, ktoré popisuje príslušný riadok tabuľky S-boxu. Štyri prostredné bity  $b_2$  až  $b_5$  vytvárajú 4-bitové číslo medzi 0-15, ktorému zodpovedá príslušný stĺpec tabuľky. Napr. ak je vstupom 6 bitov 110011, riadok je určený bitmi 11, t. j. 3. riadok a stĺpec bitmi 1001, t.j. 9. stĺpec. V S-boxe 6 je na tejto pozícii číslo 14 (riadky aj stĺpce počítame od nuly). Výstupom je binárny zápis tohto čísla teda 4 bity 1110. [22]

**Úprava kľúča:** na začiatku dôjde k redukcii kľúča zo 64 bitov na 56 bitov, zanedbaním každého nadbytočného ôsmeho bitu, nasledujúcim spôsobom: ako prvý bit sa vyberie bit 57., ako druhý 49. bit, atď. až po 56. bit, ktorý sa obsadí pôvodným štvrtým bitom.

57, 49, 41, 33, 25, 17, 9, 1, 58, 50, 42, 34, 26, 18,  
10, 2, 59, 51, 43, 35, 27, 19, 11, 3, 60, 52, 44, 36,  
63, 55, 47, 39, 31, 23, 15, 7, 62, 54, 46, 38, 30, 22,  
14, 6, 61, 53, 45, 37, 29, 21, 13, 5, 28, 20, 12, 4

Potom sa 56-bitový kľúč rozdelí na dve 28-bitové polovice, ktoré sa posunú rotáciou o jeden, alebo dva bity vľavo, podľa čísla rundy:

Runda	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Posun	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Z takto posunutého 56-bitového kľúča sa *kompresnou permutáciou* vytvorí 48-bitový kľúč.

14, 17, 11, 24, 1, 5, 3, 28, 15, 6, 21, 10,  
23, 19, 12, 4, 26, 8, 16, 7, 27, 20, 13, 2,  
41, 52, 31, 37, 47, 55, 30, 40, 51, 45, 33, 48,  
44, 49, 39, 56, 34, 53, 46, 42, 50, 36, 29, 32

### Jednotlivé permutácie:

*Počiatočná permutácia:*

58, 50, 42, 34, 26, 18, 10, 2, 60, 52, 44, 36, 28, 20, 12, 4,  
62, 54, 46, 38, 30, 22, 14, 6, 64, 56, 48, 40, 32, 24, 16, 8,  
57, 49, 41, 33, 25, 17, 9, 1, 59, 51, 43, 35, 27, 19, 11, 3,  
61, 53, 45, 37, 29, 21, 13, 5, 63, 55, 47, 39, 31, 23, 15, 7

*Koncová permutácia* (inverzná k počiatočnej)

40, 8, 48, 16, 56, 24, 64, 32, 39, 7, 47, 15, 55, 23, 63, 31,  
38, 6, 46, 14, 54, 22, 62, 30, 37, 5, 45, 13, 53, 21, 61, 29,  
36, 4, 44, 12, 52, 20, 60, 28, 35, 3, 43, 11, 51, 19, 59, 27,  
34, 2, 42, 10, 50, 18, 58, 26, 33, 1, 41, 9, 49, 17, 57, 25

*Expanzná permutácia E:*

32, 1, 2, 3, 4, 5, 4, 5, 6, 7, 8, 9,  
8, 9, 10, 11, 12, 13, 12, 13, 14, 15, 16, 17,  
16, 17, 18, 19, 20, 21, 20, 21, 22, 23, 24, 25,  
24, 25, 26, 27, 28, 29, 28, 29, 30, 31, 32, 1

*P-box permutácia P* (permutované sú bity vychádzajúce z S-boxov vid' obrázok 3.11):

16, 7, 20, 21, 29, 12, 28, 17, 1, 15, 23, 26, 5, 18, 31, 10,  
2, 8, 24, 14, 32, 27, 3, 9, 19, 13, 30, 6, 22, 11, 4, 25

*S-boxy:*

S1:

14, 4, 13, 1, 2, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0, 7,  
0, 15, 7, 4, 14, 2, 13, 1, 10, 6, 12, 11, 9, 5, 3, 8,  
4, 1, 14, 8, 13, 6, 2, 11, 15, 12, 9, 7, 3, 10, 5, 0,  
15, 12, 8, 2, 4, 9, 1, 7, 5, 11, 3, 14, 10, 0, 6, 13

S2:

15, 1, 8, 14, 6, 11, 3, 4, 9, 7, 2, 13, 12, 0, 5, 10,  
3, 13, 4, 7, 15, 2, 8, 14, 12, 0, 1, 10, 6, 9, 11, 5,  
0, 14, 7, 11, 10, 4, 13, 1, 5, 8, 12, 6, 9, 3, 2, 15,  
13, 8, 10, 1, 3, 15, 4, 2, 11, 6, 7, 12, 0, 5, 14, 9

S3:

10, 0, 9, 14, 6, 3, 15, 5, 1, 13, 12, 7, 11, 4, 2, 8,  
13, 7, 0, 9, 3, 4, 6, 10, 2, 8, 5, 14, 12, 11, 15, 1,  
13, 6, 4, 9, 8, 15, 3, 0, 11, 1, 2, 12, 5, 10, 14, 7,  
1, 10, 13, 0, 6, 9, 8, 7, 4, 15, 14, 3, 11, 5, 2, 12

S4:

7, 13, 14, 3, 0, 6, 9, 10, 1, 2, 8, 5, 11, 12, 4, 15,  
13, 8, 11, 5, 6, 15, 0, 3, 4, 7, 2, 12, 1, 10, 14, 9,  
10, 6, 9, 0, 12, 11, 7, 13, 15, 1, 3, 14, 5, 2, 8, 4,  
3, 15, 0, 6, 10, 1, 13, 8, 9, 4, 5, 11, 12, 7, 2, 14

S5:

2, 12, 4, 1, 7, 10, 11, 6, 8, 5, 3, 15, 13, 0, 14, 9,  
14, 11, 2, 12, 4, 7, 13, 1, 5, 0, 15, 10, 3, 9, 8, 6,  
4, 2, 1, 11, 10, 13, 7, 8, 15, 9, 12, 5, 6, 3, 0, 14,  
11, 8, 12, 7, 1, 14, 2, 13, 6, 15, 0, 9, 10, 4, 5, 3

S6:

12, 1, 10, 15, 9, 2, 6, 8, 0, 13, 3, 4, 14, 7, 5, 11,  
10, 15, 4, 2, 7, 12, 9, 5, 6, 1, 13, 14, 0, 11, 3, 8,  
9, 14, 15, 5, 2, 8, 12, 3, 7, 0, 4, 10, 1, 13, 11, 6,  
4, 3, 2, 12, 9, 5, 15, 10, 11, 14, 1, 7, 6, 0, 8, 13

S7:

4, 11, 2, 14, 15, 0, 8, 13, 3, 12, 9, 7, 5, 10, 6, 1,  
13, 0, 11, 7, 4, 9, 1, 10, 14, 3, 5, 12, 2, 15, 8, 6,  
1, 4, 11, 13, 12, 3, 7, 14, 10, 15, 6, 8, 0, 5, 9, 2,  
6, 11, 13, 8, 1, 4, 10, 7, 9, 5, 0, 15, 14, 2, 3, 12

S8:

