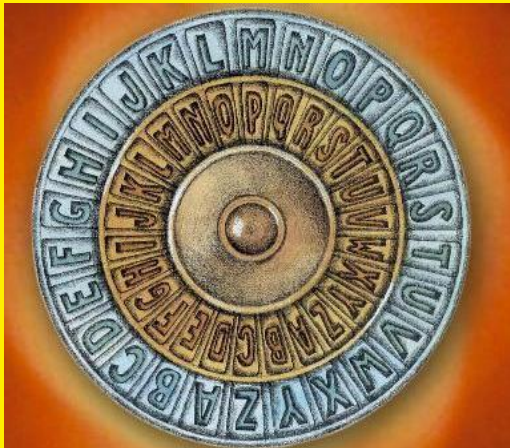


Dálnopisný stroj D-302 „Dalibor“
vyráběný ve Zbrojovce Brno



Kryptografie klasické šifry & historie



Pavel Vondruška, MFF UK Praha, CETIN a.s.

Chiffre de SULLY (1599)									
A	B	C	D	E	F	G	H	I	L
3	2	0	8	1	7	2	15	4	12
J	f	h	d	x	y	g	c	6	8
4	y	7	3	+	7	0	0	7	5
M	N	O	P	Q	R	S	T	U	X
1	3	1	1	3	1	1	3	1	1
6	8	5	7	4	18	6	9	2	2
9	g	h	d	x	y	g	c	6	8
10	4	y	7	3	+	7	0	0	7
V	W	X	Y	Z					
1	3	1	1	3					
6	8	5	7	4					
9	g	h	d	x					
10	4	y	7	3					
11	6	8	5	7					
12	9	g	h	d					
13	10	4	y	7					
14	11	6	8	5					
15	12	9	g	h					
16	13	10	4	y					
17	14	11	6	8					
18	15	12	9	g					
19	16	13	10	4					
20	17	14	11	6					
21	18	15	12	9					
22	19	16	13	10					
23	20	17	14	11					
24	21	18	15	12					
25	22	19	16	13					
26	23	20	17	14					
27	24	21	18	15					
28	25	22	19	16					
29	26	23	20	17					
30	27	24	21	18					
31	28	25	22	19					
32	29	26	23	20					
33	30	27	24	21					
34	31	28	25	22					
35	32	29	26	23					
36	33	30	27	24					
37	34	31	28	25					
38	35	32	29	26					
39	36	33	30	27					
40	37	34	31	28					
41	38	35	32	29					
42	39	36	33	30					
43	40	37	34	31					
44	41	38	35	32					
45	42	39	36	33					
46	43	40	37	34					
47	44	41	38	35					
48	45	42	39	36					
49	46	43	40	37					
50	47	44	41	38					
51	48	45	42	39					
52	49	46	43	40					
53	50	47	44	41					
54	51	48	45	42					
55	52	49	46	43					
56	53	50	47	44					
57	54	51	48	45					
58	55	52	49	46					
59	56	53	50	47					
60	57	54	51	48					
61	58	55	52	49					
62	59	56	53	50					
63	60	57	54	51					
64	61	58	55	52					
65	62	59	56	53					
66	63	60	57	54					
67	64	61	58	55					
68	65	62	59	56					
69	66	63	60	57					
70	67	64	61	58					
71	68	65	62	59					
72	69	66	63	60					
73	70	67	64	61					
74	71	68	65	62					
75	72	69	66	63					
76	73	70	67	64					
77	74	71	68	65					
78	75	72	69	66					
79	76	73	70	67					
80	77	74	71	68					
81	78	75	72	69					
82	79	76	73	70					
83	80	77	74	71					
84	81	78	75	72					
85	82	79	76	73					
86	83	80	77	74					
87	84	81	78	75					
88	85	82	79	76					
89	86	83	80	77					
90	87	84	81	78					
91	88	85	82	79					
92	89	86	83	80					
93	90	87	84	81					
94	91	88	85	82					
95	92	89	86	83					
96	93	90	87	84					
97	94	91	88	85					
98	95	92	89	86					
99	96	93	90	87					
100	97	94	91	88					
101	98	95	92	89					
102	99	96	93	90					
103	100	97	94	91					
104	101	98	95	92					
105	102	99	96	93					
106	103	100	97	94					
107	104	101	98	95					
108	105	102	99	96					
109	106	103	100	97					
110	107	104	101	98					
111	108	105	102	99					
112	109	106	103	100					
113	110	107	104	101					
114	111	108	105	102					
115	112	109	106	103					
116	113	110	107	104					
117	114	111	108	105					
118	115	112	109	106					
119	116	113	110	107					
120	117	114	111	108					
121	118	115	112	109					
122	119	116	113	110					
123	120	117	114	111					
124	121	118	115	112					
125	122	119	116	113					
126	123	120	117	114					
127	124	121	118	115					

Abychom si rozuměli

Kryptologii můžeme zjednodušeně označit jako vědu o utajení obsahu zpráv.

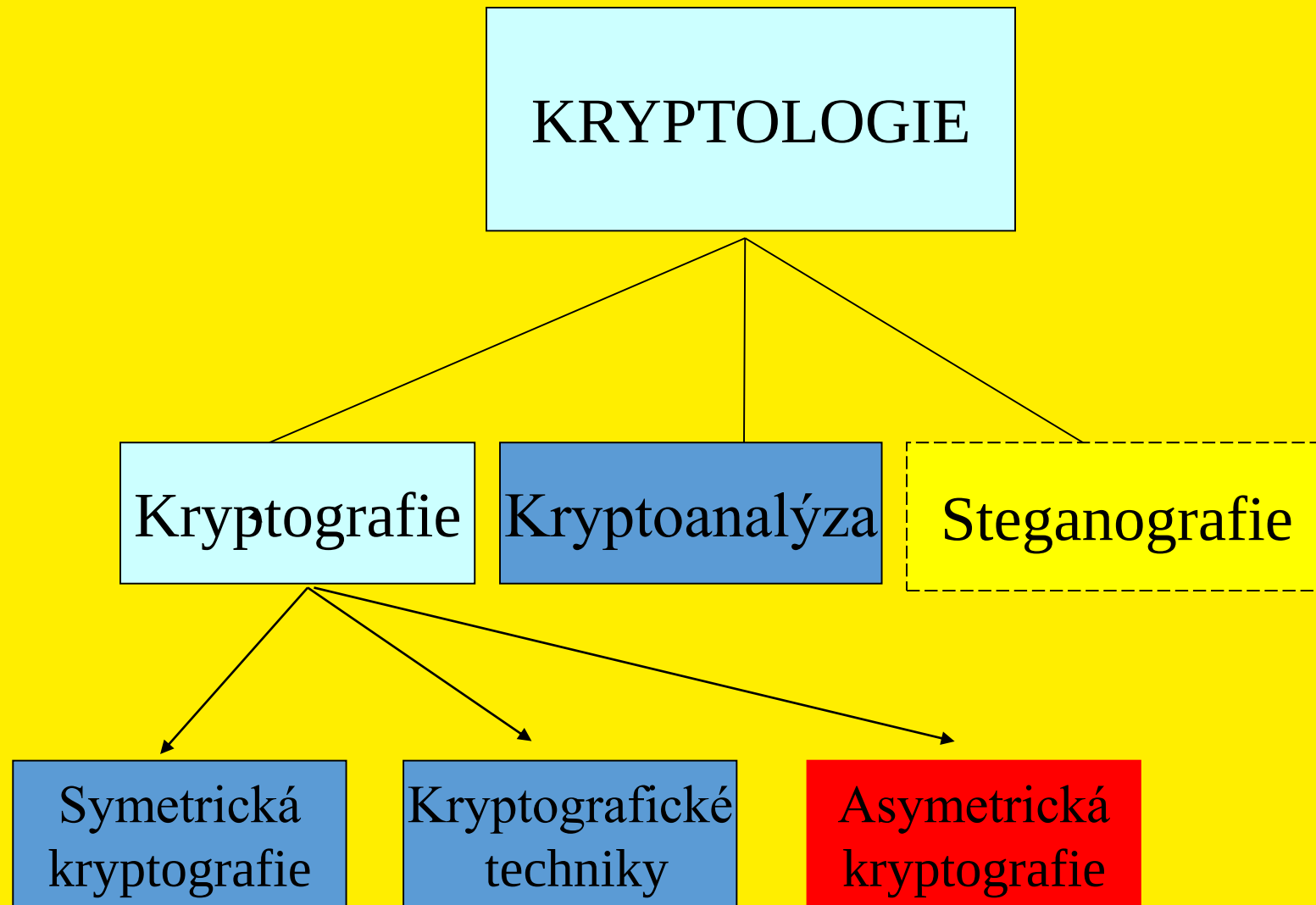
Kryptografie se zabývá matematickými metodami se vztahem k takovým **prvkům informační bezpečnosti**, jako je zajištění **důvěrnosti zprávy**, **integrity dat** (neporušenosti), **autentizace entit** (ověření subjektu) a **původu dat** (vlastnictví) – včetně zkoumání jejich silných stránek a slabin i odolnosti vůči různým metodám útoků.

