Spolufinancováno Evropskou unií

Ministerstvo životního prostředí

UNIVERZITA J.E. PURKYNĚ V ÚSTÍ NAD LABEM

OSVĚTOVĚ ODBORNÝVZDĚLÁVACÍ PROGRAM V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

vzdělávací akce realizovaná v rámci projektu

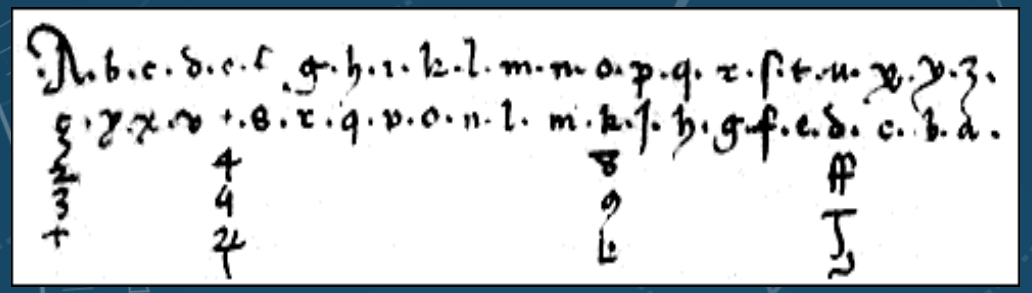
CZ.10.02.01/00/22_002/0000210, Aktivita KA1_B.3.10

RUR – Region univerzitě, univerzita regionu

Centrum kybernetické bezpečnosti

RUR - Region univerzitě, univerzita regionu
reg. č. CZ.10.02.01/00/22_002/0000210

RUR

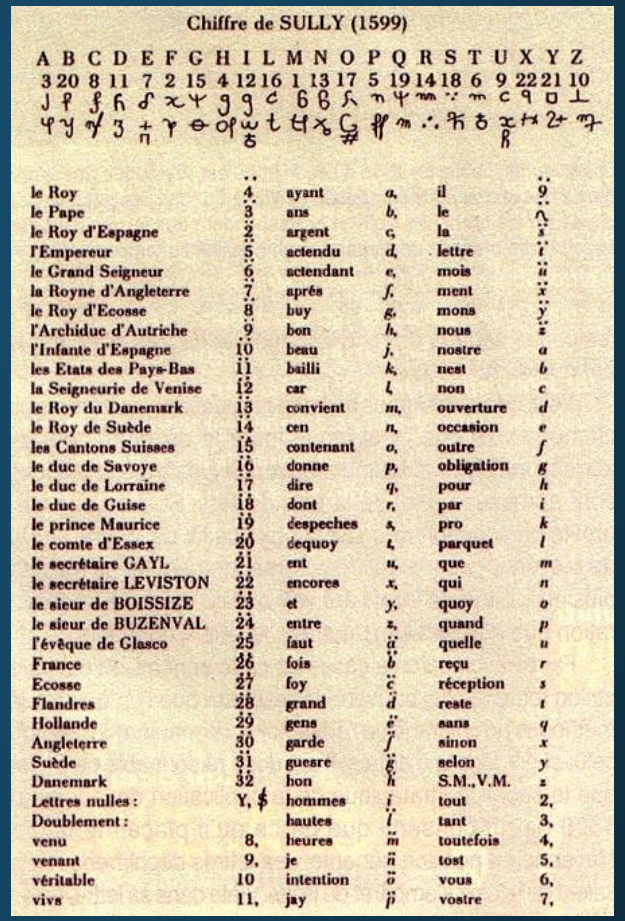


http://crypto-world.info/informace/usti.pptx

KRYPTOLOGIE, ŠIFROVÁNÍ A TAJNÁ PÍSMA

PAVEL VONDRUŠKA

MFF UK Praha, KYBERCENTRUM



ABYCHOM SI ROZUMĚLI ….

Kryptologii můžeme zjednodušeně označit jako vědu o utajení obsahu zpráv.

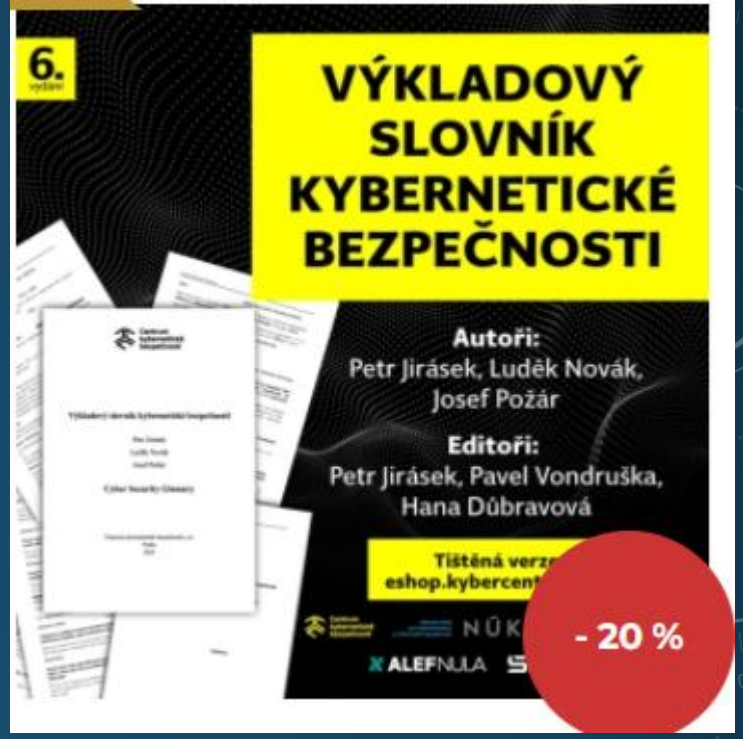
Kryptografie se zabývá matematickými metodami se vztahem k takovým **prvkům informační bezpečnosti**, jako je zajištění **důvěrnosti zprávy**, **integrity dat** (neporušenosti), **autentizace entit** (ověření subjektu) a **původu dat** (vlastnictví) – včetně zkoumání jejich silných stránek a slabin i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



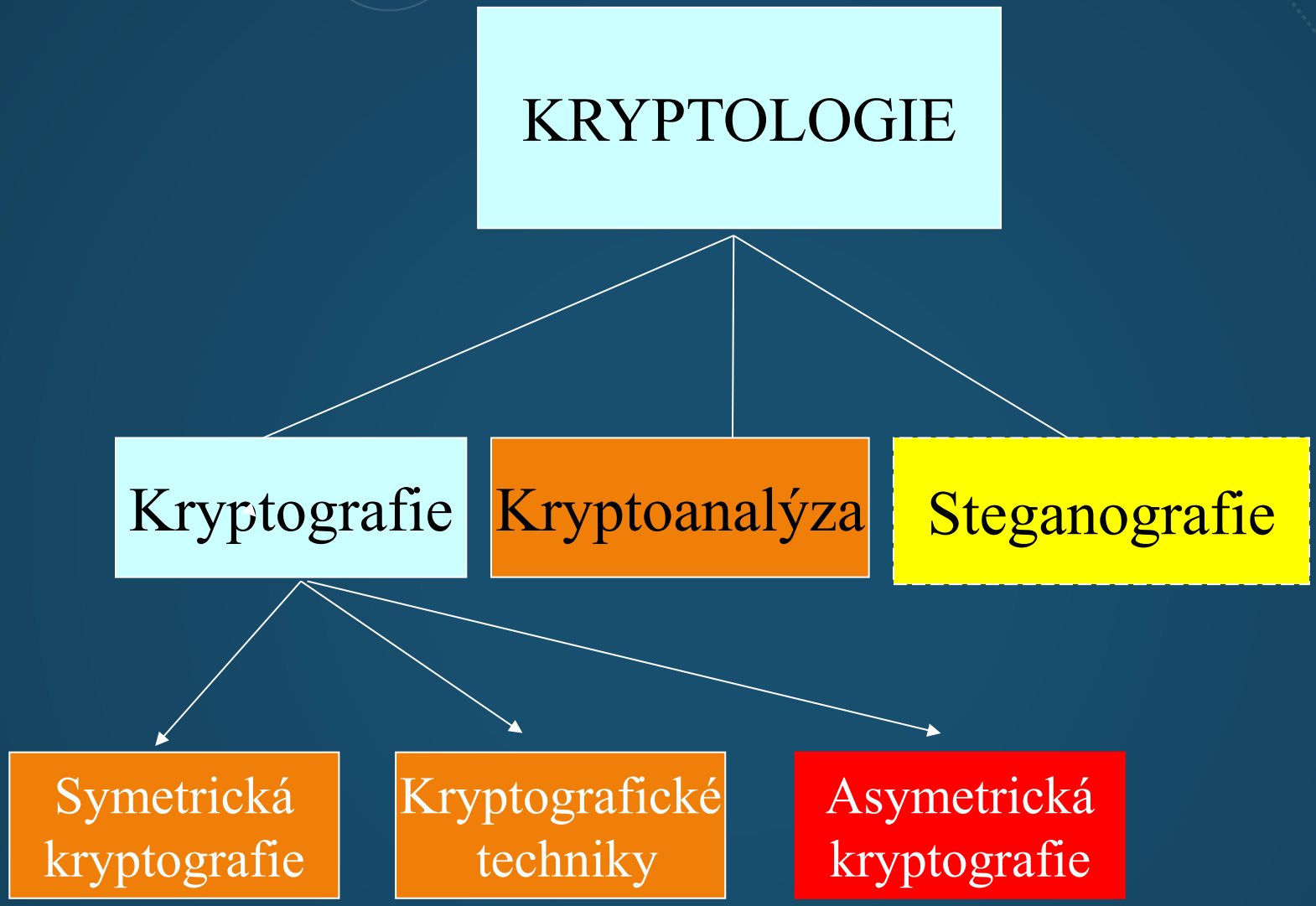
Otevřený text

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.