13, 2, 8, 4, 6, 15, 11, 1, 10, 9, 3, 14, 5, 0, 12, 7,  
1, 15, 13, 8, 10, 3, 7, 4, 12, 5, 6, 11, 0, 14, 9, 2,  
7, 11, 4, 1, 9, 12, 14, 2, 0, 6, 10, 13, 15, 3, 5, 8,  
2, 1, 14, 7, 4, 10, 8, 13, 15, 12, 9, 0, 3, 5, 6, 11

Dešifrovanie textu pomocou DES je rovnaké ako šifrovanie, s tým rozdielom, že kľúče musia byť použité v opačnom poradí. T. j. ak boli v rundách pri šifrovaní použité kľúče  $K_1, K_2, \dots, K_{16}$ , tak pri dešifrovaní musia byť použité v poradí  $K_{16}, K_{15}, \dots, K_1$ . Posun kľúča prebieha doprava a počty krokov sú 1,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1. [22]

Napr. ak je otvoreným textom správa "0123456789ABCDEF" a šifrujeme ju pomocou kľúča "133457799BBCDFF1", dostaneme šifrovaný text "85E813540F0AB405". Ak je tento text dešifrovaný s tým istým tajným kľúčom "133457799BBCDFF1", výsledkom je pôvodný otvorený text "0123456789ABCDEF".

### 3.2.9 Asymetrické šifrovanie

Pri asymetrickom šifrovaní sa na hodinách zameriame iba na ozrejmienie filozofie asymetrického šifrovania. Prakticky si túto činnosť preskúšame na šifrovacom softvéri PGP, ktorý je možný získať bezplatne napr. na adrese [www.pgp.cz](http://www.pgp.cz). K detailnému opisu asymetrických šifrov (akou je napr. RSA) je potrebná znalosť určitých celkov z teórie čísel a z teórie výpočtovej zložitosti. Tento proces prenechávame až na vysokú školu. Pre študentov

strednej školy postačí znalosť tejto problematiky na používateľskej úrovni, t. j. schopnosť ovládať nástroje (PGP softvér), ktoré asymetrické šifrovanie využívajú.

Asymetrické šifrovanie aplikuje, narozdiel od symetrických šifrov uvedených v predošlých kapitolách, iný kľúč pre šifrovanie a iný pre dešifrovanie. Označenie pre takúto dvojicu v anglickej literatúre je *keypair* – pár kľúčov. Kľúč, pomocou ktorého sa šifruje, sa nazýva *verejný kľúč* (*public key*) a kľúč, ktorým sa dešifruje, sa nazýva *súkromný kľúč* (*private key*). Princíp činnosti asymetrického kryptológie je nasledovný: Bob má svoj pár kľúčov – jeden súkromný a jeden verejný kľúč. Jeho verejný kľúč poznajú všetci, k súkromnému má prístup iba Bob. Ktokoľvek mu chce poslať tajnú správu, zašifruje ju jeho verejným kľúčom. Jediný, kto môže správu rozlúštiť je Bob, dokonca ani odosielateľ ju nemôže rozšifrovať.

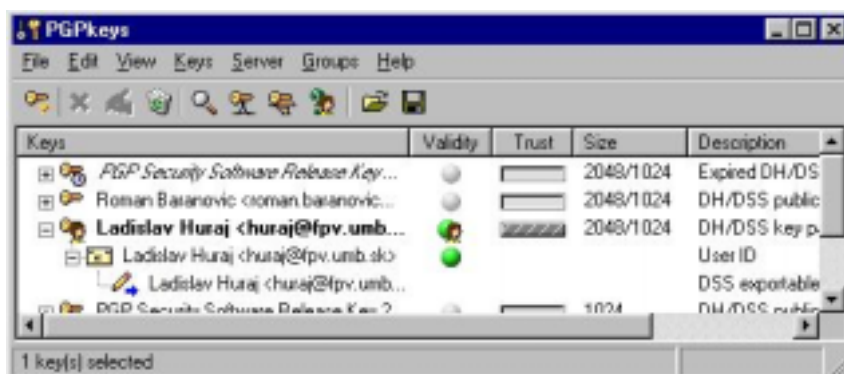
Tento princíp má svoje výhody. Účastníci komunikácie si nemusia pred jej započatím vymeniť kľúče bezpečným kanálom, čiže je potrebných menej kľúčov. Verejný kľúč môžu poznať všetci a ktokoľvek chce poslať tajnú správu Bobovi, zašifruje ju Bobovým verejným kľúčom.

Ďalšou funkciou, ktorú je možné realizovať pomocou asymetrickej kryptológie je *digitálny podpis*. Pomocou *hašovacích funkcií* (napr. MD5), vytvoríme tzv. *odtlačok správy*. Hašovacia funkcia z ľubovoľnej správy na vstupe vytvorí jednoznačný odtlačok pevnej dĺžky (128, príp. 160 bitov). Ak by sa v správe zmenilo iba jediné písmeno, dostaneme na výstupe úplne iný odtlačok. Hašovacie funkcie sú známe a ktokoľvek si môže z akejkoľvek správy taký odtlačok vytvoriť. Navyše platí, že je výpočtovo veľmi obtiažne vytvoriť k ľubovoľnej správe správu inú, ktorá má rovnaký odtlačok.

Odtlačok správy sa "zašifruje súkromným kľúčom" (je vykonaná opačná transformácia k transformácii šifrovania), čím dostávame žiadaný digitálny podpis, ktorý sa pripojí na koniec pôvodnej správy. Ak by sa na koniec správy nepripojil iba odtlačok, ale celá pôvodná správa "zašifrovaná súkromným kľúčom", znamenalo by to nárast správy o dvojnásobok. Pri odtlačku to znamená nárast len o niekoľko bajtov. [35] Pretože odtlačok bol "zašifrovaný súkromným kľúčom", je zrejmé, že jeho autorom mohol byť iba držiteľ súkromného kľúča.

Program PGP využíva systém asymetrickej kryptológie. Aj keď spôsob narábania s dátami je zložitejší, na strednej škole posluží ako vhodný príklad. Tento nástroj umožňuje šifrovať, podpisovať, dešifrovať a overiť podpis správy zaslanej elektronickou poštou.

Pred zaslaním zašifrovanej správy, potrebujeme: vlastný pár kľúčov, t. j. súkromný (na podpisovanie a príp. dešifrovanie správy) a verejný kľúč (zverejnený na niektorom z PGP verejných serverov napr. [www.pgp.cz](http://www.pgp.cz)), aby nám pomocou neho používatelia zasielali šifrované správy a verejné kľúče osôb, ktorým chceme šifrovanú správu odoslať.



Obr. 3.12 Manažér kľúčov v programe PGP

Pri inštalácii softvéru PGP sa automaticky nainštalujú nástroje na využívanie asymetrickej kryptológie do programov zabezpečujúcich elektronickú poštu (MS Outlook, Qualcomm Eudora) a jednoduchým kliknutím na tlačidlá sa dajú tieto nástroje ovládať. Pri inštalácii sa taktiež vygeneruje pár kľúčov (ak doteraz neexistoval), pričom je možné verejný kľúč exportovať napr. na disketu, príp. server, aby s ním mohli manipulovať aj ostatní žiaci.

Po týchto úkonoch už študenti môžu používať asymetrické šifrovanie v elektronickej pošte. Zašifrovaný mail, ktorý sme obdržali, PGP softvér dešifruje a verifikuje, t. j. skontroluje pravosť digitálneho podpisu. Pred a za správu je pridaná PGP hlavička, ktorá informuje o stave digitálneho podpisu, kto je autor podpisu, čas podpisu a verifikácie a kde začína a končí samotná správa.