Ve starším chápání to byla především věda o tom, jak navrhovat a používat šifrovací systémy, a tedy disciplína, která se zabývala převedením informace do podoby, v níž je tato informace skryta.

Jejím úkolem bylo tedy učinit výslednou zprávu nečitelnou i v situacích, kdy je plně prozrazená, zachycená třetí – nepovolanou stranou. Tím se liší od steganografie, jejímž úkolem je skrýt samotnou existenci zprávy

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

Kryptoanalýza je jakýsi "opak" kryptografie. Z toho plyne, že jedním z hlavních cílů je studium metod luštění šifrovacích systémů. Obecněji se kryptoanalýza zabývá analýzou odolnosti (síly) kryptografických systémů; a hledá metody vedoucí k proniknutí do těchto systémů.



Šifrový systém

Šifrový systém nebo také **šifrovací** či **kryptografický systém** je jakýkoliv systém, který lze použít ke změně textu nějaké zprávy s cílem učinit ji nesrozumitelnou komukoliv jinému s výjimkou adresáta, kterému je určena.

Otevřený text

Původní text zprávy, ještě před tím, než byl zašifrován, se nazývá **otevřený text** nebo **otevřená zpráva**.

Abeceda otevřeného textu / znak otevřeného textu

Abecedou nebo **znakem** v otevřeném textu rozumíme jakékoliv písmeno, číslici, interpunkční znaménko atd., které se mohou v otevřeném textu vyskytnout. **Řetězec** je jakákoliv posloupnost po sobě jdoucích znaků. **Délka řetězce** je počet znaků, které řetězec obsahuje.

Šifrová abeceda

Šifrová abeceda resp. **šifrové znaky** mohou být tvořeny abecedou otevřeného textu, ale mohou být tvořeny i jinými znaky.

Znaky šifrové abecedy vytváří řetězce (skupiny). Od poloviny 19.století je zvykem zapisovat šifrové znaky do skupin po pěti šifrových znacích. Zvyk souvisí s předáváním šifrových zpráv pomocí telegramů, kde se platilo za slovo. Průměrná délka slova v otevřeném textu je u většiny evropských jazyků 5 znaků otevřeného textu, a proto z důvodu platby bylo vyžadováno, aby i šifrový text byl členěn do skupin obdobné délky.

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

Dešifrování × luštění

Dešifrování

Dešifrování je opačný proces k šifrování. Jedná se o rekonstrukci původního otevřeného textu zprávy z šifrovaného textu pomocí domluvené kryptografické metody a znalosti příslušného klíče.

Dešifrování provádí zpravidla zamýšlený příjemce zprávy, který tuto zprávu dešifruje pomocí domluvené kryptografické metody a znalosti příslušného klíče. Bývá to většinou šifrant nebo šifréř. Může je však provádět i neoprávněná osoba, která se dostala k příslušnému klíči použitého šifrovaného systému. Klíč mohl být získán např. pomocí špionáže, ztrátou apod.

Luštění

Kryptoanalytici se snaží získat ze zašifrované zprávy její původní podobu – otevřený text. Cílem však může být i získání alespoň části skrytých informací.

Tento proces hledání se nazývá **luštění šifrované zprávy** a pokud je kryptoanalytik úspěšný a podaří se mu vniknout do některého šifrovaného systému, řekneme, že šifra byla **zlomena** nebo **rozbita**, slangově „**brejknuta**“ (z anglického break).

Šifry a kódy

Budeme rozlišovat mezi šiframi a kódy. Pomocí **šifry** nebo přesněji šifrovacího systému se odesílatel a adresát snaží utajit obsah zprávy před nepovolanou osobou. Smyslem **kódu** není zprávu utajit, ale upravit ji tak, aby ji bylo možné dále příslušným technickým prostředkem zpracovávat, např. přenést nějakým kanálem. Kódovaná zpráva tedy může být na základě znalosti příslušného kódování převedena zpět do původního tvaru.

Mezi nejznámější příklady kódu patří ASCII kód (A = 65) a Morseova abeceda (A = .-).... (čárové kódy EAN, binární kódy..)

Kód v kryptologii

V kryptologii má slovo kód také své místo. Vztahuje se k jednomu speciálnímu šifrovému systému, který pracuje s lingvistickými (jazykovými) prvky. Těmito prvky mohou být vybraná slova, celé věty nebo souvětí. Např. kód *vejce* může znamenat *granát*, kód *oko* může znamenat *chci se s tebou sejít* apod. Pokud je význam kódů veřejně známý (např. radiový Q-kód, kde QRX znamená *zavolám později*, QTC *mám pro vás telegram*), jedná se o kód v klasickém smyslu. Pokud je význam kódů utajen, jedná se o speciální šifrový systém...

Klíč / Klíčový prostor / Klíčové hospodářství

V minulosti se šifrovalo i velice jednoduchými metodami, kde bezpečnost často závisela pouze na utajení metody.

Např. bezpečnost Caesarovy šifry, která převádí otevřený text na šifrový tak, že každé písmeno otevřeného textu nahradí písmenem, který od něj leží o 3 místa dále v abecedě (details k této šifře najdete dále), je závislá na tom, zda je tento systém útočníkovi (osobě, která se snaží získat otevřený text, který pro ni není určen) znám nebo ne.

Podívejme se, co se stane, pokud bychom šifru jen nepatrně modifikovali např. tak, že posun při náhradě znaku otevřeného textu za znak šifrové abecedy by nebyl vždy 3 znaky vpravo jako u Caesarovy šifry, ale byl by různý.

Zjistíme, že situace se výrazně změnila, pokud luštitel konkrétní zprávu vyluští, nemá automaticky zajištěno, že lze další zprávy dešifrovat. (Klíč / parametr dané šifry...)