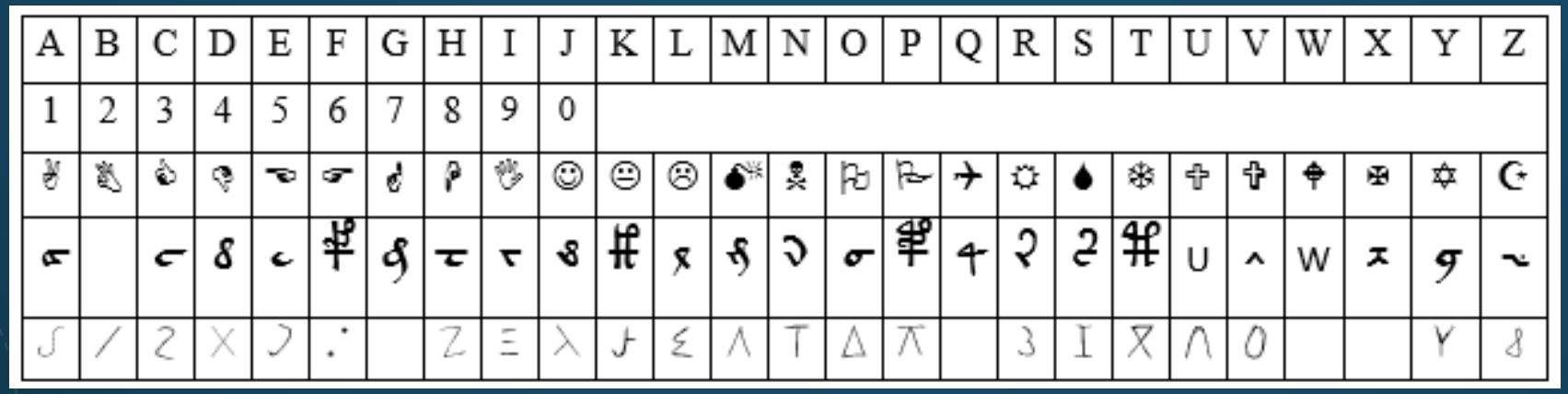
věda o utajení obsahu zpráv



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.



Dešifrování × luštění

Dešifrování

Dešifrování je opačný proces k šifrování. Jedná se o rekonstrukci původního otevřeného textu zprávy z šifrového 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 šifrér. Může je však provádět i neoprávněná osoba, která se dostala k příslušnému klíči použitého šifrového 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 šifrové zprávy** a pokud je kryptoanalytik úspěšný a podaří se mu vniknout do některého šifrového 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 (detaily 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.

Jen malá poznámka na závěr: domluvě na používání klíčů, jejich distribuci, výběru, způsobu zneplatnění atd. se říká **klíčové hospodářství.**

1883

Holandský kryptolog Auguste Kerckhoffs (1835-1903) vydal 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).

V knize formuloval Auguste Kerckhoffs zásadu, že šifrovací systém nesmí vyžadovat utajení a musí být schopna bez potíží padnout do rukou nepřítele.
Jde o druhý ze šesti požadavků na vojenské šifry, konkrétně požaduje, že bezpečnost šifry musí spočívat v klíči, nikoliv v utajení samotného algoritmu.

Caesarova 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	Z	A	B	C

A potom se každé písmeno zprávy zaměnění za písmeno, které leží o tři místa dále v abecedě.

K záměně lze také s výhodou použít převodovou tabulku.

MUNDUS VULT DECIPI PXQGXV YXOW GHFLSL

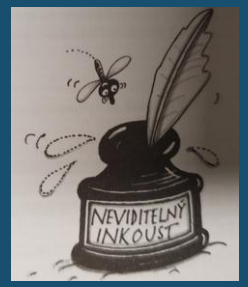
Augustův systém - verze Caesarovy šifry

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

B C D E F G H I K L M N O P Q R S T V X AA

MUNDUS VULT DECIPI (svět chce být klamán)

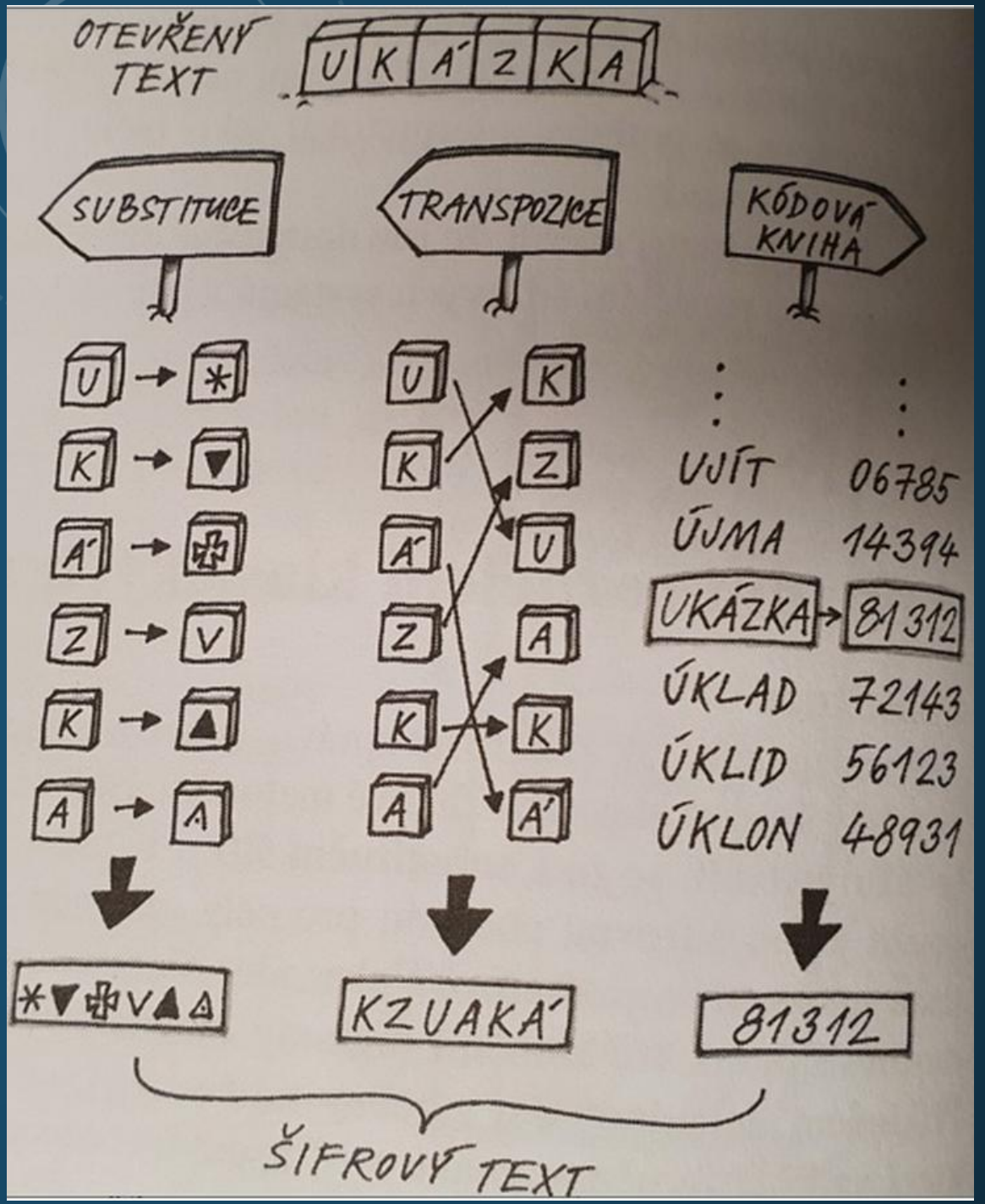
NXOEXT XXMV EFDKQK



Šifra **Atbash**

Samotný název „Atbash“ (v hebrejštině **אתבש**) je vlastně návodem, jak šifru vytvořit:

- **A** (Alef - 1. písmeno) → **T** (Tav - poslední písmeno)
- **B** (Bet - 2. písmeno) → **Sh** (Shin - předposlední písmeno)



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 klášterech

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 prvé příklady využití (Egypt a Izrael použito jako označení pro dva italské státy)

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

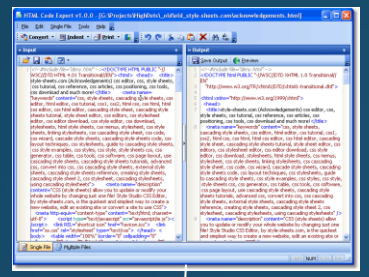
Pro Boha ! je podle těchto pravidel zašifrováno jako PRP BPHB !

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
```



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

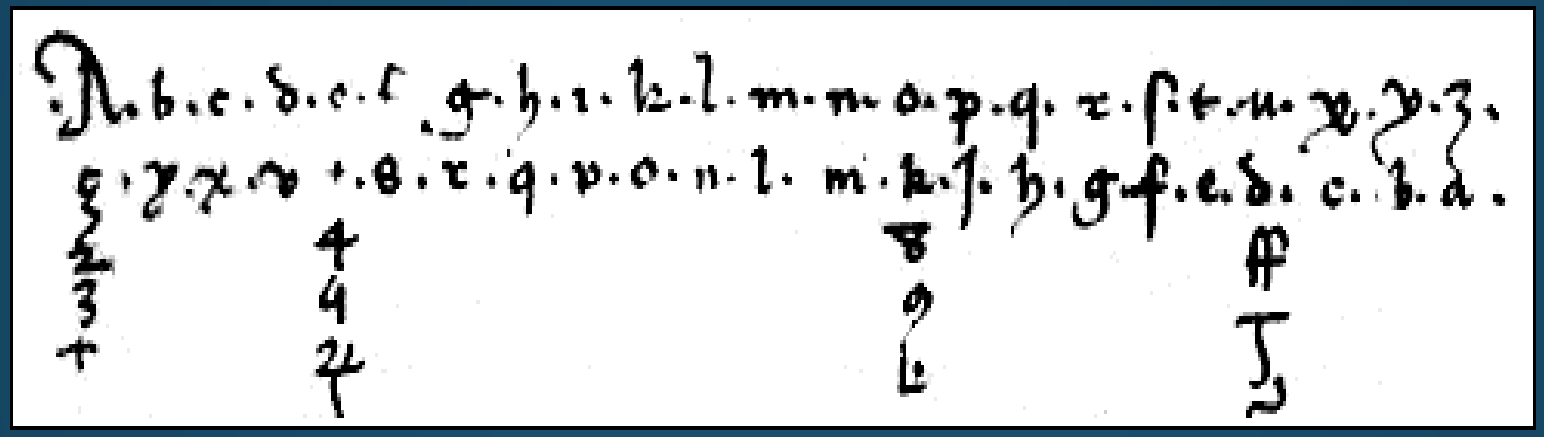
A =	195	1,00
B =	425	2,17
C =	1461	7,47
D =	361	1,84
E =	776	3,97
F =	925	4,73
G =	557	2,85
H =	1290	6,59
I =	285	1,46
J =	1613	8,24
K =	614	3,14
L =	1958	10,00
M =	1786	9,13
N =	656	3,35
O =	8	0,04
P =	990	5,06
Q =	1167	5,96
R =	1027	5,25
S =	103	0,53
T =	680	3,47
U =	650	3,32
V =	809	4,13
W =	18	0,09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