#### Príklad podpísanej a zašifrovanej správy v PGP

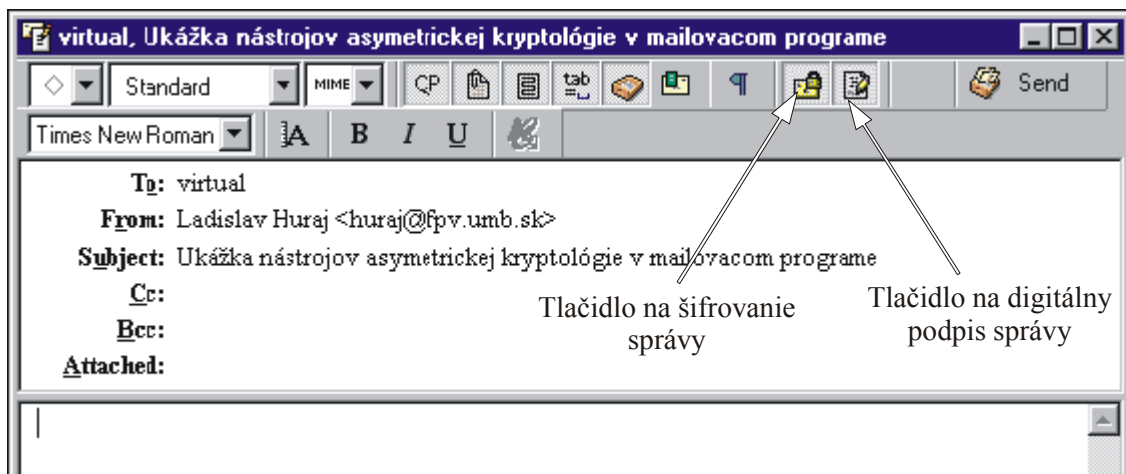
```
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 7.0.3 for non-commercial use <http://www.pgp.com>
qANQRlDBwU4DL0Aw6BkZg/cQCACl40QCjGXAlnUhkRIr5sccpWUTzyeK38AnLvBx
9Lz7pvEypnj7th0lFikmQXqBS8cv4xYtejUide5r27LOj/+GzFXOXexlzpJO+3Zw
Vvfl1iYz40QgvqZu+0jqejXdKlqjGLLwcqhbXHeuNw+SY0NA4//bYwuka2vLzf0AN
iPz3Ldl345gRtmUIuzX5MYw5nC5sQ9gUz1UBCINr24ypdM8rfDDjZhbvPXQrvhBJ
3ldJ8tjo3nMb8oBKItf5UViP/hyOZ0+/AcJIU5jrD9IZoQFAlQJA67FBYm5i0CNR
EVsDPKnp04fsCpl7KG5SNmQfhFn4xxp5SH7013Ok1Gf70sx/CADX2gClADq89dh8
1mECiGBhhaVzuqaRNvD8DnChpQwsWxZDS4ubKLAjntqenmnSBVaiNe/FYKhOyLA9
yf7sy08RPvPlvAtXnI41c9zk/9RC/auuV8xAvF46xFbWVcj4tsHmW/zulqqwISAR
s/k2Ez+dBT9sgLm794PNIdFf+sFycwLja7eVaThdGYWrM5CBmTRD2810QNQ5jwOu
0hrd9CcXSqK7vK938xQ8ZLMFtn+amDzwdHuX1rJhRh8q5BjiZO4Djxwog4CfMNHp
AccFDIGM1IEQGR2Svq8Cj9mDu/4DbtjeJfCkDmAai2pP7o401e/5pCCcgbShHCRr
Qne40qr0yZIkS0Dl2RYMHRgFGSgnNwR2em3TknGBG0qCetV9++lFF0dsBfPoIbTB
IJbYIBkZ/7KbQvMga2r+K0jdqpXyfl85/yHrACTfbwLPhptVpHejhFF945wD+DJQ
BVIMV6M+OYyfcLl8k+J+qWQWhRMbaAz3Aj6M3yyrxsQ+TVjpvm8qQdcOFoIW6EwL
PIUJVzOQjib2DA==
=m6Wr
-----END PGP MESSAGE-----
```

a jej obsah po dešifrovaní a verifikácii podpisu:

```
*** PGP Signature Status: good
*** Signer: Ladislav Huraj <huraj@fpv.umb.sk>
*** Signed: 3.10.2001 10:18:39
*** Verified: 3.10.2001 10:19:46
*** BEGIN PGP DECRYPTED/VERIFIED MESSAGE ***
Toto je sifrovana a podpísana správa.
*** END PGP DECRYPTED/VERIFIED MESSAGE ***
```

Správu môžeme iba podpísať, čo znamená, že informácia nie je tajná, ale je daný autor správy, čiže je zaručená pravosť odosielateľa. V hlavičke je uvedený hašovací algoritmus (SHA1) použitý na vytvorenie odtlačku správy. Opäť je možné urobiť verifikáciu podpisu.