Pokud luštitel ví, jaký systém je použit, může najít správné řešení také tím, že postupně otestuje všechny klíče. Takovému postupu se říká **útok hrubou silou**. Je zřejmé, že kvalitní šifrové systémy musí být konstruovány (mimo jiné) tak, aby prostor všech klíčů byl tak velký, aby luštitel nebyl schopen je v rozumném čase všechny otestovat. Malá poznámka na závěr: domluvě na používání klíčů, jejich distribuci, výběru, způsobu zneplatnění atd. se říká **klíčové hospodářství**.

Kerckhoffsovy principy

Holandský kryptolog Auguste Kerckhoffs (1835-1903) vydal roku 1883 knihu *La Cryptographie Militaire* (Vojenská kryptografie).

(Kniha by byla významnou prací již pouze tím, že v ní Kerckhoffs publikuje metodu, jak rozluštit obecnou polyalfabetickou šifru s neperiodickým klíčem za předpokladu, že klíč byl použit vícekrát.)

Z hlediska vývoje kryptografie Kerckhoffsovu knihu proslavila především skutečnost, že hledal odpovědi na praktické problémy, které vyvstaly před kryptologií v nových podmínkách (masové nasazení polní šifry, potřeba šifrovat telegrafní zprávy, jednoduchost provozu). Autor v knize uvádí řadu požadavků, které by měl vojenský šifrovací systém splňovat. Tyto požadavky jsou známy jako tzv. Kerckhoffsovy principy.

Snad nejdůležitější zásadou, kterou lze z těchto principů snadno odvodit, je, že system musí odolat i za předpokladu, kdy protivník zná šifrovací systém a nezná pouze šifrovací klíče.

Ještě nyní se někdy aplikují přístupy, že se šifrovací algoritmy tají....

Hledá se BEZPEČNÁ šifra – Evropa 12.-13.století)

Princip využívaný princip je záměna znaků otevřeného textu znaky šifrové abecedy (šifra).

Cesta k substitučním šifrám v Evropě 12. a 13.století vedla nejprve přes **vlastní vývoj** v kláštorech

V benátském archívu je dochován spis z roku 1226, kde tečky nebo křížky nahrazují samohlásky v některých vybraných slovech. Fl.r-nc+-

Snaha zakrýt samohlásky v textu byla dále zdokonalena záměnnou samohlásek za jiná písmena.

PŘÍKLAD: A E I O U
 B D P G Q

Druhý princip, který byl použit k budování šifrového systému je užití kódu

-vznik kódů má svůj původ ve zkratkách a dále v magii, kde byly používány různé symboly s nejasným významem pro nezasvěcené

-Ve vatikánském archívu jsou doloženy první příklady využití (Egypt a Izrael použito jako označení pro dva italské státy)

Postupně byly znalosti doplněny studiem antické literatury (kniha Suetonia, kde se popisuje Caesarova a Augustova šifra).

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

Postupně byly znalosti doplněny studiem antické literatury (kniha Suetonia, kde se popisuje Caesarova a Augustova šifra).
znám vliv arabského světa.

A je zmapován i vliv hebrejských systémů (**ATBAŠ-ALBAM-ATBAH**)

Není znám vliv arabského světa.

Atbash, Albam e Atbah

Atbash

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

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
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

Atbah

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

11	10	9	8	7	6	5	4	3	2	1
ט	י	ט	ח	ז	ו	ה	ד	ג	ב	א
ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
12	13	14	15	16	17	18	19	20	21	22

Hledá se BEZPEČNÁ šifra – České království 15.století)

Pravděpodobně prvním dochovaným dokladem o používání šifer v Čechách jsou listy Mistra Jana Husa z Kostnice (1415).

Jeho šifrový systém byl velice jednoduchý, šifroval pouze samohlásky, a to tak, že je nahradil písmenem, které jej v abecedě následuje.

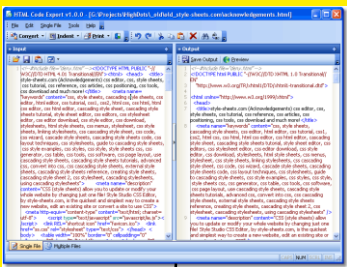
Místo A psal B, místo E napsal F atd.

Pro Boha ! je podle těchto pravidel zašifrováno jako PRP BPHB !

Hledá se odolná šifra proti frekvenční analýze – 14.století

Frekvence bigramů

EN	=	303
ST	=	277
NA	=	277
NI	=	254
NE	=	242
OV	=	235
AN	=	227
RA	=	226
PR	=	224
RP	=	6
CH	=	183
HC	=	1



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

The length of the plain text is 19571 letters.
Cipher Text Alphabet: **MIKULAS**BCDEFGHJNOPQRTVWXYZ
Plain Text Alphabet : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Frekvence trigramů

OVA	=	100
SIF	=	93
IFR	=	89
MEN	=	80
STI	=	71
VAN	=	66
PRO	=	65
EHO	=	65
OST	=	62
ROV	=	60
ENA	=	60
ENI	=	59
STA	=	58
STR	=	16

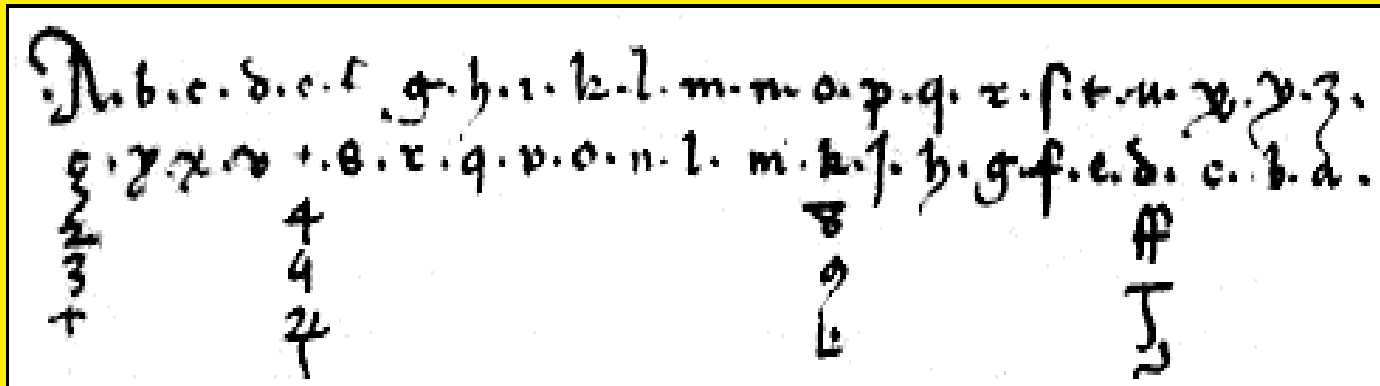
Frekvence znaků

A	=	195	1,00
B	=	425	2,17
C	=	1461	7,47
D	=	361	1,84
E	=	776	3,97
F	=	925	4,73
G	=	557	2,85
H	=	1290	6,59
I	=	285	1,46
J	=	1613	8,24
K	=	614	3,14
L	=	1958	10,00
M	=	1786	9,13
N	=	656	3,35
O	=	8	0,04
P	=	990	5,06
Q	=	1167	5,96
R	=	1027	5,25
S	=	103	0,53
T	=	680	3,47
U	=	650	3,32
V	=	809	4,13
W	=	18	0,09
X	=	31	0,16
Y	=	608	3,11
Z	=	578	2,95

Abū-Yūsuf Ya'qūb ibn Ishāq al-Kindīho (801–873)
X Evropa 14.století

Hledá se odolná šifra proti frekvenční analýze – 14.století

V polovině 14.století se jako přirozený výsledek tohoto snažení objevily homofonní šifry.