```
The length of the plain text is 19571 letters.
Cipher Text Alphabet: MIKULASBCDEFGHJNOPQRTVWXYZ
Plain Text Alphabet : ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

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 Simone de Crema, profesionální šifrér působící ve službách rodu **Gonzagů** v Mantově. Představuje jeden z důležitějších milníků v dějinách kryptografie. Jde o první (známý) systematický pokus o překonání frekvenční analýzy.

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

NOMENKLÁTOR 16.STOLETÍ

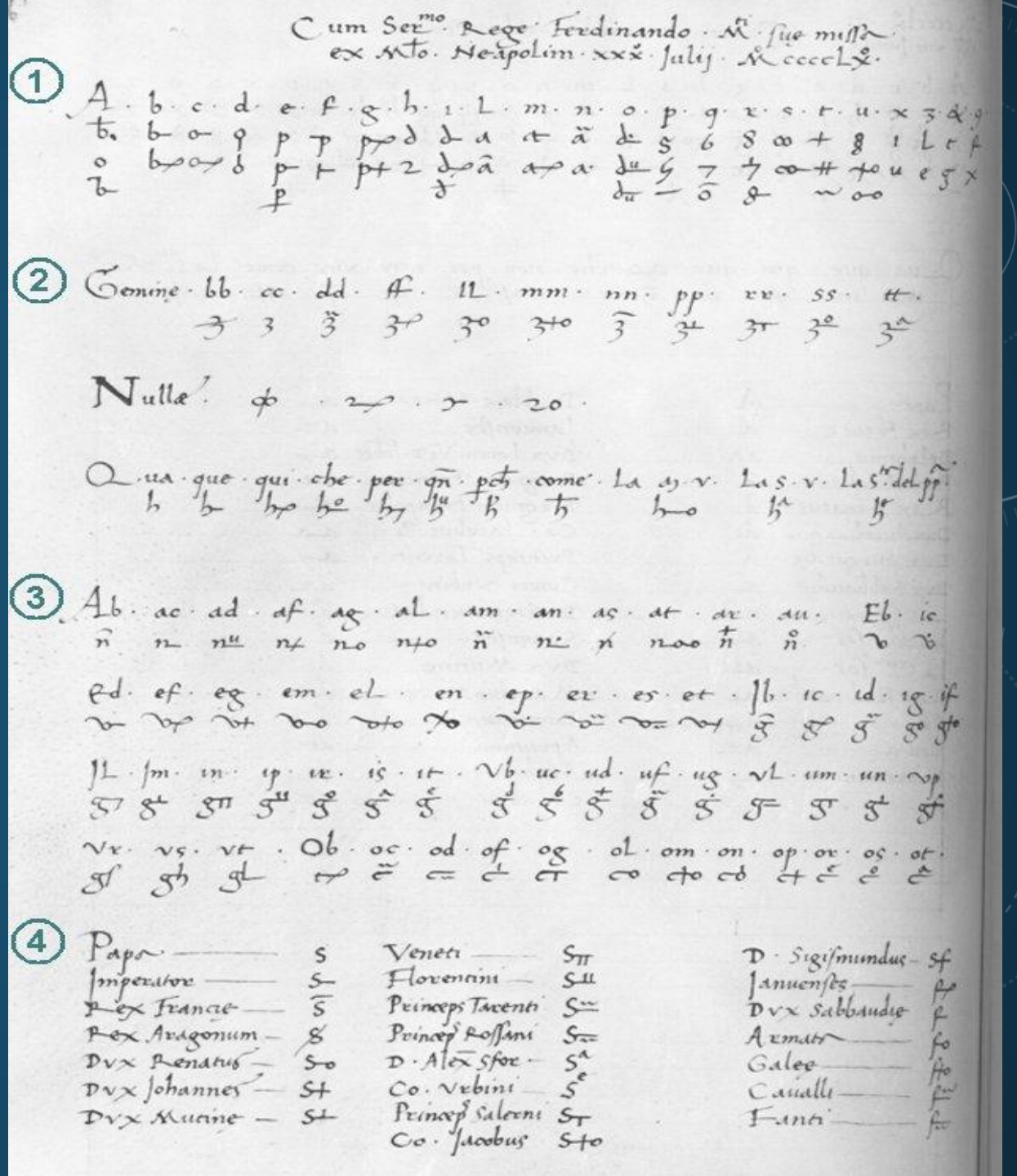
Nomenklátory z konce patnáctého století a začátku šestnáctého století již obsahují mimo klasické substituční homofonní záměny (na obrázku v odstavci označeném 1)

znaky pro zdvojená písmena (odstavec 2)

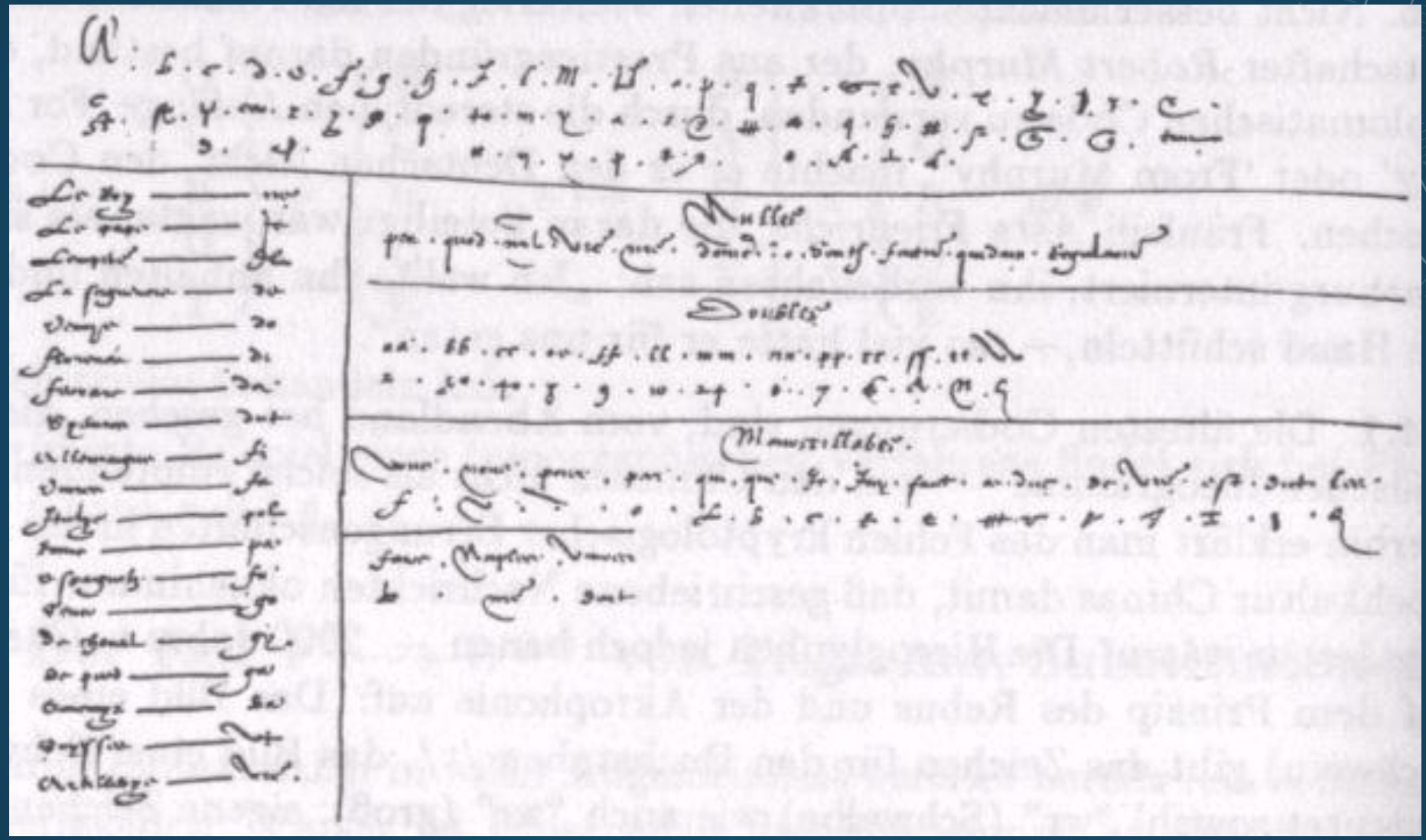
a slabiky (odstavec 3) a dále kódy pro nejfrekventovanější slova a jména (odstavec 4)

a klamače (druhý řádek odstavce 2)