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
Toto je iba podpísana správa.
-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 7.0.3 for non-commercial use <http://www.pgp.com>
iQA/AwUBO7rGI6248RkUNAmjEQLmvgCbBVd4fYbL+Kodr5i2PoWdiYrhsO4AoOH7
13E0w038osPlNoKxr2FGfrlZ
=dhly
-----END PGP SIGNATURE-----
```



Obr. 3.13 Doinštalované tlačidlá v programe pre elektronickú poštu Eudora

### 3.3 Záver

V tejto kapitole sme popísali niektoré metodické postupy vychádzajúce z fylogénzy kryptografie. Ontogénzu sme rozdelili do dvoch celkov. V prvom sa žiaci na základnej škole hravou formou oboznamujú s klasickými šifrovacími systémami. V tomto celku žiaci transformujú konkrétny otvorený text na zašifrovaný text s využitím niektorého šifrovacieho algoritmu. Na celok nadväzuje druhý, na strednej škole, kde študenti najskôr narábajú už so samotnými šifrovacími algoritmami na všeobecnej úrovni a až potom prichádza k šifrovaniu jednotlivých textov.

Uvedené aktivity sú pre žiakov zaujímavé, podnecujú ich zvedavosť.

Uviedli sme len časť úloh, ktoré je možné so žiakmi robiť. Niektoré ďalšie je možné nájsť v [5], [32], príp. v [33], kde je možné nájsť aj návrh šifrovacieho kruhu s diakritikou.

## Kapitola 4

### Podporné programy

K vyučovaniu celku kryptografia sme vytvorili sadu podporných programov, ktoré umožňujú šifrovať text pomocou jednotlivých šifrovacích algoritmov. Programy slúžia predovšetkým učiteľovi, jednak na rýchle overenie správnosti šifrovaného textu, jednak na pochopenie programových postupov implementácií algoritmov. Pri vytváraní programov na strednej škole je možné poskytnúť "exe" tvary programov aj študentom, aby si mohli porovnať správnosť vlastných algoritmov.

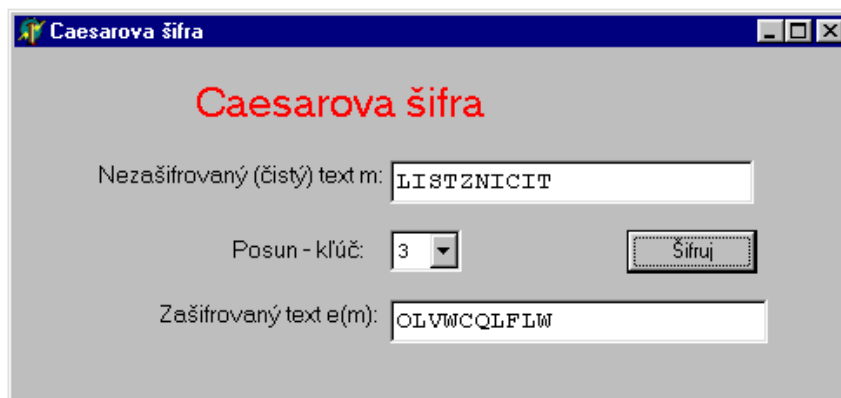
Programov je celkovo sedem. Realizujú šifry: Caesarovu, bigramovú, Vigenеровu, autokľúč, Vernamovu dekadickú, Vernamovu binárnu a šifru DES.

#### 4.1 Prostredie programov

Na úspešný chod programov je potrebný minimálne operačný systém MS Windows 95, príp. vyššie verzie tohto systému.

Programy majú jednotný dizajn. V hlavnom okne programu sa vždy nachádza názov šifry, ktorú program implementuje. Ďalej okno obsahuje editovací riadok, do ktorého sa wpisuje otvorený text a riadok, v ktorom je zobrazený zašifrovaný text a tlačidlo *Šifruj*, po stlačení ktorého prebehne zašifrovanie otvoreného textu. Program môže ešte obsahovať ďalšie komponenty, ak ich daná šifra vyžaduje.

Pri zadávaní textu je dôležité zadávať text *bez diakritiky*. Program automaticky zmení malé písmená v texte na veľké a odstráni medzery z textu. Takéto isté úpravy vykoná aj pri zadávaní kľúča.



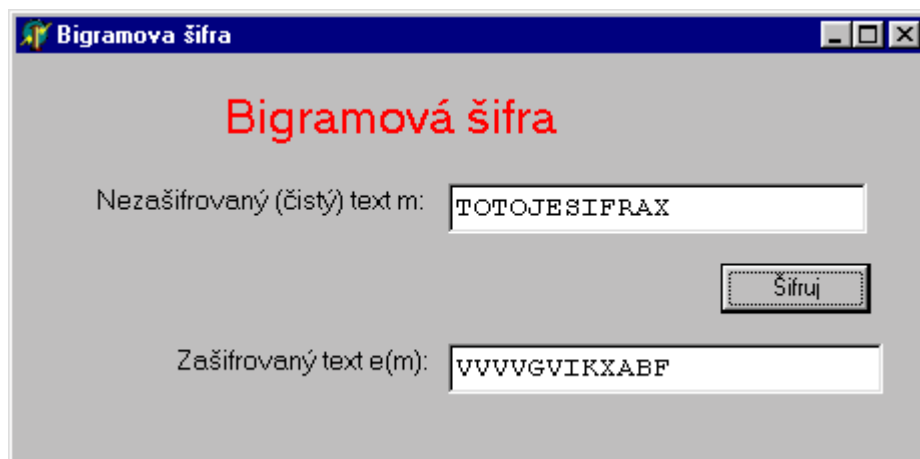
Obr. 4.1 Podporný program pre Caesarovú šifru

## Caesarova šifra

Program Caesarovej šifry obsahuje okrem riadku pre otvorený a zašifrovaný text aj roztvárací zoznam (Combo box) pre voľbu posunutia znakov v abecede. Roztvárací zoznam obsahuje hodnoty od 1 po 26, pričom automaticky je predvolená hodnota 1.

## Bigramová šifra

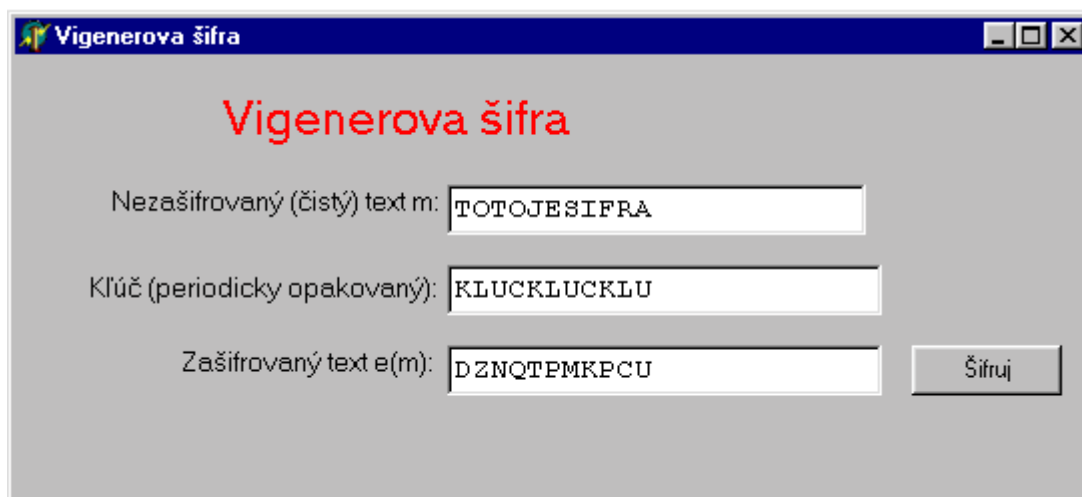
Hlavné okno programu obsahuje iba základné tri komponenty: vstupný a výstupný editovací riadok a tlačidlo šifruj. Ak je potrebné, otvorený text sa automaticky dopĺňa na párny počet znakov znakom X.



Obr. 4.2 Podporný program pre bigramovú šifru

## Vigenerova šifra

V okne sa nachádza ešte editovací riadok pre zadanie kľúča. Ak je kľúč kratší ako otvorený text, automaticky sa podpíše pod celý text.

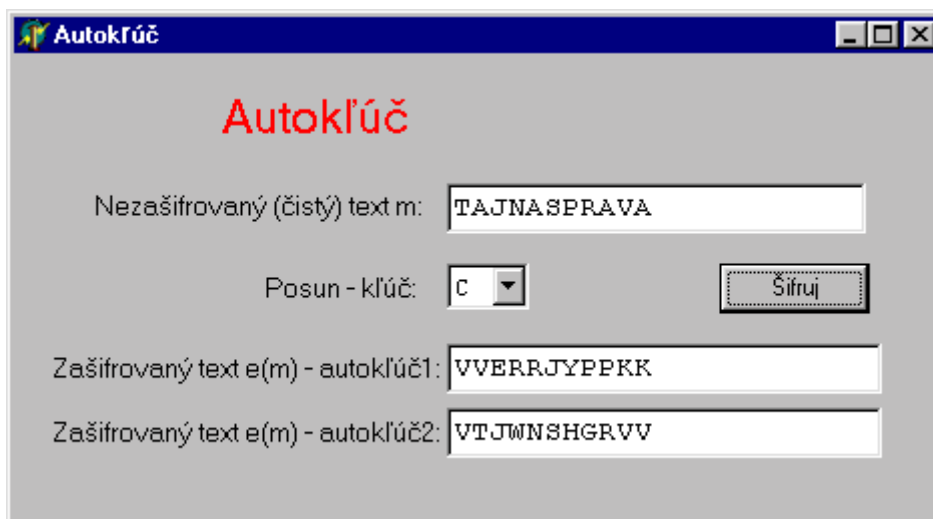


Obr. 4.3 Podporný program pre Vigenerovu šifru

## Autokľúč

Program realizujúci šifrovanie autokľúčom obsahuje až dva výstupné riadky, pretože záleží od zvolenej metódy šifrovania, či sa v kľúči sčítavajú buď znaky otvoreného, alebo šifrovaného textu. V okne sa ďalej nachádza roztvárací zoznam pre výber prvého písmena

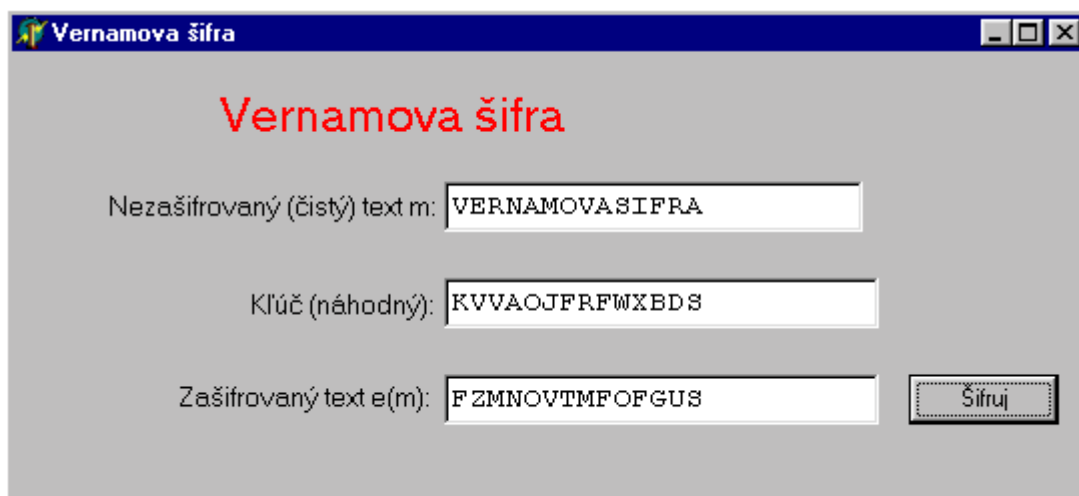
klúča. Roztvárací zoznam obsahuje hodnoty od A po Z, pričom automaticky je predvolená hodnota A.



Obr. 4.4 Podporný program pre šifrovanie autokľúčom

### Vernamova šifra – dekadická

V okne sa nachádza aj editovací riadok pre zadanie kľúča. Ak je kľúč kratší ako otvorený text, automaticky sa vygeneruje náhodný kľúč pod celý otvorený text.



Obr. 4.5 Podporný program pre Vernamovu šifru dekadickú

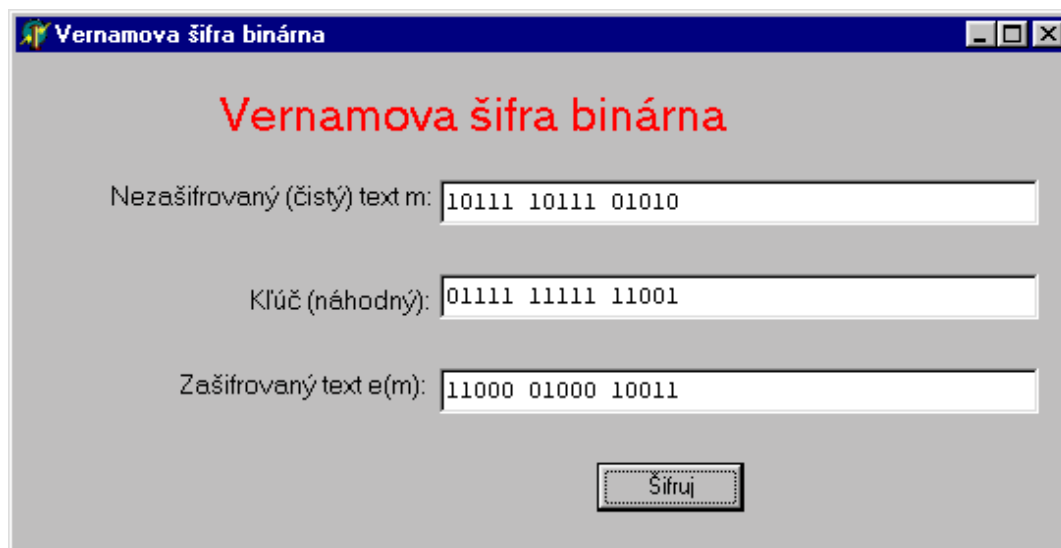