Homofonní šifra, kterou používal vévoda Simeone de Crema z Mantovy, z roku 1401.

Čistě homofonní šifry byly velmi brzy (na základě zkušeností s luštěním) nahrazeny novým velmi zajímavým systémem – **nomenklátorem**.

Nomenklátor 16.století

Nomenklátory z konce patnáctého století a začátku šestnáctého století již obsahují mimo klasické substituční homofonní záměny (na obrázku v odstavci označeném 1)

znaky pro zdvojená písmena (odstavec 2)

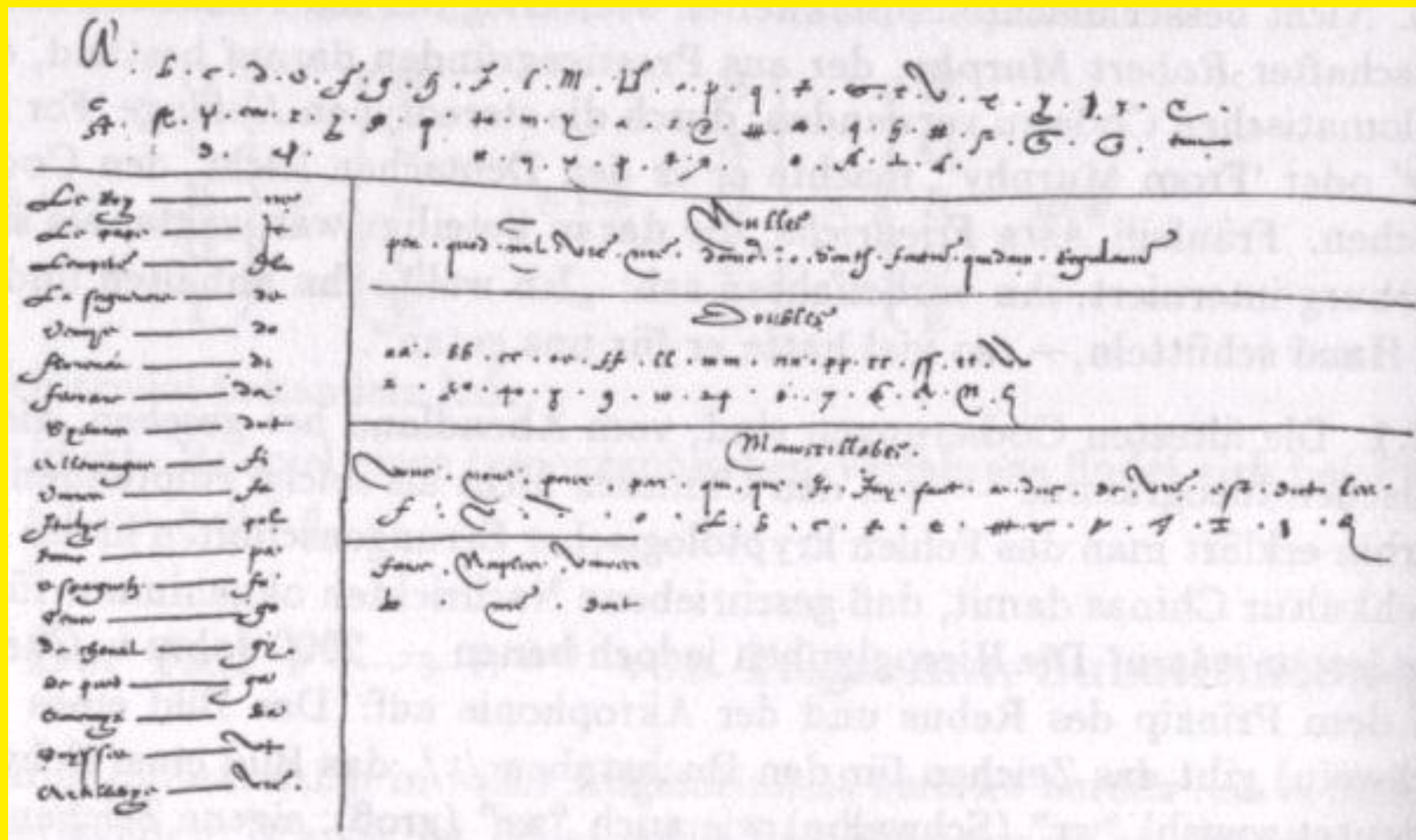
a slabiky (odstavec 3) a dále kódy pro nejfrekventovanější slova a jména (odstavec 4)

a klamače (druhý řádek odstavce 2)

(Klamače – nevýznamové skupiny písmen, které měly ztížit kryptoanalýzu zašifrovaných textů).



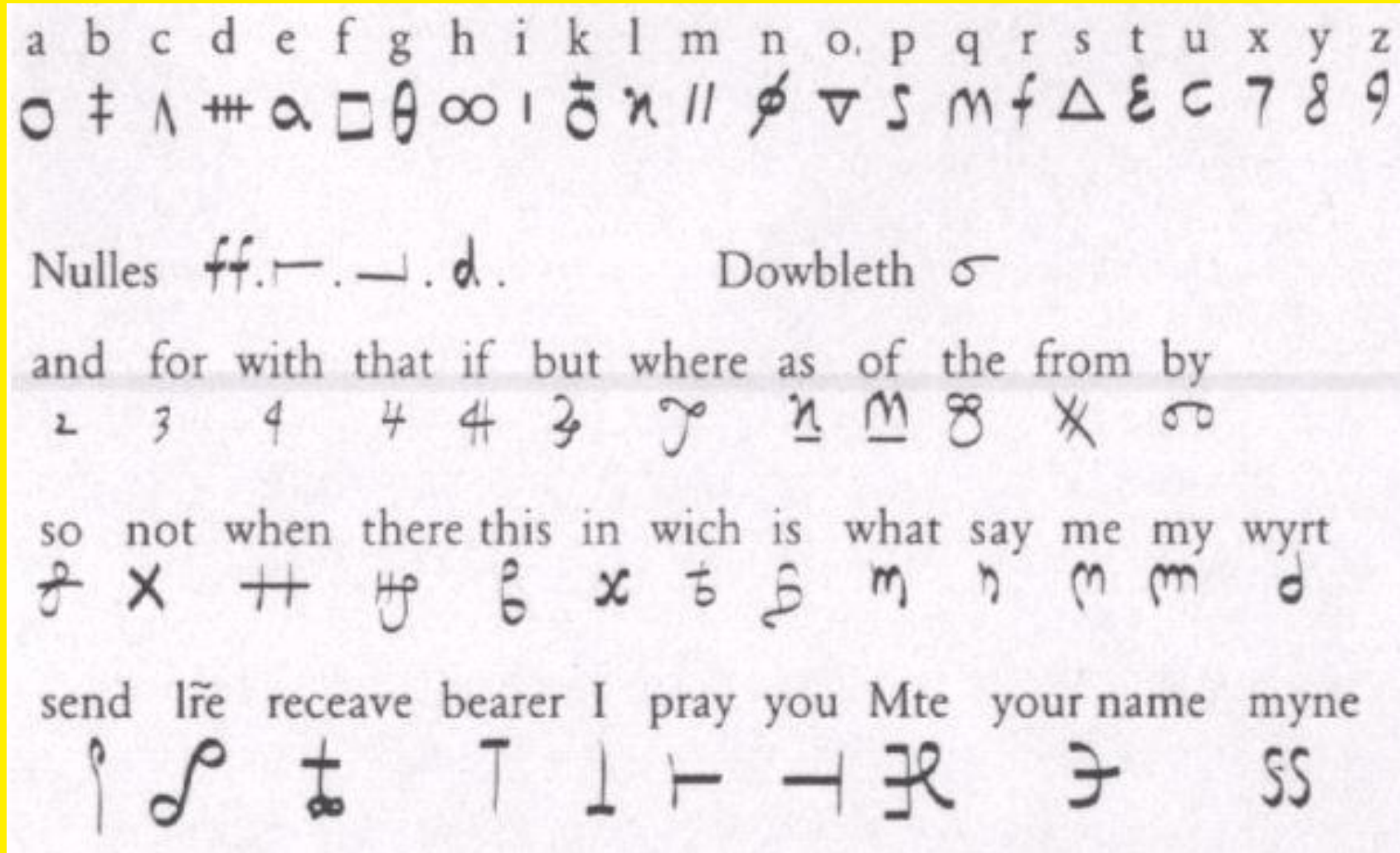
Hledá se odolná šifra proti frekvenční analýze – 16.století