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



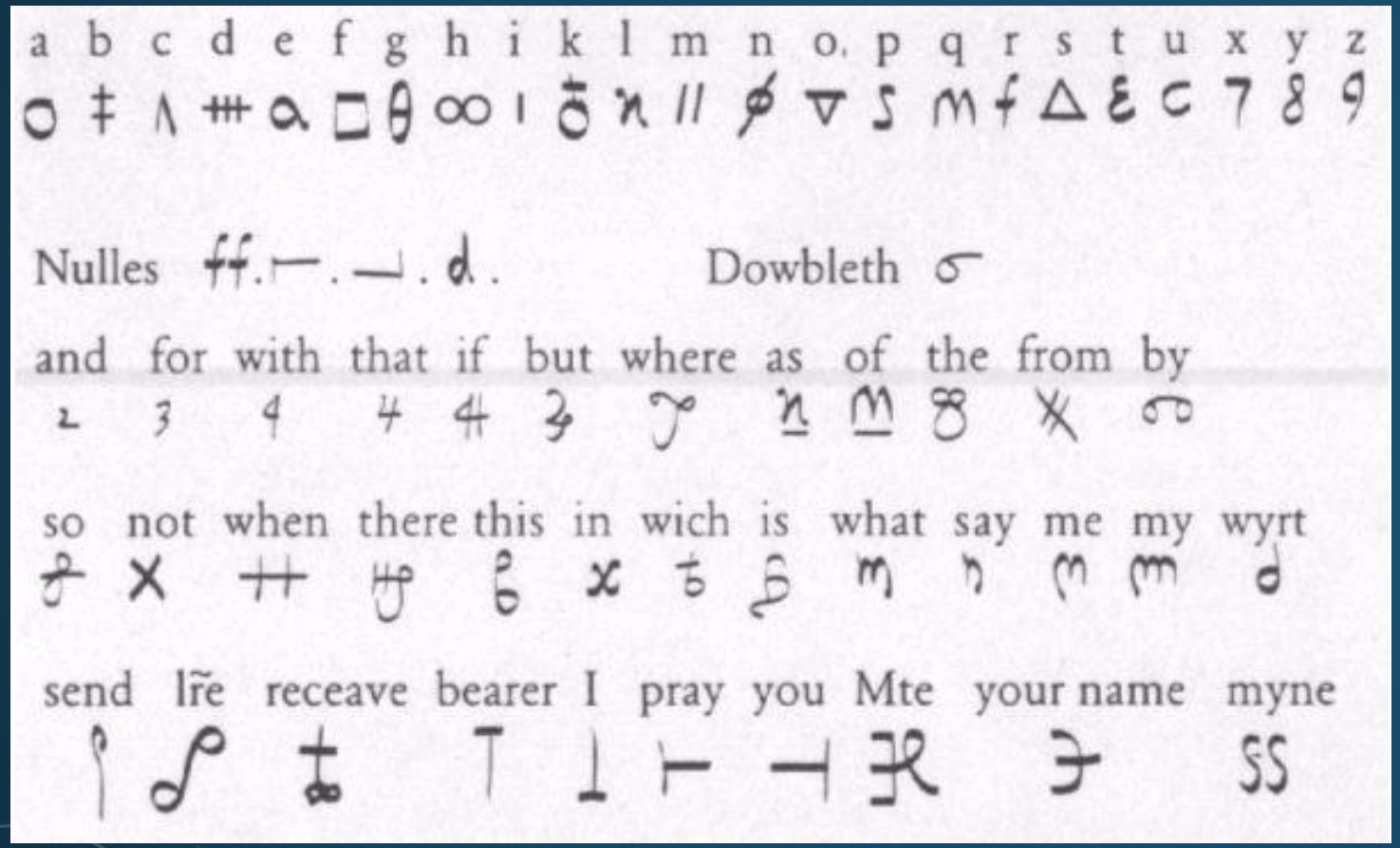
HLEDÁ SE ODOLNÁ ŠIFRA PROTI FREKVENČNÍ ANALÝZE – 16.STOLETÍ



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

OSOBNÍ NOMENKLÁTOR 16.STOLETÍ

Přepis osobního nomenklátoru skotské královny Marie Stuartovny



Prolomení nomenklátoru (v roce 1586)

Provedl Alžbětin šéfšpion sir Francis Walsingham a jeho kryptolog Thomas Phelippes.
Dopisy se jim podařilo zachytit, přečíst a následně podvrženými informacemi Marii ještě více kompromitovat. (Phelippes k dešifrovanému dopisu, který ji byl pak doručen, připsal padělanou žádost, aby Marie odhalila jména ostatních spiklenců....)

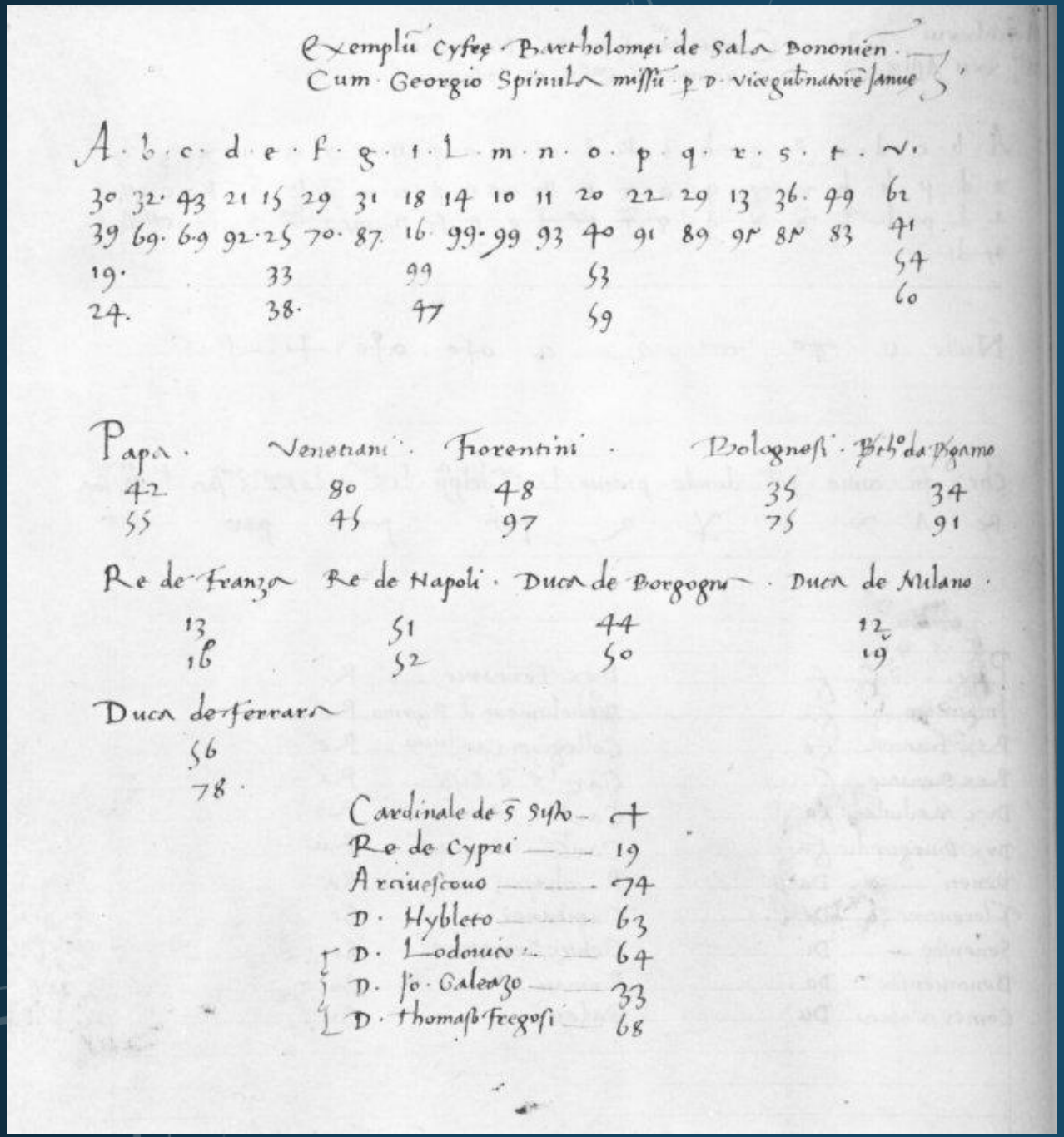
Usvědčení ze zrady vedlo k odsouzení a následné popravě 8. února 1587.

DOBA NOMENKLÁTORŮ A JEJICH LUŠTITELÉ - BENÁTKY

Malý nomenklátor benátského dóžete **Michele Stena** z roku 1411 (dóže 1400 - 1413)

Malý – (piccolo) v té době neznamenal slabý, ale spíše **kapesní/pohotovostní**

Benátčané jako první zavedli systémovou správu klíčů:
Archivace: Každý nomenklátor byl pečlivě očíslován a uložen v archivech Rady deseti (Capi dei Dieci).
Pravidelná obměna: Benátky si uvědomovaly, že i nejlepší šifra se časem „opotřebuje“ (protivník ji může odposlechnout nebo ukrást), proto klíče pravidelně měnily.



Doba nomenklátorů a jejich luštitelé - Miláno

Milán byl v té době (stejně jako Benátky) špionážní velmocí. Simonetta vytvořil v Miláně státní šifrovou kancelář, která byla efektivní, že dokázala číst zprávy většiny ostatních italských st

Cicco Simonetta napsal první vědecké pojednání o dešifrování Evropě.
Liber notes reverendi domini Cicchi Simonette (v překladu: Kn záznamů důstojného pána Cicca Simonetty). Dokončeno 4. července 1474.
Na rozdíl od předchozích autorů, kteří psali o tom, jak šifry tvo se Simonetta zaměřil na to, jak je luštit (kryptoanalýza).

Ukázka je ze sbírky šifer **milánského úředníkaFrancesca Tanchredina** (1470-1480, Sbírka obsahuje více než **150 různých nomenklátorů**.