### Vernamova šifra – binárna

Obdobne ako v predchádzajúcom príklade, ale do vstupného riadku sa vpisujú iba znaky 0 alebo 1. Program automaticky doplní vstupný reťazec na dĺžku deliteľnú piatimi a upraví text vo vstupnom a výstupnom riadku na päťice.

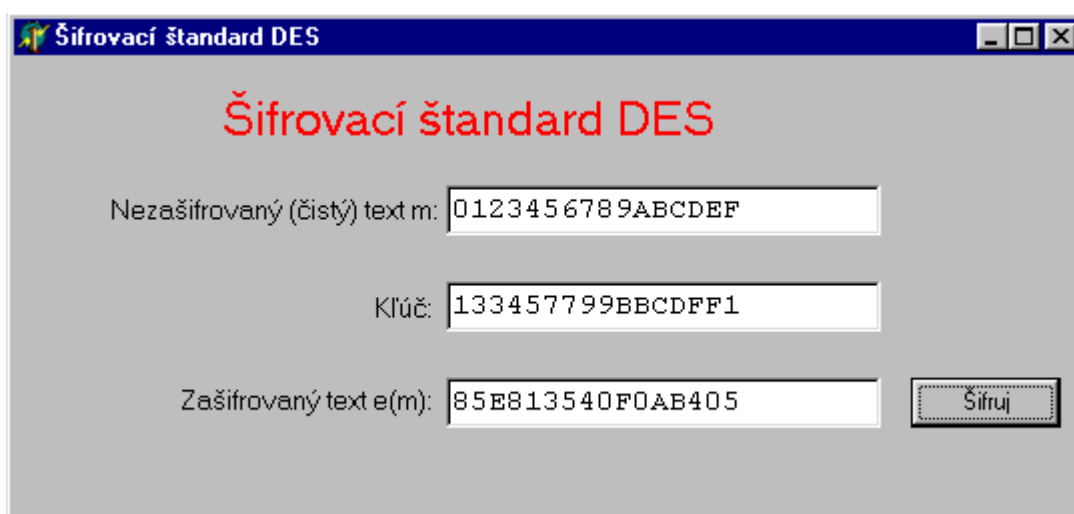


## DES

V okne sa nachádza editovací riadok pre zadanie kľúča. Ak je kľúč kratší ako otvorený text, automaticky sa vygeneruje náhodný kľúč pod celý otvorený text. Pretože algoritmus DES pracuje so 64-bitovými blokmi, program automaticky doplní vstupný reťazec na dĺžku jedného 64-bitového bloku.



Obr. 4.6 Podporný program pre Vernamovu šifru binárnu



Obr. 4.7 Podporný program pre šifru DES

## 4.2 Technická realizácia

Podporné programy boli napísané v prostredí Borland Delphi 5. Nie je nutná ich inštalácia. K svojmu behu nevyžadujú žiadne ďalšie knižnice, ani iné súbory.

Samotné šifrovanie prebieha v metóde `TForm1.Button1Click`. Program využíva pomocnú procedúru `upravtext`, ktorá zabezpečuje odstránenie medzier v zadanom otvorenom texte. V metóde `TForm1.FormCreate` sú počiatočné nastavenia, buď Combo boxov, alebo je volaná inicializácia generátora náhodných čísel procedúrou `Randomize`.

Programy je jednoduché upraviť spôsobom, že jednotlivé znaky sa načítavajú zo vstupného textového súboru a zapisujú sa do výstupného textového súboru.

## Kapitola 5

### Záver

Našou snahou bolo v práci poukázať na fakt, že pri vyučovaní kryptografie je možné a potrebné vychádzať z historického vývinu tohto odboru.

Okrem zmapovania dôležitých zlomov vo fylogénéze kryptografie sme v práci uviedli aj sadu aktivít, ktoré je možné využiť už na základnej, ale aj na strednej škole. Aktivitty okrem toho, že poskytujú nemalý priestor motivácii, rozvíjajú u žiakov schopnosť experimentovania, logické a algoritmické myslenie, rozvíjajú schopnosť manipulácie s údajmi.

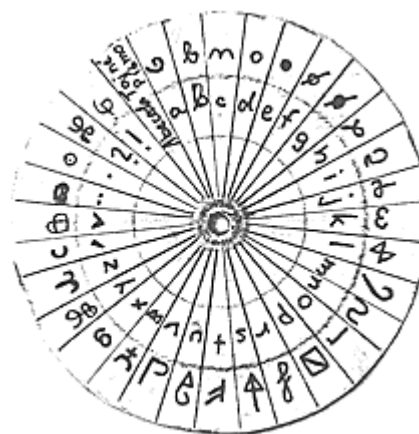
Bezprostredne po celku kryptografia by mal nasledovať celok týkajúci sa informačnej bezpečnosti a úlohe kryptografie v tejto oblasti.

V prípade, že žiaci prejavili o oblasť kryptografie záujem, je možné na kryptografické aktivity nadviazať paralelnou líniou kryptológie a to kryptoanalýzou jednotlivých klasických kryptosystémov. Popis niektorých kryptoanalytických problémov pre strednú školu je možné nájsť v [5]. Je v nej uvedená metóda kryptoanalýzy Caesarovej šifry, monoalfabetických substitučných šifier, polyalfabetickej Vigenereovej šifry a traspozičných šifier z pohľadu študenta strednej školy. Kryptoanalytické postupy je možné nájsť aj v [7] a [36].

Ďalšou oblasťou, ktorá môže nadväzovať na prebraný celok je steganografia – metóda zaoberajúca sa ukrývaním dát. Aj v tejto metóde je možné uplatniť postup genetickej paralely, počínajúc tajnými atramentmi, zaliatymi tabuľkami, správami písanými na ľudské telo, skrývaním správ v obrazoch a textoch, až po modernú počítačovú steganografiu využívajúcu zmenu v zložkách farieb v obrázkoch, drobné zmeny vo zvukových stopách a videu, ktoré sú pre ľudské zmysly nepostrehnuteľné.

Na záver chceme uviesť posledný argument potvrdzujúci, že s kryptografiou je možné narábať už na základnej škole. Dvaja žiaci 6. ročníka používajú na komunikáciu medzi sebou (a nielen počas vyučovania) šifrovací disk Obr. 5.1. Dôvodom používania disku bola snaha, aby nikto nemohol ich správy rozlúštiť.

Disk realizuje jednoduchú substitúciu medzi dvoma abecedami, slovenskou a abecedou znakov vytvorenou žiakmi. Ak vezmeme do úvahy fakt, že žiaci šifrovanie používajú samostatne a dobrovoľne a na zostrojenie disku



Obr. 5.1 Šifrovací disk žiakov  
šiestej triedy ZŠ

vynaložili určitý čas, je veľký predpoklad, že po predložení kryptografických aktivít ich záujem o šifrovanie ešte vzrastie.

Veríme, že naša práca pomôže pri skvalitnení vyučovania dynamicky sa rozvíjajúceho predmetu informatika na strednej, ale aj na základnej škole.