Typický nomenklátor sestavený ve Florencii roku 1554, používaný za vlády **Cosimo de Medici**.

Osobní nomenklátor 17.století

Přepis osobního nomenklátoru skotské královny Marie Stuartovny (kolem roku 1600)



Doba nomenklátorů a jejich luštitelé - Francie

Ve Francii byl jedním z prvních kryptologů **Philibert Babou (1513-1570)**,
luštěním se zabýval i matematik **François Viète (1540-1603)**,

CODE de 1558																						Affaires Etrangères													
																						Correspondance du Roy Henri II													
																						avec Philibert Babou de la Bourdaisière, son Ambassadeur à Rome													
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X													
6	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3													
4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6													
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2													
n																																			
EE				FF				LL				MM				NN				PP				RR				SS							
4				R				3				m				2				7				>				2				3			
Nomenclature										Vocabulaire																									
l'église 7										con 6 le 2 que ne																									
Le Roy d'Espagne 2										de 2 qui 6																									
Monsi 1										ent 0 mais 3																									
Royne fff										est 8 ont 2 sa 2																									
Sa Sainteté le Pape D										et 2 par 4 si 4																									
Nulles										faire 7 pour 2																									
2 3 4 5 6 7 8										fait 2 nous 2 vous 2																									

CODE DE 1595 DE HENRI IV																						
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	sz	t	uv	y	
ð	n	x	a	x	h	m		⊖	ℓ	u	7	p	5	no	ff	##	h	4	3			
o		ϕ	ε	δ	u			†	q	2	do	g3			al	∞	a	q				
			u	=				w4					u				53	5				

⊖

groupe nul

ℓ

par

u

que

ð

vous

Ukázka nomenklátorů, které byly těmito muži prolomeny

....

Doba nomenklátorů a jejich luštitelé - Vatikán

Mateo zpracoval příručku o kryptologii. Ta obsahuje celou řadu nomenklátorů a shrnuje vše nejlepší z renesanční kryptologie, ale obsahuje jeho vlastní nápady a vylepšení.

- Zavedli použití slov pro zapamatování klíče, praxe se velmi rychle rozšířila
- qu sloučili v jediný znak
- zdvojená písmena začali psát jednoduše (sollemnis – solemnis)
- šifrový text (při jedno-dvoudílné záměně apod.) začali dělit na dvojice
- zavedli polyfony (šifrová slova, která mají více významů v otevřeném textu a je nutné je dosadit dle významu zprávy)
- důsledně používali klamače a to promyšleným způsobem
- nomenklátory sestavují pro jednotlivé země různé a vždy na základě rozboru (lingvistického a statistického) příslušného jazyka
- Popsali způsob řešení homofonní šifry pomocí vyhledávání „skoro opakování“

např.

11	3	16	87	29	96
11	3	16	46	29	96

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	X	Y	Z
3	20	8	11	7	2	15	4	12	16	1	13	17	5	19	14	18	6	9	22	21	10
J	f	g	h	d	x	y	g	g	c	b	f	n	y	m	.	m	c	q	o	l	
y	y	y	3	+	y	o	o	o	t	t	x	G	f	m	.	f	o	x	t	z	m

Doba nomenklátorů a jejich luštitelé - Francie

(Antoine Rossignol (*1.1.1600-?.12.1682), který od roku 1628 sloužil jako kryptolog nejprve u kardinálu Richelieu a později u krále Ludvíka XIII. a Ludvíka XIV. , ..)

Nomenklátory měly z hlediska kryptoanalýzy jednu "malou vadu" (přesněji řečeno vadu velkou). Pro rychlé vyhledávání byla slova řazena abecedně. Pokud kód bylo nějaké tří nebo vícemístné číslo (jak tehdy bylo běžným zvykem) a tato čísla byla také řazena vzestupně, znamenalo to, že luštitel mohl odhadnout, jakým písmenem začíná slovo, které kód představuje.

Atd.

le Roy	4	ayant	a,	il	9
le Pape	3	ans	b,	le	8
le Roy d'Espagne	2	argent	c,	la	7
l'Empereur	5	actendu	d,	lettre	6
le Grand Seigneur	6	actendant	e,	mois	5
la Royne d'Angleterre	7	après	f,	ment	4
le Roy d'Ecosse	8	buy	g,	mons	3
l'Archiduc d'Autriche	9	bon	h,	nous	2
l'Infante d'Espagne	10	beau	j,	nostre	1
les Etats des Pays-Bas	11	bailli	k,	nest	0
la Seigneurie de Venise	12	car	l,	non	9
le Roy du Danemark	13	convient	m,	ouverture	8
le Roy de Suède	14	cen	n,	occasion	7
les Cantons Suisses	15	contenant	o,	oultre	6
le duc de Savoye	16	donne	p,	obligation	5
le duc de Lorraine	17	dire	q,	pour	4
le duc de Guise	18	dont	r,	par	3
le prince Maurice	19	despeches	s,	pro	2
le comte d'Essex	20	dequoy	t,	parquet	1
le secrétaire GAYL	21	ent	u,	que	0
le secrétaire LEVISTON	22	encores	x,	qui	9
le sieur de BOISSIZE	23	et	y,	quoy	8
le sieur de BUZENVAL	24	entre	z,	quand	7
l'évêque de Glasco	25	faut	â,	quelle	6
France	26	fois	b,	reçu	5
Ecosse	27	foy	c,	réception	4
Flandres	28	grand	d,	reste	3
Hollande	29	gens	e,	sans	2
Angleterre	30	garde	f,	sinon	1
Suède	31	guesre	g,	selon	0
Danemark	32	hon	h,	S.M., V.M.	9
Lettres nulles :	Y, \$	hommes	i,	tout	8
Doublement :		hautes	l,	tant	7
venu	8,	heures	m,	toutefois	6
venant	9,	je	n,	tost	5
véritable	10	intention	o,	vous	4
vivs	11,	jay	p,	vostre	3

Doba nomenklátorů a jejich luštitelé - Francie

Protože si tuto slabinu A.Rossignol uvědomil, doporučil pro výrobu nomenklátorů pro „*státní*“ účely **promíchat** kódy.

