

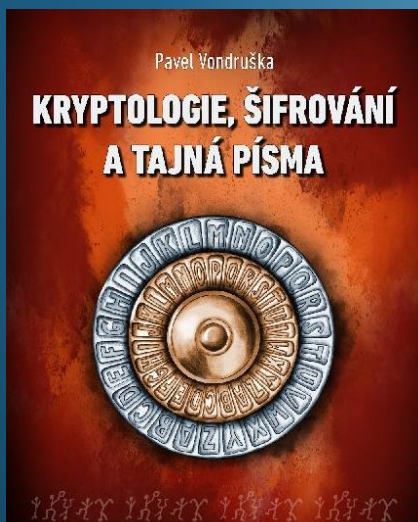
Dálnopisný stroj D-302 „Dalibor“
vyráběný ve Zbrojovce Brno



BEZPEČNOST, KTERÁ NESTÁRNE

PAVEL VONDRUŠKA

MFF UK Praha

[illegible]

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

ABCDEFGHIJKLMNOPQRSTUVWXYZ

BCDEFGHIJKLMNOPQRSTUVWXYZAA

MUNDUS VULT DECIPI (svět chce být klamán)

NXOEXT XXMV EFDKQK

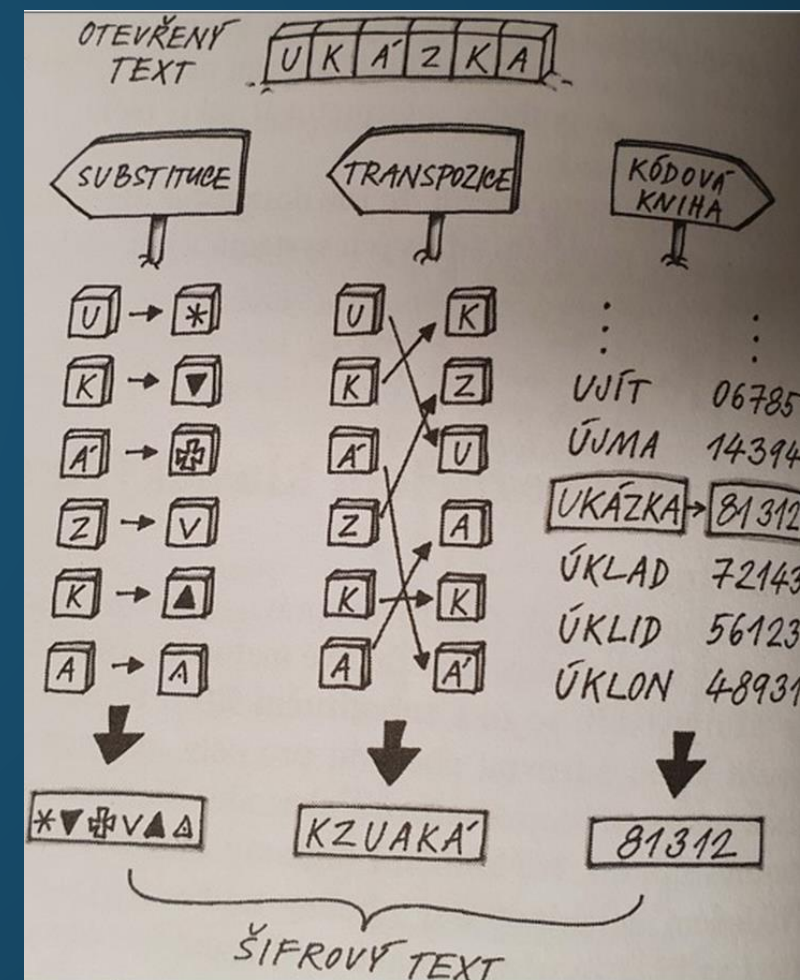
Šifra Atbash

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

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

11	10	9	8	7	6	5	4	3	2	1
כ	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

A. b. c. d. e. f. g. h. i. k. l. m. n. o. p. q. r. s. t. u. v. w. x. y. z.
 g. y. x. v. +. e. r. q. p. o. n. l. m. k. j. h. g. f. e. d. c. b. a.
 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100



HLEDÁ SE ODOLNÁ ŠIFRA PROTI FREKVENČNÍ ANALÝZE – 14. STOLETÍ

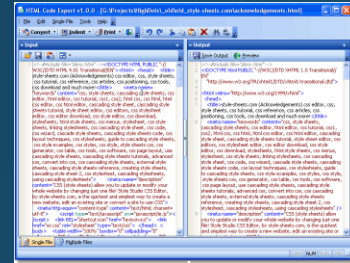
Abū-Yūsuf Ya'qūb ibn Ishāq al-Kindīho (801–873) X Evropa 14. století