## Kapitola 6

### Slovník pojmov

**Asymetrický algoritmus** – kryptografický algoritmus, ktorý používa pri zašifrovaní verejný kľúč a pri dešifrovaní súkromný kľúč. Tieto kľúče vytvárajú dvojicu asymetrických kľúčov.

**Atbaš** – jednoduchá reverzná substitučná šifra používaná Hebrejcami. V tejto šifrovacej metóde je prvé písmeno abecedy nahradené posledným, druhé predposledným, atď.

**Brainstorming** – didaktická metóda – kreatívna metóda riešenia problémov založená na skupinovom riešení, ktorá má uľahčiť generovanie kreatívnej stratégie.

**DES** (Data Encryption Standard) – verejný kryptografický algoritmus, ktorý prostredníctvom podpory amerického National Institute of Standards and Technology a verejnej správy USA získal podporu a popularitu. Jedná sa o symetrický blokový algoritmus. DES je jedným zo svetových štandardov pre kryptografické algoritmy používaným v bankovníctve. V súčasnosti je nahradený algoritmom Rijndael.

**Dešifrovanie** – opak procesu zašifrovania, prevod šifrovaného textu do textu pôvodného.

**Digitálny podpis** – dáta pripojené k správe. Cieľom je umožniť príjemcovi správy preveriť jej obsah a ochrániť ju proti modifikácii. Digitálny podpis je funkciou samotnej správy a tajného súkromného kľúča odosielateľa. Podpis je možné overiť pomocou verejného kľúča odosielateľa.

**Hašovacia funkcia** – matematická funkcia, ktorá vypočíta na základe postupnosti čísel (číselne zakódovaného dokumentu ľubovoľnej konečnej nenulovej dĺžky) číslo pevnej dĺžky (napríklad 128 miestne). Pritom hašovacia funkcia spĺňa nasledujúce požiadavky: hašovacia hodnota sa počíta ľahko; na základe hašovacej hodnoty je ťažké nájsť dokument s touto hašovacou hodnotou; je ťažké nájsť dva rozličné dokumenty s rovnakou hašovacou hodnotou.

**Homofónna substitúcia** – substitučná šifra podobná monoalfabetickej substitúcii. Rozdiel spočíva v tom, že jeden znak otvoreného textu môže byť nahradený jedným znakom z niekoľkých možných znakov šifrovaného textu. Napr. znak A môže byť nahradený buď ako 5, 13, 25 alebo 56, znak B ako 7, 19, 31 alebo 42 atď. Cieľom je pozmeniť frekvenciu výskytu niektorých často sa vyskytujúcich znakov v texte.

**Klamač** – nevýznamová (nadbytočná) skupina písmen, ktorá má za úlohu sťažiť kryptoanalýzu zašifrovaných textov.

**Kľúč** – sekvencia znakov (bitov), slúžiaca na kontrolu vykonávaných operácií.

**Kód** – algoritmus na transformáciu zrozumiteľnej správy na nezrozumiteľnú využívajúci kódovaciu tabuľku. Kód zväčša narába s lingvistickými prvkami.

**Kryptoanalýza** – analýza kryptografického systému a (alebo) vstupných a výstupných hodnôt za účelom zistenia dôverných hodnôt a (alebo) citlivých dát, vrátane pôvodného nezašifrovaného textu, kryptografického kľúča a pod.

**Kryptografia** – vedecká disciplína, ktorá zahŕňa princípy, prostriedky a metódy pre transformácie dát za účelom utajenia ich informačného obsahu, zabráneniu ich nedetekovanej modifikácii a použitiu. Kryptografia sa zaoberá metódami, ktoré sú používané pri šifrovaní a dešifrovaní, pričom kryptoanalýza sa zaoberá pokusmi o prekonanie týchto metód.

**Kryptológia** – veda o informačnej celistvosti zahŕňajúca kryptografiu a kryptoanalýzu.

**Monoalfabetická (jednoduchá) substitúcia** – substitučná šifra, v ktorej je každý znak otvoreného textu nahradený príslušným znakom šifrovaného textu, napr. Caesarova šifra.

**Nomenklátor** – metóda šifrovania správy. Nomenklátory obsahujú okrem úplnej substitučnej abecedy aj dvoj písmenové kódy pre jeden až dva tucty najfrekvencovanejších slov alebo mien a navyše tiež tzv. klamače.

**Otvorený text** – zrozumiteľný text, ešte nezašifrovaná správa.

**PGP** (Pretty Good Privacy) – je kryptografický softvérový balík, ktorý je využívaný predovšetkým pre šifrovanie správ a súborov a vytváranie/overovanie digitálnych podpisov. Jeho autorom je Američan Philip R. Zimmermann. Prvá verzia tohoto programu bola uvoľnená v júni 1991 ako "free software". Dnes patrí PGP medzi najrozšírenejší prostriedok pre šifrovanie elektronickej pošty a pre overovanie jej pravosti pomocou digitálneho podpisu.

**Polyalfabetická substitúcia** – substitučná šifra, ktorá sa skladá z niekoľkých jednoduchých šifier. Túto šifru môže tvoriť napríklad päť rôznych jednoduchých substitučných šifier. Jednotlivé šifry sú za radom aplikované na jednotlivé po sebe idúce znaky otvoreného textu.

**Polygramová substitúcia** – substitučná šifra, v ktorej šifrovanie prebieha medzi skupinami znakov. Napr. skupina znakov ABA môže byť nahradená skupinou RTQ, ABB skupinou SLL atď.

**Rotor** – mechanický disk, ktorý realizuje nejakú substitúciu.

**RSA** – algoritmus založený na kryptografii verejného kľúča vyvinutý autormi Rivest, Shamir, a Adelman. Algoritmus sa používa na šifrovanie a autentifikáciu a je založený na obtiažnosti faktorizácie veľkých čísel.

**Skytalé** – prvá známa mechanická pomôcka na šifrovanie. Mala tvar dreveného valca. Na valec sa prúžok za prúžkom tesne vedľa seba namotal pruh papyrusu, kože alebo pergamenu, na ktorý sa písala správa.