DOBA NOMENKLÁTORŮ A JEJICH LUŠTITELÉ - VATIKÁN

Mateo Argenti zpracoval příručku o kryptologii (**Traktát o šifrách** (*Trattato del modo di cifrare*). 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“

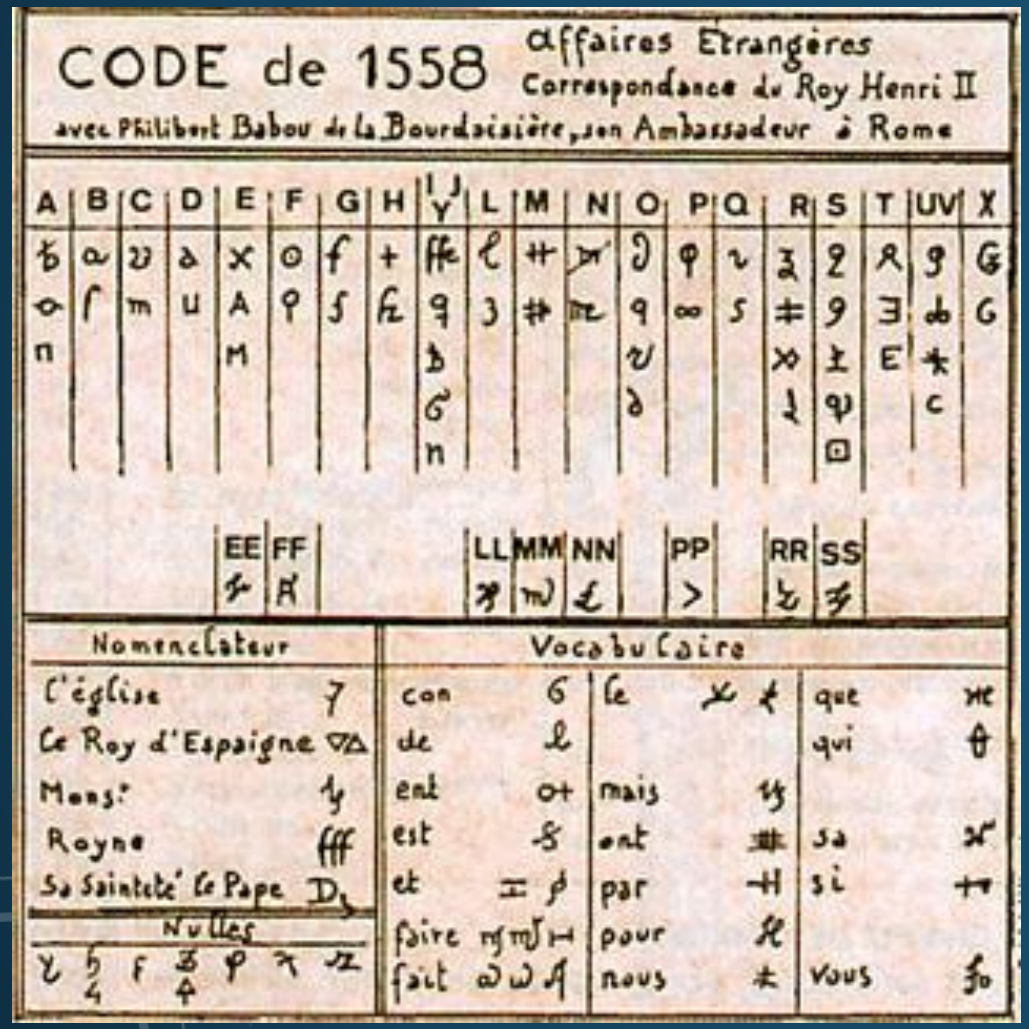
např. 11 3 16 **87** 29 96

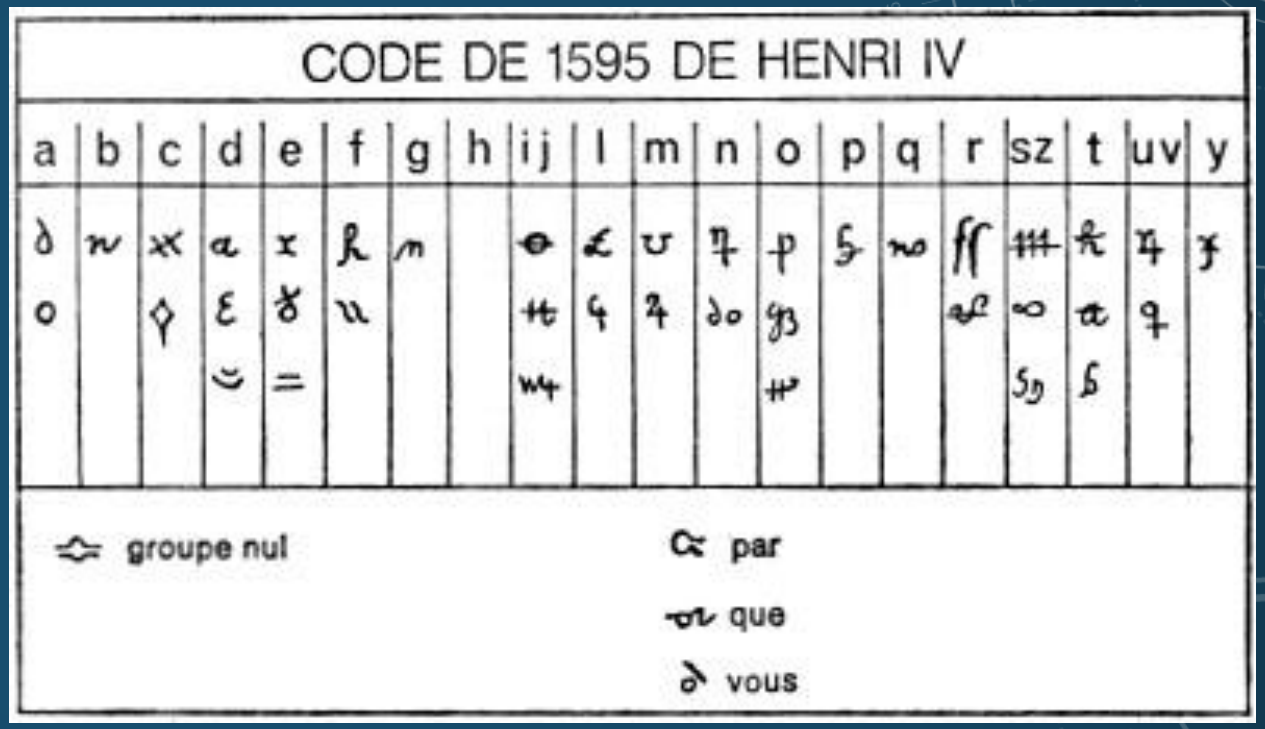
11 3 16 **46** 29 96

DOBA NOMENKLÁTORŮ A JEJICH LUŠTITELÉ - FRANCIE

Ve Francii byl jedním z prvních kryptologů **Philibert Babou (1513-1570)**,

luštěním se zabýval i matematik **François Viete** (1540-1603),





Ukázka nomenklátorů, které byly těmito muži prolomeny ….

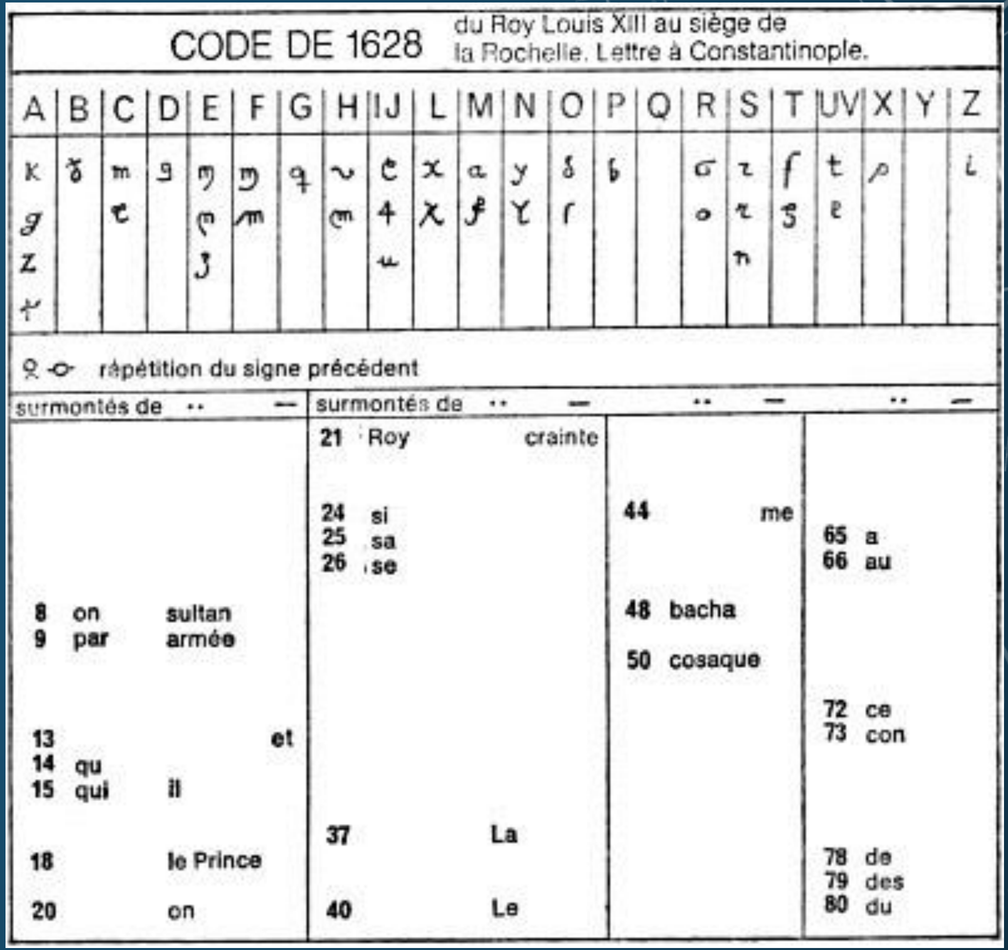
DOBA NOMENKLÁTORŮ A JEJICH LUŠTITELÉ - FRANCIE

Bezesporu nejvýznamnějším byl **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.