Frekvence znaků

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

Frekvence trigramů

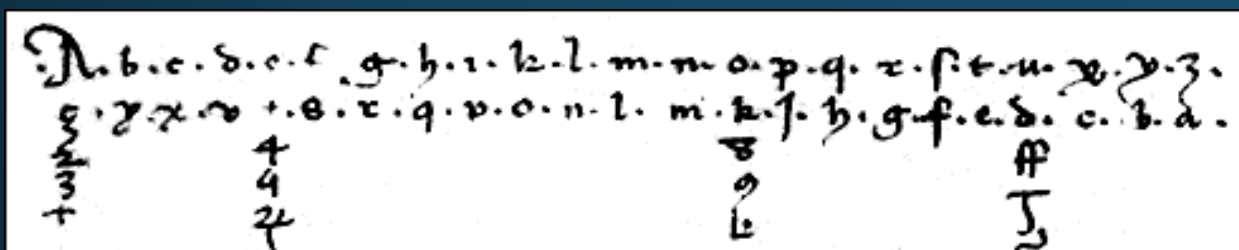
OVA = 100
SIF = 93
IFR = 89
MEN = 80
STI = 71
VAN = 66
PRO = 65
EHO = 65
OST = 62
ROV = 60
ENA = 60
ENI = 59
STA = 58
STR = 16

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: **MIKULAS**BCDEFGHJNOPQRTVWXYZ

Plain Text Alphabet : ABCDEFGHIJKLMNOPQRSTUVWXYZ



NOMENKLÁTOR 16.STOLETÍ

- Homofonní substituční záměny (*odstavec 1*).
- Znaký pro zdvojená písmena (*odstavec 2*).
- Kódy pro slabiky (*odstavec 3*).
- Nulle / Klamače (*2. řádek odstavce 2*). Bezvýznamové prvky vkládané do šifrového textu ke zmatení luštitele a narušení statistické analýzy.
- Kódy pro nejčastěji používaná (frekventní) slova a jména (*odstavec 4*).

Cum Ser^{mo}. Rege Ferdinando. M. sue missa
ex Mto. Neapolim. xx^o. Julij. M. cccc. lxi.

① A. b. c. d. e. f. g. h. i. l. m. n. o. p. q. r. s. t. u. x. z. d. g.
 b. b. o. p. p. p. d. d. a. t. ã. d. s. 6. 8. ∞. +. g. i. l. r. f.
 o. b. o. b. p. t. p. t. 2. d. a. a. p. a. d. u. 9. 7. 7. ∞. #. 7. o. u. e. g. x.
 b. f. d. u. - o. g. ~ ∞

② *Gemine*. bb. cc. dd. ff. ll. mm. nn. pp. vv. ss. tt.
 $\bar{3}$ 3 $\bar{3}$ 3^+ 3^0 3^{+0} $\bar{3}$ 3^+ 3^+ 3^e 3^a

Nulla. ϕ . ∞ . γ . ∞ .

Qua. que. qui. che. per. qñ. pch. come. La. ay. v. La s. v. La s. del. pp.

③ Ab. ac. ad. af. ag. al. am. an. as. at. av. au. Eb. ic.
 n n ne nt no nto ñ ne xi nao ñ ñ v v
 Ed. ef. eg. em. el. en. ep. ev. es. et. Ib. ic. id. ig. if.
 v v vt vo vto x v v v v v g g g g g
 Il. Im. in. ip. ir. is. it. Vb. uc. ud. uf. ug. vl. um. un. vp.
 g g g g g g g g g g g g g g g g
 Vr. vs. vt. Ob. oc. od. of. og. ol. om. on. op. or. os. ot.
 g gh gl r r r r r r r r r r r r r r

④	Papa	S	Venet	SM	D. Sigismundus	sf
	Imperator	S	Florentini	SII	Januenses	pf
	Rex France	S	Princeps Tarenti	SM	Dux Sabaudie	f
	Rex Aragonum	S	Princeps Rossini	SM	Armato	fo
	Dux Penatus	So	D. Alex sfor	SA	Galeo	fo
	Dux Johannes	St	Co. Urbini	SE	Cavalli	fu
	Dux Mucine	St	Princeps Salemi	ST	Fanti	fu
			Co. Jacobus	Sto		

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
J	f	g	h	d	x	y	g	g	c	6	6	h	n	y	m	·	m	c	9	□	⊥
4	y	y	3	+	γ	θ	o	ω	t	⊥	x	G	ff	m	·	h	δ	x	+	2	7

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 Roynie 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	ā,	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	j,	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

- Nomenklátory se začaly měnit – neustále se zvětšoval počet kódů
- Abecední řazení odhalovalo vztah mezi slovem a kódem.
- Luštitel mohl odhadnout počáteční písmeno hledaného slova.
- Rossignol zavedl náhodné přiřazování kódů.
- Vznikly samostatné seznamy pro šifrování a dešifrování.
- Nomenklátory se rozvinuly v rozsáhlé kódové knihy.