**SSL** (Secure Sockets Layer) – špecifikovaný mechanizmus vyvinutý firmou Netscape na zabezpečenie prenášaných dát medzi klientom a serverom.

**Steganografia** – vedecká disciplína, ktorá zahrňuje princípy, prostriedky a metódy pre utajenie samotnej existencie dát.

**Substitúčná šifra** – šifra nahradzuje každý znak otvoreného textu za iný znak šifrovaného textu. Aby príjemca získal otvorený text, musí na zašifrovaný text použiť invertovanú funkciu.

**Súkromný kľúč** – jeden z dvojice kľúčov asymetrického systému určitej entity (osoby, servera, ...). V prípade systému zabezpečujúceho šifrovanie sa jedná o dešifrovací kľúč danej entity a v prípade systému digitálneho podpisu sa jedná o kľúč, ktorý slúži na tvorbu digitálneho podpisu správy.

**Symetrický algoritmus** – kryptografický algoritmus, pri ktorom je možné zo šifrovacieho kľúča odvodiť dešifrovací a naopak. Väčšina symetrických algoritmov používa pri zašifrovaní a pri dešifrovaní rovnaký kľúč.

**Šifra** – kryptografická metóda, príp. jej aplikácia, pri ktorej na základe určitej informácie (napr. kľúča) prichádza k transformácii dát za účelom ich ochrany – obvykle utajenia obsahu. Transformácia je vykonaná na základe daného kryptografického algoritmu.

**Šifrovanie, zašifrovanie** – kryptografický termín označujúci proces transformácie nešifrovaných dát na dáta šifrované takým spôsobom, že pôvodné dáta buď nemôžu byť získané, alebo môžu byť získané len použitím príslušného inverzného procesu dešifrovania.

**Šifrovaný text** – zašifrovaná podoba textu.

**Transpozičná šifra** – pri tejto šifre sa znaky otvoreného textu nemenia, mení sa usporiadanie znakov, napr. stĺpcová transformácia, skytalé.

**Verejný kľúč** – jeden z dvojice kľúčov asymetrického systému určitej entity (osoby, servera, ...). V prípade systému zabezpečujúceho šifrovanie sa jedná o šifrovací kľúč danej entity a v prípade systému digitálneho podpisu sa jedná o kľúč, ktorý slúži na overenie digitálneho podpisu.

## Zoznam citovanej literatúry

1. Rybár, J., 2000. Fylogénéza a ontogenéza poznania, seminár KOGNITÍVNE VEDY-CogSci2000. [http://math.chtf.stuba.sk/CogSci\\_2000.htm](http://math.chtf.stuba.sk/CogSci_2000.htm)
2. Hejný, M.: História učí učiť. In: Matematické obzory, 23/1984, s. 3-11
3. Olejar, D., Stanek, M.: Some Aspects of Cryptology Teaching. 1st World Conference on Information Security Education WISE1. Stockholm, Sweden, 1999.
4. Blahová, V. a kol.: Nové trendy v informatike. Bratislava: Phare I, 1997, 90 s.
5. Olejár, D., 1999. Informačná bezpečnosť a kryptológia. (prednáška pre stredoškolských učiteľov). <http://www.didinfo.input.sk>
6. Brown, L., 2001. Cryptography and Computer Security. <http://www.cs.adfa.oz.au/teaching/studinfo/csc/lectures/ss-less02.html>
7. Grošek, O., Porubský, Š.: Šifrovanie – algoritmy, metódy, prax. Praha: Grada a.s., 1992, 272 s. ISBN 80-58424-62-2.
8. Savard, J. J. G., 1999. A Cryptographic Compendium. <http://home.ecn.ab.ca/~jsavard/crypto/jscrypt.htm>
9. Klíma, V.: Utajené komunikace. In: Chip, 1994, č. 5, s. 194-197
10. Klíma, V.: Utajené komunikace. In: Chip, 1994, č. 6, s. 184-188
11. Leary, T. Early Cryptology. <http://home.att.net/~mleary/history.htm>
12. National Security Agency, 2000. Codes and Ciphers. <http://www.otr.com/ciphers.html>
13. Klíma, V.: Utajené komunikace. In: Chip, 1994, č. 7, s. 138-141
14. Savard, J. J. G., 2000. Polygraphic Ciphers and Fractionation. <http://home.ecn.ab.ca/~jsavard/crypto/pp010302.htm>
15. Dupuy, P. J. Jr., Advancement of Learning. <http://fly.hiwaay.net/~paul/bacon/advancement/book6ch1.html>
16. Inventors museum, 1999. Thomas Jefferson. <http://www.inventorsmuseum.com/Jefferson.htm>
17. Klíma, V.: Utajené komunikace. In: Chip, 1994, č. 8, s. 118-121
18. Klíma, V.: Utajené komunikace. In: Chip, 1994, č. 9, s. 210-215
19. Klíma, V.: Utajené komunikace. In: Chip, 1994, č. 10, s. 216-221
20. The National Security Agency. The Enigma. <http://www.nsa.gov/museum/enigma.html>
21. Klíma, V.: Utajené komunikace. In: Chip, 1994, č. 11, s. 166-172
22. Příbyl, J., Kodl, J.: Ochrana dat v informatice. Praha: Vydavatelství ČVUT, 1996, 299 s., ISBN 80-01-01664-1
23. Klíma, V.: Utajené komunikace. In: Chip, 1995, č. 4, s. 136-138
24. Mára, L.: Save Our Souls. In: Chip, 1998, č. 10, s. 78
25. Klíma, V.: Utajené komunikace. In: Chip, 1995, č. 6, s. 174-175

26. Klíma, V.: DES sestřelen za 41 dní: Když zaútočí celá planeta. In: Chip, 1998, č. 4, s. 46-48