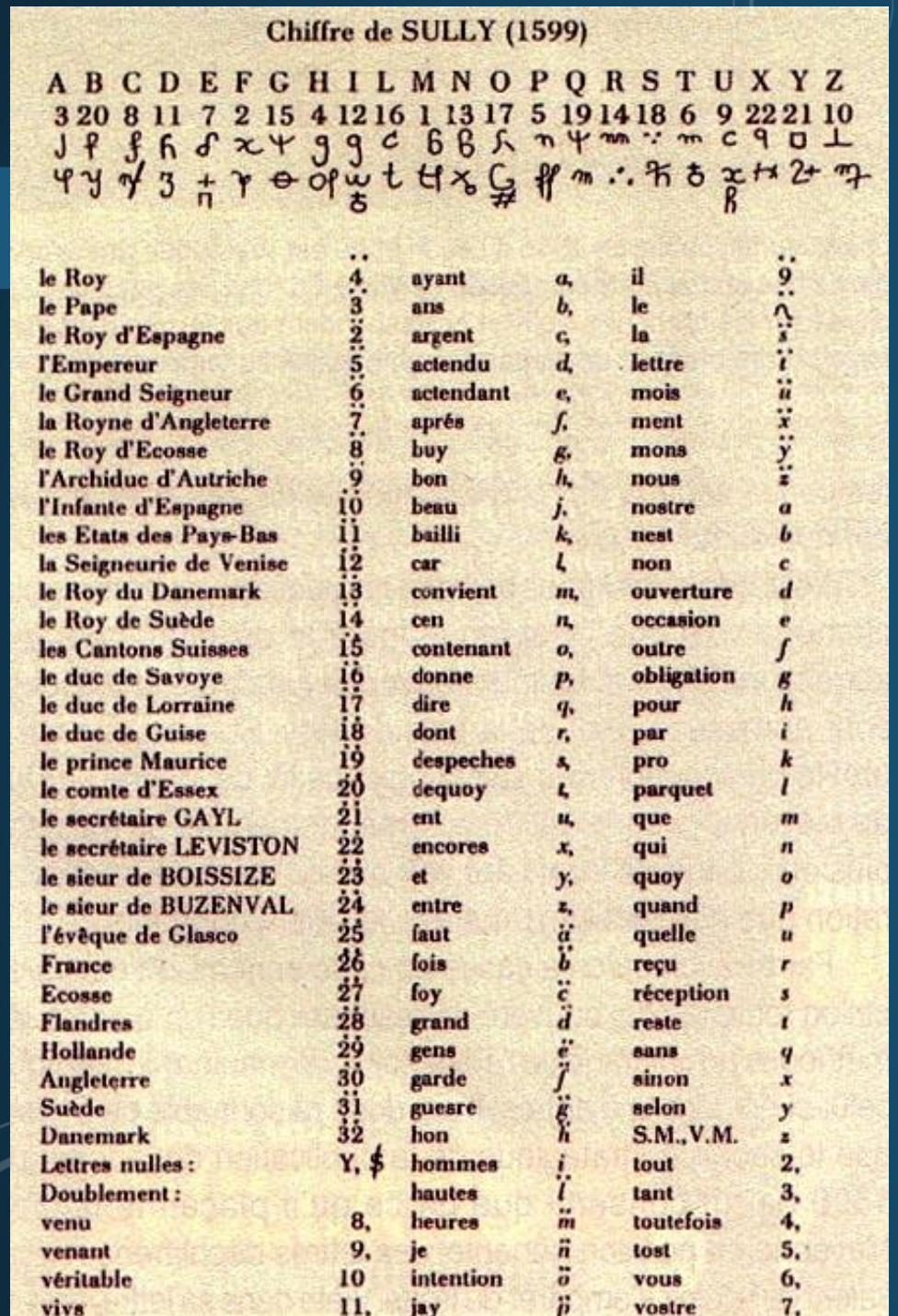
Společně se synem **Bonaventure Rossignol** (?-1705), byli pokládáni za nejskvělejší luštitele v Evropě.

Oba dva dosáhli velkého ocenění a získali značný majetek.

Přínos **Antoine R.** byl v oblasti zabezpečení šifrové služby francouzského království a především ve zdokonalení nomenklátoru. Jeho vylepšení se podařilo udržet v tajnosti po několik desetiletí.



A.Rossignol byl přijat po té, co vyluštil zprávu zašifrovanou výše uvedeným nomenklátorem a dopomohl tak vítězství u la Rochelle.


Chiffre de SULLY (1599)

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

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

DOBA NOMENKLÁTORŮ A JEJICH LUŠTITELÉ - FRANCIE

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.

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 seřazeny 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)

První písmeno zprávy
[illegible]
Druhé písmeno
nahradíte písmenem z
2. řádku (posun o 1
místo).
Třetí písmeno
[illegible]
ze 3. řádku (posun o 2
místa).
Takto pokračujete až k
poslednímu řádku, a
pak se případně vrátíte
na začátek.

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 XYZABCDEFGHIJKLMNOPQRSTUVW
25 YZABCDEFGHIJKLMNOPQRSTUVWX
26 ZABCDEFGHIJKLMNOPQRSTUVWXY

O K O

O L Q

1508 **Polygraphia** (6 dílů)

Vytištěna 1518

Ave Maria (písmenům přiřazena slova)

5 díl – „Tabula recta"

Vydávána a přepisována po celá staletí (1620 de Hotting)

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

GIOVANNI BATTISTA 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

1554 – ve třetím vydání doplněn systém autoklíče

GIROLAMO CARDANO (AUTOKLÍČ)

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 polyalfabetickcých šifer

- Změna hesla před každou zprávou !

- Použití autoklíč , neformuluje dokonale, opětovné použití klíče na začátku slova, nestanoví předání počátku hesla autoklíče

GIOVANNI BATTISTA PORTA (OBECNÁ POLYALFABETICKÁ ŠIFRA)

1535-1615, věnoval se přírodním vědám a magii

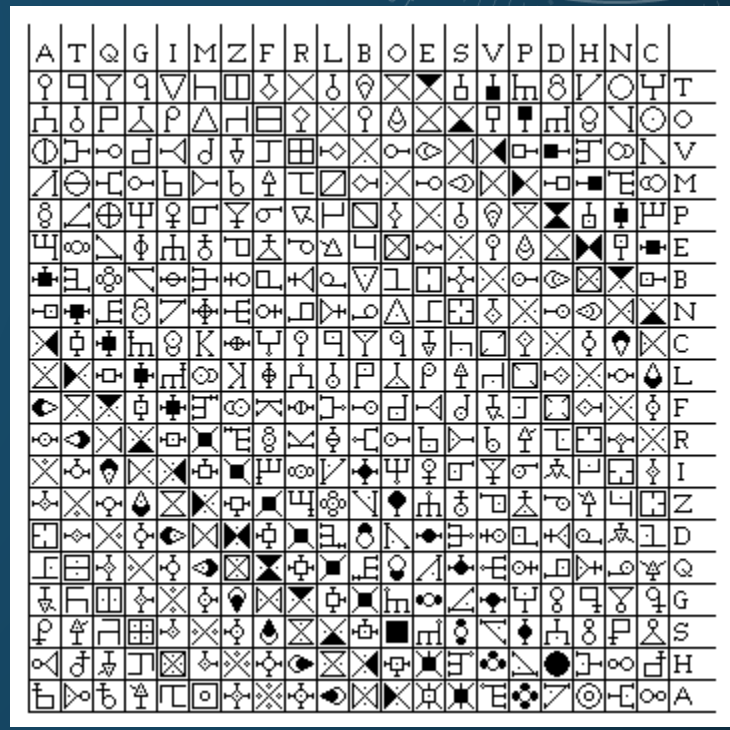
1563 vydal mimořádné dílo, obsah, pedagogický výklad **De Furtivis Litararum Notis**

4 části (staré šifry, moderní šifry, luštění, jazykové zvláštnosti)

Klasifikace – změna pořadí písmen, změna tvaru písmene, změna kvality

- Jako první popsal digrafickou šifru (realizace tabulkou)

- popis jak luštit monoalfabetickou šifru bez znalosti dělby slov

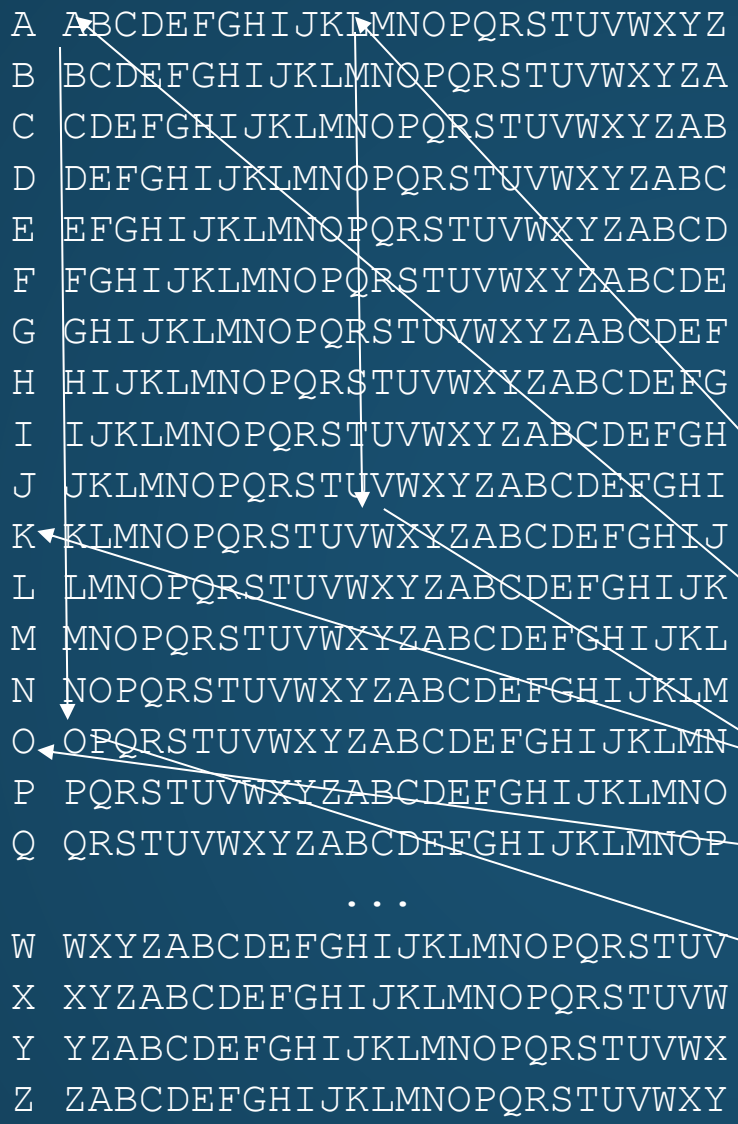


- Odmítl nerozluštitelnost polyalfabetických šifer

- doporučil používat co nejdelší klíč

-**Trithemiova tabulka NEMUSÍ obsahovat jen vzájemně posunuté abecedy**

BLAISE DE VIGENÉRE



Francouz Blaise de Vigenére (1523-1596)

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

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

Klíč:	OKNOOKNO
Otevřený text:	ALBATROS
Šifrový text:	OVOOHBBG

BLAISE DE VIGENÉRE

Téměř celý život byl ve službách vévody Navarrského.