Nomenklátory se pak musely začít vytvářet dva - jeden pro šifrování (výrazy seřazené „abecedně“) a druhý pro dešifraci (číselné kódy seřazené vzestupně, „abecedně“ nebo podle jiného vhodného kritéria).

Díky tomuto opatření se mohly nomenklátory (resp. kódová část) dále rozšiřovat.

Kódová část začala mít až desítky tisíc výrazů....

A TO BYL VLASTNĚ I KONEC DOBY NOMENKLÁTORŮ, které byly nahrazeny KÓDOVOU KNIHOU.

Leon Battista Alberti (první polyalfabetický šifrový systém)



1404-1472, všestranně nadaný, stavitel, varhaník, básník, filozof,
...

na podnět papežského tajemníka Leonarda Data se na sklonku
života začal zabývat utajováním zpráv

25 stránková práce

Otec západní kryptologie

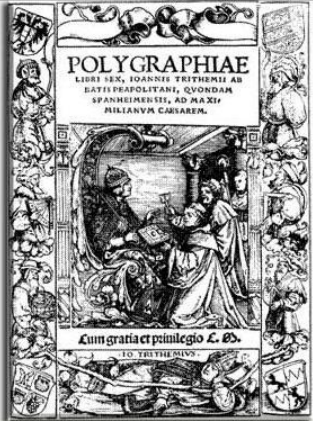
Albertiho disk - otáčením se zajišťoval
výběr příslušné šifrové abecedy.

Alberti doporučuje posunout abecedy
vždy po třech nebo čtyřech slovech.

3 mezníky:

- Luštění na základě frekvencí (systematický výklad)
- Polyalfabetický šifrový systém (pomůcka)
- zašifrování kódů

Johannes Trithemius 1452-1516 (tabula recta)



The title page illustration from Johannes Trithemius' 1518 "Polygraphiae libri sex" shows the author wearing his Benedictine habit and kneeling to present his book to the Holy Roman Emperor Maximilian.

1 ABCDEFGHIJKLMNOPQRSTUVWXYZ
 2 BCDEFGHIJKLMNOPQRSTUVWXYZA
 3 CDEFGHIJKLMNOPQRSTUVWXYZAB
 4 DEFGHIJKLMNOPQRSTUVWXYZABC
 5 EFGHIJKLMNOPQRSTUVWXYZABCD
 6 FGHIJKLMNOPQRSTUVWXYZABCDE
 7 GHIJKLMNOPQRSTUVWXYZABCDEF
 8 HIJKLMNOPQRSTUVWXYZABCDEFG
 9 IJKLMNOPQRSTUVWXYZABCDEFGH
 10 JKLMNOPQRSTUVWXYZABCDEFGHI
 11 KLMNOPQRSTUVWXYZABCDEFGHIJ
 12 LMNOPQRSTUVWXYZABCDEFGHIJK
 ...
 24 XYZABCDEFGHIJKLMNPOQRSTUVWXYZ
 25 YZABCDEFGHIJKLMNPOQRSTUVWXYZ
 26 ZABCDEFGHIJKLMNPOQRSTUVWXYZ

1508 **Polygraphia** (6 dílů)

Vytištěna 1518

Ave Maria (písmenům přiřazena slova)

Vydávána a přepisována po celá
staletí (1620 de Hotting)

O K O

O L Q

5 díl – „Tabula recta“

*Šest knih o polygrafii od Johanna Trithemia, opata z Würzburgu, dříve ze Spanheimu
věnované císaři Maxmiliánovi*

Giovanniho Battisty Belasa (zavedení klíče)

Italský šlechtic ,1513 **La cifra**, rozvinul práce Albertiho a Trithemia

- Zavedl **tajný klíč** pro volbu abecedy (dohoda na pořadí využití abeced)
- Klíč : slovo, věta

Girolamo Cardano

1501-1576, milánský fyzik a matematik

Chorobná touha získat popularitu, vydal 131 knih a 111 zůstalo v rukopise

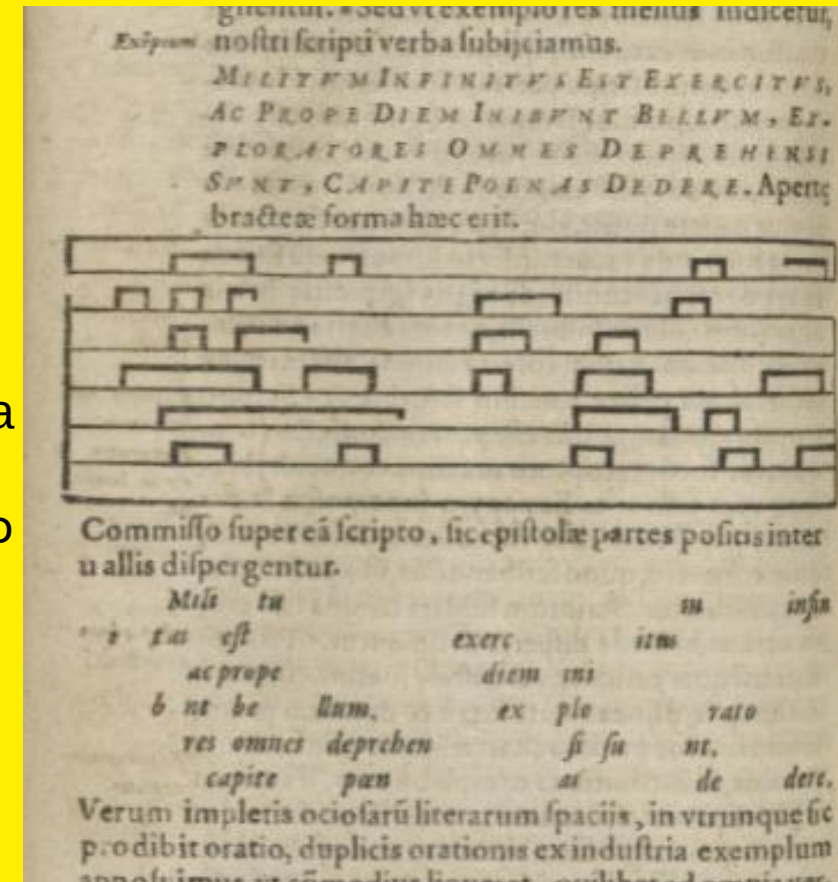
Ve dvou spisech zabývajících se popularizací vědy **De Substiliate** (1550) a **De Rerum Varietate Libri XVII** (1557) se věnuje i kryptologii, vtipné, zajímavé, anekdotické příběhy, bohaté ilustrace. Překládány a vydávány po celé Evropě.

- Cardanova mřížka

-Uvědomil si význam hesla pro bezpečnost polyalfabetických šifer

- **Změna hesla před každou zprávou !**

- zavádí pojem autoklíč , neformuluje dokonale



Blaise de Vigenère 1523-1596

1586 - *Traicté des chiffres*
(*Pojednání o šifrách*) (600 stran).

Díky systému, který zde představil, se natrvalo zapsal mezi nejznámější kryptology.