27. Klíma, V.: Představujeme kandidáty na AES: Šifra Rijndael. In: Chip, 1999, č. 11, s. 64-65
28. Klíma, V.: Zvítězil Rijndael. In: Chip, 2000, č. 11, s. 48-49
29. Huraj, L.: Vyučovanie Internetu na základnej škole. Bratislava: MC Bratislava, 1997, 56 s., ISBN 80-8052-022-4
30. Petty, G.: "Moderní vyučování", Praha: Portál, 1996, ISDN 80-7178-070-7
31. The Freemason Cipher. <http://www.mastermason.com/temple1/cipher.htm>
32. Chromčák, S, 2000. Šifrování pro děti. <http://www.fw.cz/ANCHOR/sifry/index.htm>
33. Zapletal, M.: Tisíc malých dobrodružství. II., Podzim - zima, Praha: SNDK, 1961
34. National Institute of Standards and Technology (NIST): Data Encryption Standard (DES), Federal Information Processing Standard (FIPS) PUB 46, 1988
35. Skynet, 2000. Úvod do kryptografie. <http://www.pgp.cz/uvod.html>
36. Janeček, J.: Odhalená tajemství šifrovacích klíčů minulosti. Praha: Naše vojsko, 1994, 184 s. ISBN 80-206-0462-6
37. Hönigová, A., Matyáš, V.: Anglicko-česká terminologie bezpečnosti informačních technologií. Praha: Computer Press, 1996, 95 s., ISBN 80-85896-44-3



## Príloha I

### Ukážka možného šifrovania správy k aktivite 3.1.1 Motivácia

Tieto vety možno použiť ako správu:

PRED STANOM SEDIA DVAJA ČERVENOKOŽCI

MALÝ JE SYNON VELKÉHO

VELKÝ NIE JE OTCOM MALÉHO

KTO JE VELKÝ ČERVENOKOŽEC

Rozlúštením obsahu správy je slovo MATKA.

Nasleduje spôsob rozdelenia do skupín aj s opisom šifrovania. Každý žiak dostane jednu časť správy: (Texty sú napísané tak, aby sa dali ľahko rozmnožiť.)

Skupina: KOMÁRE

Tvoja šifra: pred každé písmeno vlož nejaké (ľubovoľné) ďalšie dve písmená.

Teda tvoja veta

PRED STANOM SEDIA DVAJA ČERVENOKOŽCI

vyzerá zašifrovaná takto:

TAPHERSZETNDAUSEHTDJAMINLKOFCEM

GTSUIENKDOPIFGASFDGHVIRAJJOZPA

RAČTHEDFRBNVTYEKONLKOHGKJAORTŽUFCAI

Skupina: KOMÁRE

Tvoja šifra: pred každé písmeno vlož nejaké (ľubovoľné) ďalšie dve písmená.

Teda tvoja veta

MALÝ JE SYNON VELKÉHO

vyzerá zašifrovaná takto:

DAMDFAHULRTÝKOJRSEPTSATYMONUTOKLM

DSVRTETOĽDUKRYÉNAHJIO

Skupina: KOMÁRE

Tvoja šifra: pred každé písmeno vlož nejaké (ľubovoľné) ďalšie dve písmená.

Teda tvoja veta

VELKÝ NIE JE OTCOM MALÉHO

vyzerá zašifrovaná takto:

HUVDKEKOĽDAKDRÝSANOTIRHEKLJKLE

PROVNTAUCKLOTZMKOMTUACNLUAÉDBHATO

Skupina: KOMÁRE

Tvoja šifra: pred každé písmeno vlož nejaké (ľubovoľné) ďalšie dve písmená.

Teda tvoja veta

KTO JE VEĽKÝ ČERVENOKOŽEC

vyzerá zašifrovaná takto:

TUKDGTASONMJRYEOFVRSEKOLCHKIPÝ

SAČRTETURBMVORETSNREOHDKPTOSAŽHJEPUC

Skupina: LUPA

Tvoja šifra: písmená píš striedavo pod seba do 2 riadkov.

Teda tvoja veta

PRED STANOM SEDIA DVAJA ČERVENOKOŽCI

vyzerá zašifrovaná takto:

PESAOSDAVJČREOOC

RDTNMEIDAAEVNKŽI

Skupina: LUPA

Tvoja šifra: písmená píš striedavo pod seba do 2 riadkov.

Teda tvoja veta

MALÝ JE SYNONYM VEĽKÉHO

vyzerá zašifrovaná takto:

MLJSNMEKH

AÝEYOVLÉO

Skupina: LUPA

Tvoja šifra: písmená píš striedavo pod seba do 2 riadkov.

Teda tvoja veta

VEĽKÝ NIE JE OTCOM MALÉHO

vyzerá zašifrovaná takto:

VLÝIJOCMAÉO

EKNEETOMLH

Skupina: LUPA

Tvoja šifra: písmená píš striedavo pod seba do 2 riadkov.

Teda tvoja veta

KTO JE VEĽKÝ ČERVENOKOŽEC

vyzerá zašifrovaná takto:

KOEKČREOOE

TJVLÝEVNKŽC

Skupina: BEŽEC

Tvoja šifra: jedno písmeno daj na začiatok, ďalšie na koniec, potom ďalšie ako druhé, potom predposledné, potom tretie, ...

Teda tvoja veta

PRED STANOM SEDIA DVAJA ČERVENOKOŽCI

vyzerá zašifrovaná takto:

PESAOSDAVJČREOOČIŽKNVEAADIEMNTDR

Skupina: BEŽEC

Tvoja šifra: jedno písmeno daj na začiatok, ďalšie na koniec, potom ďalšie ako druhé, potom predposledné, potom tretie, ...

Teda tvoja veta

MALÝ JE SYNONYM VEĽKÉHO

vyzerá zašifrovaná takto:

MLJSNMEKHOOÉLVOYEÝA

Skupina: BEŽEC

Tvoja šifra: jedno písmeno daj na začiatok, ďalšie na koniec, potom ďalšie ako druhé, potom predposledné, potom tretie, ...

Teda tvoja veta

VEĽKÝ NIE JE OTCOM MALÉHO

vyzerá zašifrovaná takto:

VLÝIJOCAÉOHLMOTEEENKE

Skupina: BEŽEC

Tvoja šifra: jedno písmeno daj na začiatok, ďalšie na koniec, potom ďalšie ako druhé, potom predposledné, potom tretie, ...

Teda tvoja veta

KTO JE VEĽKÝ ČERVENOKOŽEC

vyzerá zašifrovaná takto:

KOEKČREOOECŽKNVEÝLVJT

*Ladislav Huraj*

**Nebojme sa šifrovania**

Vydalo Metodicko-pedagogické centrum v Bratislave  
s finančnou podporou  
Združenia na podporu vzdelávania EDUKÁCIA

Výkonná redaktorka *PhDr. Soňa Hronská*

Počet strán 50

Náklad 100

1. vydanie, 2002

**ISBN 80-8052-160-3**

**EAN 9788080521608**