S kryptologií se seznámil v době kdy působil jako diplomat ve Vatikánu.

Četl práce Trithemia, Belasa, Cardana, Porty.

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

Pasáže zabývající se okultními vědami, výrobou zlata, kabale, černé magii.

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) .

Právě autoklíč je největším přínosem jeho díla.

BLAISE DE VIGENÉRE – AUTOKLÍČ OTEVŘENÉHO TEXTU

Princip autoklíče otevřeného textu
(domluvené písmeno D, otevřený text ALBATROS):
Šifrant si vytváří autoklíč D+otevřený text
autoklíč se zapíše nad otevřený text:
Klíč: **D**ALBATRO
Otevřený text: ALBATROS
Určí se jednotlivé znaky šifrového textu pomocí tabulky a Vigenérova postupu.
Šifrový text: DLMBTKFG

Blaise de Vigenére – autoklíč šifrového textu

Princip autoklíče šifrového textu (domluvené písmeno D):
Klíč: **DDOPPIZN**
Otevřený text: ALBATROS
Šifrový text: **DOPPIZN F**

GASPAR SCHOTT (SYSTÉM GRONSFELD)

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

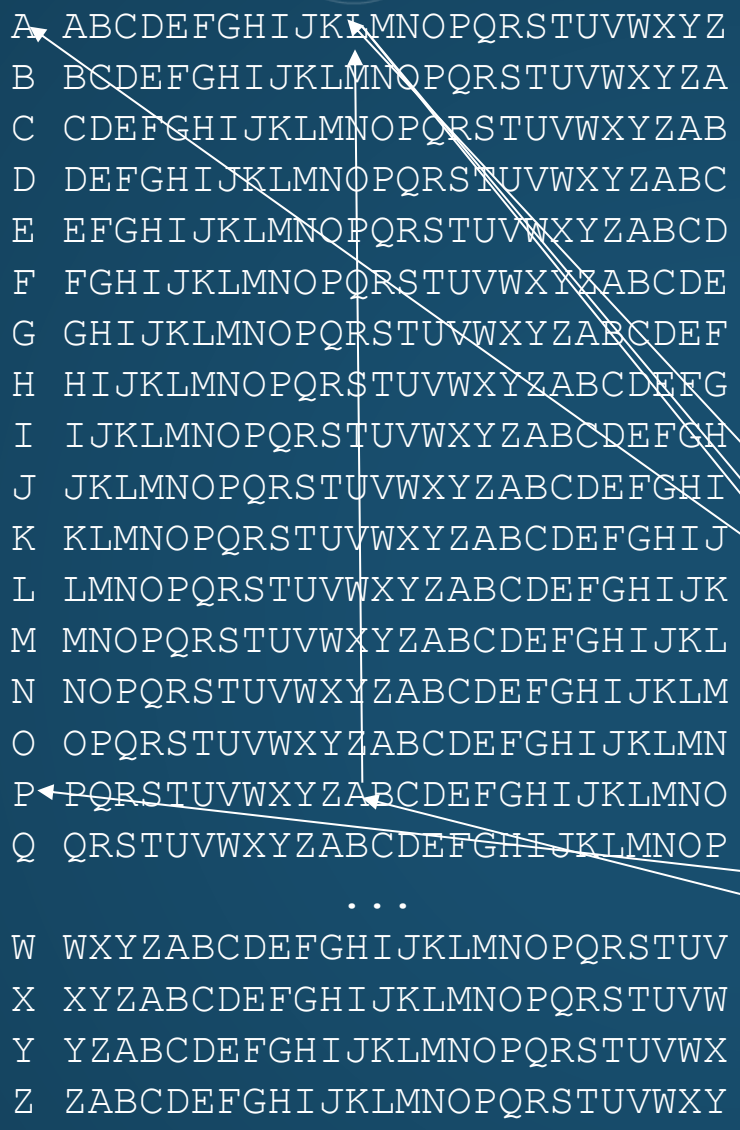
-zjednodušení (čísla, 10 abeced) vedlo k vyšší rychlosti a menší chybovosti

-oblíbený ještě ve 20.století používán (galérka)

Klíč:	5297 352973520
Otevřený text:	DNES NEPRIJDU
Šifrový text:	IPNZ QJRAPMIW

GIOVANNI SESTRI (BEAUFORTOVA VARIANTA VIGENÉROVY ŠIFRY, SESTRI-BEUAFORT)

- 1710 - Ital Giovani Sestri
- Úprava Vigenérově systému…
- V 19.století pojmenován podle obdobného systému admirála Beuforta (se kterým se někdy zaměňuje)



Klíč:	PAVELPAV
Otevřený text:	ALBATROS
Šifrový text:	LLGWICOX

SVĚT CHCE ŠIFROVAT

1. Morseovka

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

(první oficiální dálková zpráva byla odeslána až v roce **1844** z Washingtonu do Baltimoru. Text zněl: *"What hath God wrought"* (Co Bůh způsobil).)

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

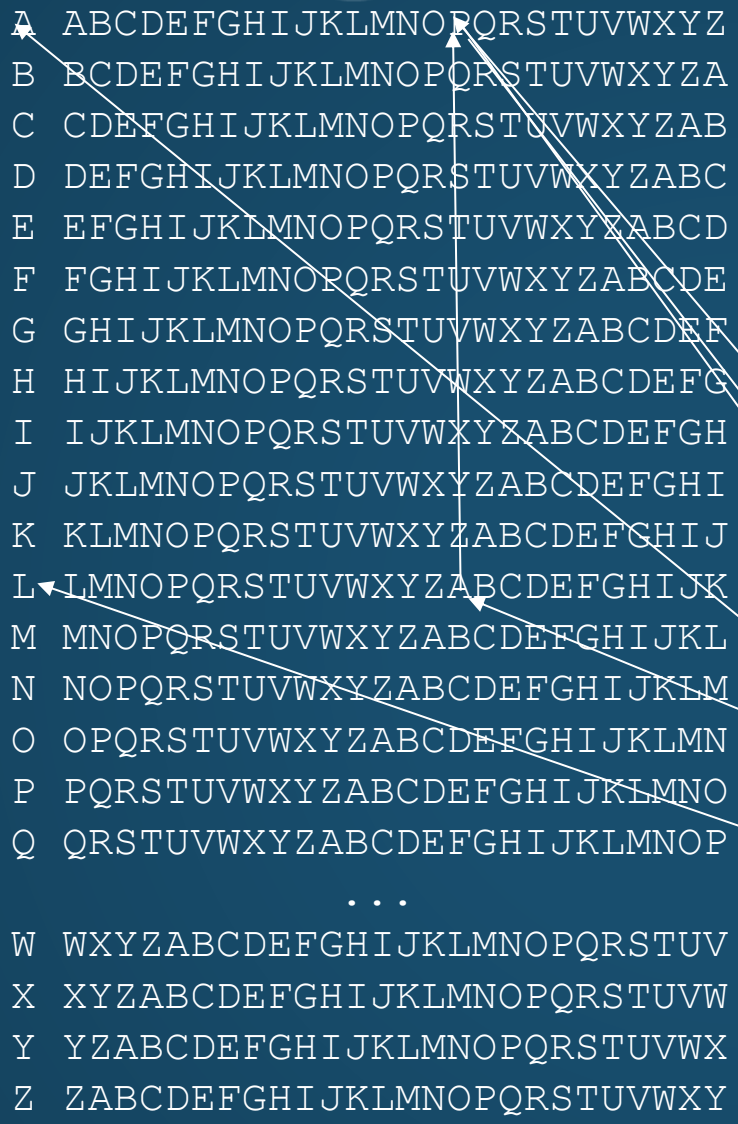
Francis O. J. Smith vydal komerční telegrafní kód pod názvem *The Secret Corresponding Vocabulary; Adapted to Morse's Electro-Magnetic Telegraph* (Slovník tajného dopisování upravený pro použití ve spojení s Morseovým elektromagnetickým telegramem). Obsahuje i 67 vět .

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 tvoření hesel.

Klíč:	PAVELPAV
Otevřený text:	ALBATROS
Šifrový text:	PPUEYMD

POROVNÁNÍ SYSTÉMŮ

Šifrování

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

Dešifrování

Tritheim, Cardano Vigenére, Gronsfeld			Beuafort			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.