A	ABCDEFGHIJKLMNOPQRSTUVWXYZ
B	BCDEFGHIJKLMNOPQRSTUVWXYZA
C	CDEFGHIJKLMNOPQRSTUVWXYZAB
D	DEFGHIJKLMNOPQRSTUVWXYZABC
E	EFGHIJKLMNOPQRSTUVWXYZABCD
F	FGHIJKLMNOPQRSTUVWXYZABCDE
G	GHIJKLMNOPQRSTUVWXYZABCDEF
H	HJKLMNOPQRSTUVWXYZABCDEFG
I	IJKLMNOPQRSTUVWXYZABCDEFGH
J	JKLMNOPQRSTUVWXYZABCDEFGHI
K	KLMNOPQRSTUVWXYZABCDEFGHIJ
L	LMNOPQRSTUVWXYZABCDEFGHIJK
M	MNOPQRSTUVWXYZABCDEFGHIJKL
N	NOPQRSTUVWXYZABCDEFGHIJKLM
O	OPQRSTUVWXYZABCDEFGHIJKLMN
P	PQRSTUVWXYZABCDEFGHIJKLMNO
Q	QRSTUVWXYZABCDEFGHIJKLMNOP
...	
W	WXYZABCDEFGHIJKLMNOPQRSTU
X	XYZABCDEFGHIJKLMNOPQRSTUV
Y	YZABCDEFGHIJKLMNOPQRSTUVW
Z	ZABCDEFGHIJKLMNOPQRSTUVWXY

Pasáže zabývající se okultními vědami, výrobou zlata, kabalou, černou magií.

Obsahuje cenné informace o šifrách (přesné citace, přesný výklad).

Systematicky se zabýval polyalfabetickými šiframi a ve svém výkladu uvedl vše, co bylo do té doby na tomto poli vykonáno.

Udává různé výběry abeced z Trithemiova čtverce (abecedy mohou být i přeházené), za sebou, podle hesla (např. báseň), definuje již správně autoklíč (včetně předání jeho počátku)

Klíč:

OKNOOKNO

Otevřený text:

ALBATROS

Šifrový text:

QVOOHBBG

Gaspar Schott (systém Gronsfeld)

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

Německý kryptolog Gaspar Schott (1608-1666) vydává v roce 1665 knihu *Schola steganographica*.

-zjednodušení (čísla, 10 abeced) vedlo k vyšší rychlosti a menší chybovosti

-oblíbený ještě ve 20.století používán (galérka)

Klíč:

5297 352973520

Otevřený text:

DNES NEPRIJDU

Šifrový text:

IPNZ QJRAPMIW

A	ABCDEFGHIJKLMNOPQRSTUVWXYZ
B	BCDEFGHIJKLMNOPQRSTUVWXYZA
C	CDEFGHIJKLMNOPQRSTUVWXYZAB
D	DEFGHIJKLMNOPQRSTUVWXYZABC
E	EFGHIJKLMNOPQRSTUVWXYZABCD
F	FGHIJKLMNOPQRSTUVWXYZABCDE
G	GHIJKLMNOPQRSTUVWXYZABCDEF
H	HIJKLMNOPQRSTUVWXYZABCDEFG
I	IJKLMNOPQRSTUVWXYZABCDEFGH
J	JKLMNOPQRSTUVWXYZABCDEFGHI
K	KLMNOPQRSTUVWXYZABCDEFGHIJ
L	LMNOPQRSTUVWXYZABCDEFGHIJK
M	MNOPQRSTUVWXYZABCDEFGHIJKL
N	NOPQRSTUVWXYZABCDEFGHIJKLM
O	OPQRSTUVWXYZABCDEFGHIJKLMN
P	PQRSTUVWXYZABCDEFGHIJKLMNO
Q	QRSTUVWXYZABCDEFGHIJKLMNOP
...	
W	WXYZABCDEFGHIJKLMNOPQRSTUV
X	XYZABCDEFGHIJKLMNOPQRSTUVW
Y	YZABCDEFGHIJKLMNOPQRSTUVWX
Z	ZABCDEFGHIJKLMNOPQRSTUVWXY

Giovanni Sestri (Beaufortova varianta Vigenérový šifry, Sestri- Beuafort)

1710 - Ital Giovani Sestri

Úprava Vigenérova systému...

Popsaný systém byl v 19.století pojmenován
podle obdobného systému admirála Beuforta (se
kterým se někdy zaměňuje)

Klíč: PAVELPAV
Otevřený text: ALBATROS
Šifrový text: ELGWICOX

Svět chce šifrovat

1. Morseovka

Samuel F. B. Morse vynalezl a patentoval v roce 1840 telegraf.

2. Černé komnaty

1844 – Anglie

1848 – Francie, Rakousko-Uhersko (Geheime Kabinetts-Kanzlei)

Paradoxně si teprve nyní lidé začali o své soukromí více zajímat.

3. Ochrana telegrafních zpráv

Francis O. J. Smith vydal komerční telegrafní kód pod názvem *The Secret Corresponding Vocabulary; Adapted to Morse's Electro-Magnetic Telegraph* (Slovník tajného dopisování upravený pro použití ve spojení s Morseovým elektromagnetickým telegramem). Obsahuje i 67 vět.

Vychází další a další rozsáhlejší telegrafní kódy až se 100 000 položkami.

4. Poznámka k dělbě šifer na pětice

1. července 1904 vstoupily v platnost v Anglii nové telegrafní předpisy. Mimo jiné obsahují požadavek, že šifrový text musí být předáván ve skupinách po pěti znacích.

Francis Beaufort (systém Beaufort)

Angličan, admirál sir Francis Beaufort (1774-1857) – nabídl „lidem“ jednoduchý, levný způsob šifrování telegrafních zpráv.

Prodej – tabulka, návod na obsluhu a doporučení na tvoření hesel.

A	ABCDEFGHIJKLMNOPQRSTUVWXYZ
B	BCDEFGHIJKLMNOPQRSTUVWXYZA
C	CDEFGHIJKLMNOPQRSTUVWXYZAB
D	DEFGHIJKLMNOPQRSTUVWXYZABC
E	EFGHIJKLMNOPQRSTUVWXYZABCD
F	FGHIJKLMNOPQRSTUVWXYZABCDE
G	GHIJKLMNOPQRSTUVWXYZABCDEF
H	HJKLMNOPQRSTUVWXYZABCDEFG
I	IJKLMNOPQRSTUVWXYZABCDEFGH
J	JKLMNOPQRSTUVWXYZABCDEFGHI
K	KLMNOPQRSTUVWXYZABCDEFGHIJ
L	LMNOPQRSTUVWXYZABCDEFGHIJK
M	MNOPQRSTUVWXYZABCDEFGHIJKL
N	NOPQRSTUVWXYZABCDEFGHIJKLM
O	OPQRSTUVWXYZABCDEFGHIJKLMN
P	PQRSTUVWXYZABCDEFGHIJKLMNO
Q	QRSTUVWXYZABCDEFGHIJKLMNOP
...	
W	WXYZABCDEFGHIJKLMNOPQRSTU
X	XYZABCDEFGHIJKLMNOPQRSTUV
Y	YZABCDEFGHIJKLMNOPQRSTUVW
Z	ZABCDEFGHIJKLMNOPQRSTUVWXY

Klíč: PAVELPAV
 Otevřený text: ALBATROS
 Šifrový text: RPUEYMD

Porovnání systémů

Šifrování

Tritheim, Cardano Vigenére, Gronsfeld			Beaufort			Beaufortova varianta Vigenérova systému	
	O(1)			Š(3)			Š(3)
			Beaufort				
K(2)	Š(3)		O (1)	K(2)		K(1)	O(2)

Dešifrování

Tritheim, Cardano Vigenére, Gronsfeld			Beaufort			Beaufortova varianta Vigenérova systému	
	O(3)			O(3)			Š(1)
K(1)	Š(2)		Š (1)	K(2)		K(2)	O(3)

Porovnání systémů

Francouz de Viaris (1847-1901), vlastním jménem Marquis Gaetan Henri Leon Viarizio di Lesegno) publikoval v roce **1888** v odborném časopise *Le Génie Civil* dvoudílný příspěvek, který později vyšel jako kniha pod názvem *Cryptographie*. Příspěvek je cenný tím, že pomocí vzorců osvětlil konstrukci dříve uvedených polyalfabetických systémů.