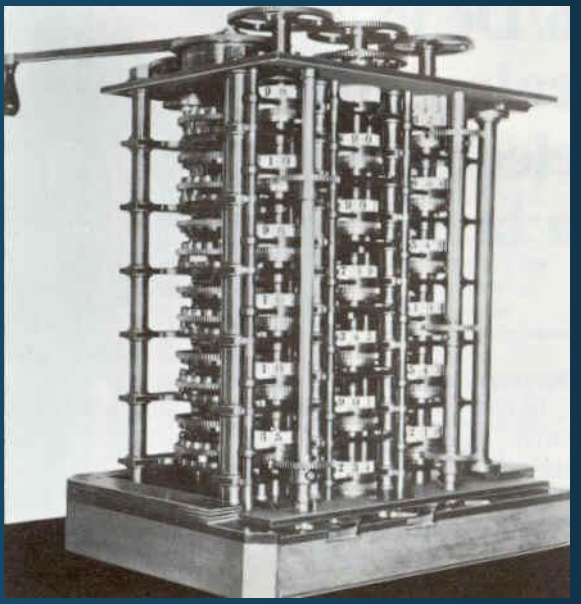
Zavedl označení pro libovolný znak šifrového textu jako řecké písmeno χ (chí), libovolný znak klíče Γ (gama) a libovolný znak otevřeného textu písmeno c. Následně dokázal, že algebraický vzorec $c + \Gamma = \chi$ popisuje Vigenérovo šifrování, a to samozřejmě bez ohledu na to, jak je technicky realizováno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

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

systém	**šifrování**	**dešifrování**
Vigenére	$O + K = Š$	$Š - K = O$
Beaufort	$K - O = Š$	$K - Š = O$
Varianta Beaufort	$O - K = Š$	$Š + K = O$

PÁD POLYALFABETICKÝCH ŠIFROVÝCH SYSTÉMŮ

Charles Babbage (1791-1871), výstřední profesor matematiky.
Difference Engine No.1 a No.2 (mechanické výpočetní stroje, programovatelné instrukce..)
Kryptoanalýza
-Řešení polyalfabetických šifer pomocí předpokládaného slova
-Studium autoklíče (jeho použití zabrání předchozímu útoku)



-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 Geheimschrifften und die Dechiffrirkunst* (Tajné šifry a umění je dešifrovat) **obecnou metodu na řešení Vigenérovy 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).

HAPPY END

Claud Elwood Shannon

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. Platí i pro „postkvantovou“ dobu.

POUŽITÍ

Po kubánské krizi se obě mocnosti (**USA a SSSR**) se domluvily na vybudování horké linky mezi hlavami obou států.

Horká linka byla uvedena do provozu 30. 8. 1963.

Bylo použilo zařízení **ETCRRM-II** (Electronic Teleprinter Cryptographic Regenerative Repeater Mixer II).

Od heslové pásky se odčítal otevřený (resp. šifrový text), páska s heslem byla ihned po použití automaticky ničena, čímž se mělo zamezit jejímu nechtěnému opětnému použití.

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

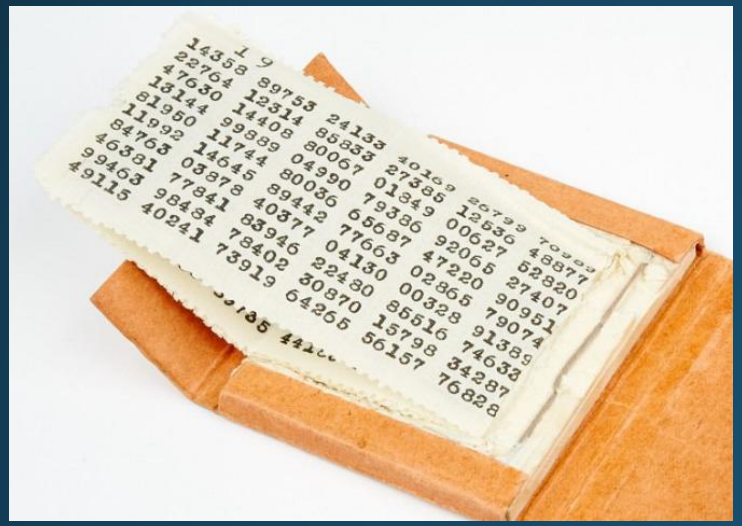
Modifikace systému byla v praxi používána špióny v době studené války tajnými službami (BND, CIA apod.) a dále pro vysílání „číselných stanic“ (dodnes).

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

Následovalo přičtení dohodnutého hesla - číselné sekvence.

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

HESLO PRO OTP



19

14358 89753 24133 40169 26799 76909
22764 12314 85833 27385 12536 48877
47630 14408 80067 01849 00627 52820
13144 99889 04990 79386 92065 27407

https://www.cryptomuseum.com/crypto/otp/index.htm

DEIN STAR – PŘEVODOVÁ TABULKA BND

Dein Star

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

https://kryptografie.de/kryptografie/chiffre/dein-star.htm

	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

Převodová tabulka používaná západoněmeckou tajnou službou BND (Bundes Nachrichten Dienst) během studené války, heslo DEIN STAR (tvá hvězda)

https://eshop.kybercentrum.cz/kryptografie-sifrovani-a-tajna-pisma

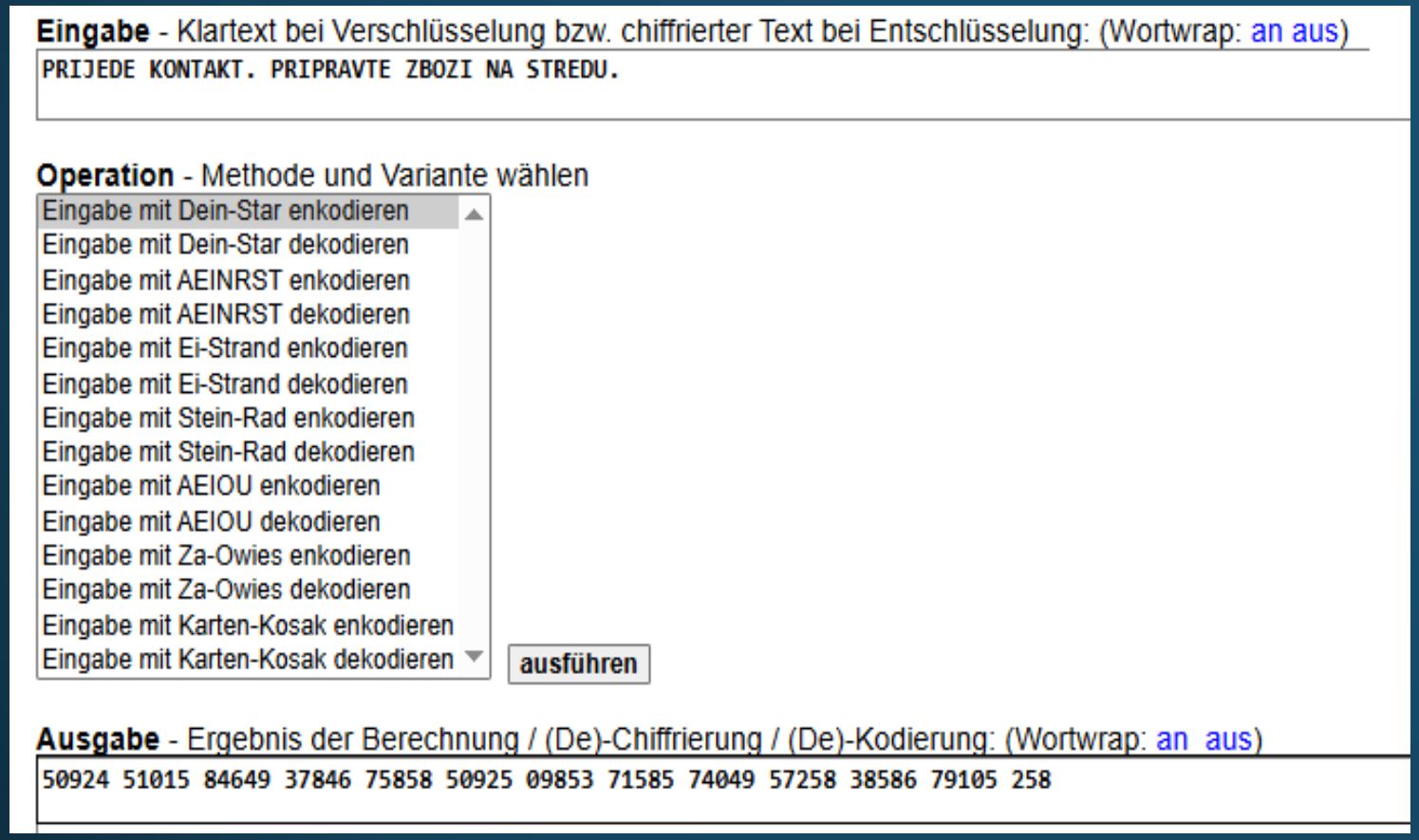
PŘÍKLAD - PŘEVOD

PRIJEDE KONTAKT. PRIPRAVTE ZBOZI NA STREDU.

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

DEIN-STAR: 50924 51015 84649 37846 75858 50925 09853 71585 74049 57258 38586 79105 258

Za-Owies: 37207 29824 84530 53440 13040 45372 07372 01408 45021 50745 34145 94020 824



VÝPOČET ŠT , OTP ŠIFROVÁNÍ

OT	PRIJEDE KONTAKT. PRIPRAVTE ZBOZI NA STREDU.												
OT (čísleny)	50924	51015	84649	37846	75858	50925	09853	71585	74049	57258	38586	79105	258
Heslo	14358	89753	24133	40169	26799	76909	22764	12314	85833	27385	12536	48877	476
ŠT	64272	30768	08772	77905	91547	26824	21517	83899	59872	74533	40012	17972	624

Vysílaná zpráva (příklad):Číselná stanice

Typická předehra (hudební, textová) a pak obvykle následuje opakované oznámení o počtu číselných skupin ve zprávě a označení hesla.
Zpráva se skládá z pětimístných skupin číslic (v jazyce používané stanicí, čeština), po nich následuje např. slovo "konec". Začátek zprávy bývá uvozen identifikační skupinou (nap a zpráva je ukončena skupinou 99999. Nakonec, po odeslání všech zpráv, se stanice nějakým charakteristickým způsobem odhlásí. Obvykle to je prostě nějaká forma slova "konec vysílání"

Předehra **13 19 13 19**
64272 30768 08772 77905 91547 26824 21517 83899 59872 74533 40012 17972 62430
konec 99999 konec vysílání

Děkuji za pozornost

Kryptologie, šifrování a tajná písma | KYBERCENTRUM - Centrum kybernetické bezpečnosti, z.ú.