Zavedl označení pro libovolný znak šifrového textu jako řecké písmeno χ (chí), libovolný znak klíče Γ (gama) a libovolný znak otevřeného textu písmeno c . Následně dokázal, že algebraický vzorec $c + \Gamma = \chi$ popisuje Vigenérovo šifrování, a to samozřejmě bez ohledu na to, jak je technicky realizováno (tabulkou, kryptografickým proužkem, šifrovacím kotoučem).

Použijeme-li dnes běžnější značení (K znak klíče, O znak otevřeného textu a $\check{S}$ znak šifrového textu), pak vzorce jednoznačně popisující nejpoužívanější polyalfabetické systémy jsou:

systém	šifrování	dešifrování
Vigenére	$O + K = \check{S} \ (c + \Gamma = \chi)$	$\check{S} - K = O$
Beaufort	$K - O = \check{S}$	$K - \check{S} = O$
Varianta Beaufort	$O - K = \check{S}$	$\check{S} + K = O$

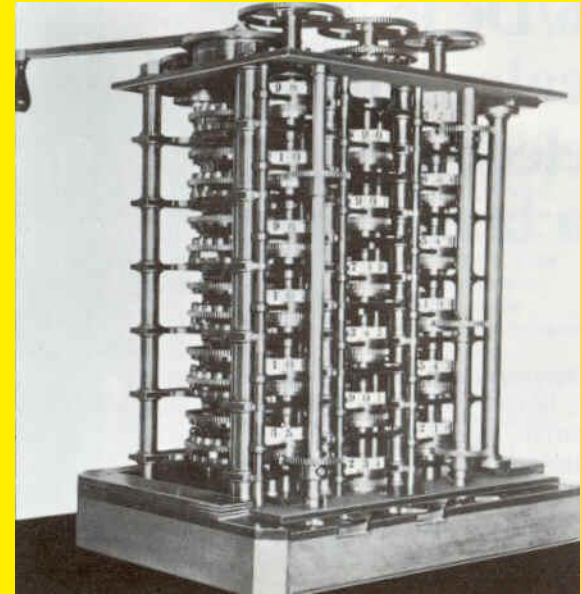
Pád polyalfabetických šifrových systémů

Charles Babbage (1791-1871), výstřední profesor matematiky. Difference Engine No.1 a No.2 (mechanické výpočetní stroje, programovatelné instrukce..)

-Jeho nejvýznamnější kryptoanalytický výsledek však pochází pravděpodobně z roku 1854. **Podařilo se mu najít obecný postup řešení Vigenérova šifrového systému s periodickým heslem, a to na základě analýzy vzdálenosti mezi opakováními v šifrovém textu.** Tento objev nebyl publikován, později byl nalezen v jeho poznámkách.

Friedrich Wilhelm Kasiski

Důstojník pruské armády Friedrich Wilhelm Kasiski zveřejnil roku **1863** v knize *Die Geheimschriften und die Deschiffirkunst* (Tajné šifry a umění je dešifrovat) **obecnou metodu na řešení Vigenérovky polyalfabetické šifry** (s periodickým heslem) pomocí vyhledání periody hesla a následným zredukováním na řešení řady monoalfabetických šifer.



Happy End

Gilbert S. Vernam

1917, Gilbert S. Vernam, zaměstnanec americké firmy AT&T, vymyslel polyalfabetický šifrovací stroj schopný používat náhodný neopakující se kód.

Do zařízení se vkládala děrná páska s otevřeným textem a současně i děrná páska, na které byl náhodně vyděrovaný klíč (heslo). Šifrový text vznikl sečtením (**odečtením**) příslušných bitů obou pásek mod 2.

Velkou výhodou zařízení bylo, že proces šifrování a dešifrování probíhal úplně stejně a automaticky (systém One Time Pad).

Claud Elwood Shannon

Happy End

V časopise *Bell System Technical Journal* vyšly dvě práce dalšího z velikánů kryptologie dvacátého století Clauda Elwooda Shannona. Práce otiskuje časopis v roce 1948 a 1949, jedná se o články "Matematická teorie sdělování" a "Sdělovací teorie tajných systémů".

Prvý z článků dal vznik teorii informací, druhý článek pojednával o kryptologii v termínech informační teorie. Pojetí nadbytečnosti (redundancy) je hlavním termínem, který Shannon zavedl.

Díky této teorii se podařilo dokázat, že systém navržený Gilbert S. Vernamem, který „vyrostl“ z polyalfabetických šifrových systémů je *bezpečný kryptosystém (tzv. absolutně bezpečný šifrový systém)*.

Podmínky:

- Heslo musí být náhodné, delší než otevřený text, použité pouze jednou
- Heslo musí být stejně pravděpodobné
- Heslo musí být nepředvídatelné

Dodnes je tento způsob šifrování jediným známým absolutně bezpečným systémem.

Použití – československý šifrátor Šifrovací stroj ŠD – 3



*Dálnopisný stroj D-302 „Dalibor“
vyráběný ve Zbrojovce Brno*



Šifrovací stroj ŠD – 3 byl vyvinut na Zvláštní správě Ministerstva vnitra ČSR v letech 1958 až 1960 a byl následně vyráběn v 1. spojovací základně Ministerstva národní obrany v Hradci Králové. Celkem bylo v několika sériích vyrobeno 815 kusů tohoto zařízení. Byl používán od roku 1962 a v armádě měl uplatnění až do začátku osmdesátých let minulého století. Jako záložní spojovací prostředek byl veden ještě v roce 1985.

Použití

Modifikace systému byla v praxi používána v době studené války tajnými službami (BND, CIA apod.).

Otevřený text se nejprve převedl do číselné podoby a to zpravidla pomocí **jedno-dvoumístné číselné záměny**.

Následovalo přičtení dohodnuté číselné sekvence – hesla.

V závěrečné ukázce použijeme originální převodovou tabulku používanou západoněmeckou tajnou službou **BND** (Bundes Nachrichten Dienst) během studené války.

Použití

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

Tabulka se podle „konstrukčního hesla“ nazývala DEIN STAR (tvá hvězda)

- Otevřený text (o):
- Převod do mezinárodní abecedy:
- Převod podle tabulky (O):
- Rozpis do pětímístných skupin:
- Heslo (K):
- Vigenére (O + K = Š):

Děkuji za pozornost.
DEKUJI ZA POZORNOST
0 1 57 63 62 2 69 8 61 60 69 60 9 3 60 4 7
01576 36226 98616 06960 93604 7
75409 78210 87302 10834 52019 3
76975 04436 75918 16794 45613 0

Děkuji za pozornost

kybersoutez@kybersoutez.cz

pavel.vondruska@crypto-world.info