Antoine Rossignol (1589–1682)

Francouzský matematik, kryptolog a kryptoanalytik, dvorní dešifrant kardinála Richelieu a králů Ludvíka XIII. a Ludvíka XIV.

KÓDOVÉ KNIHY

Kódové knihy - konec éry

- Používány až do poloviny 20. století.
- Často kombinovány s dalšími kryptografickými metodami.
- Náročná distribuce a výměna mezi uživateli.
- Vysoké riziko získání kódové knihy protivníkem.
- Nevhodné pro rychlou operativní komunikaci.
- Postupně nahrazeny ručními šiframi a později šifrovacími stroji.

Zimmermannův telegram (1917)

- Německá tajná depeše pro Mexiko.
- Nabídka spojení proti USA.
- Příklad navracení ztracených území.
- Zachycen a rozluštěn britskou rozvědkou.
- Přispěl ke vstupu USA do 1. světové války.

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

GERMAN LEGATION
MEXICO CITY

via Galveston

JAN 19 1917

862.30212/324

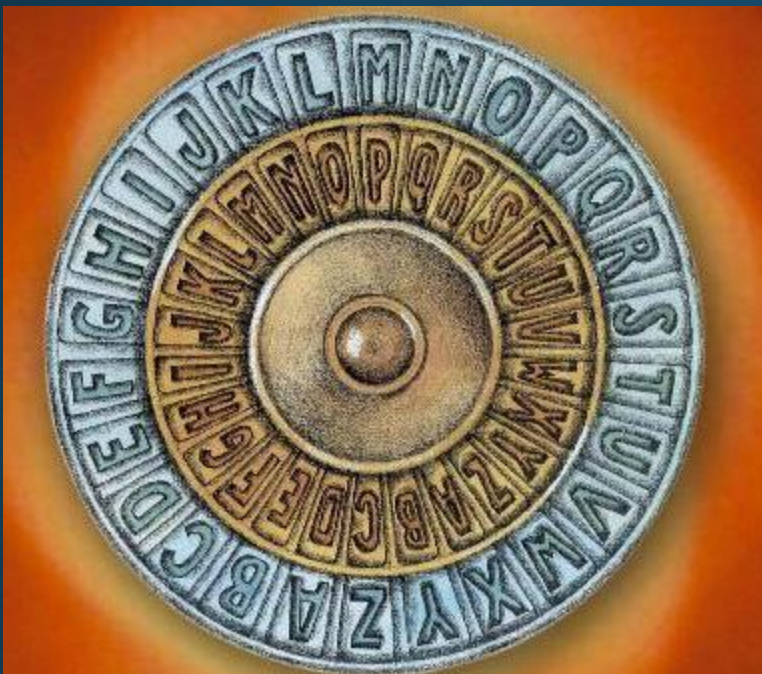
130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21560	10247	11518	23677	13605	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
23284	22200	19452	21589	67893	5569	13918	8958	12137	
1333	4725	4458	5905	17166	13851	4458	17149	14471	6706
13850	12224	6929	14991	7382	15857	67893	14218	36477	
5870	17553	67893	5870	5454	16102	15217	22801	17138	
21001	17388	7446	23638	18222	6719	14331	15021	23845	
3156	23552	22096	21604	4797	9497	22464	20855	4377	
23610	18140	22260	5905	13347	20420	39689	13732	20667	
6929	5275	18507	52262	1340	22049	13339	11265	22295	
10439	14814	4178	6992	8784	7632	7357	6926	52262	11267
21100	21272	9346	9559	22464	15874	18502	18500	15857	
2188	5376	7381	98092	16127	13486	9350	9220	76036	14219
5144	2831	17920	11347	17142	11264	7667	7762	15099	9110
10482	97556	3569	3670						

BEPNSTOPFF.

Charge German Embassy.

LEON BATTISTA ALBERTI (1404–1472)

PRVNÍ POLYALFABETICKÝ ŠIFROVÝ SYSTÉM



- Všestranně nadaný renesanční učenec: architekt, stavitel, varhaník, básník a filozof.
- Na podnět papežského tajemníka Leonarda Data se na sklonku života začal věnovat utajování zpráv.
- 1466 – vydává 25 stránkové pojednání o šifrování, traktát De Cifris
- Označován za **otce západní kryptologie**.
- Sestrojil **Albertiho disk**, který umožňoval střídání šifrových abeced.

Albertiho doporučení

- Šifrovou abecedu měnit přibližně po třech až čtyřech slovech.
- Pravidelné střídání abeced zvyšovalo odolnost proti frekvenční analýze.

Tři Albertiho kryptologické přínosy

1. První systematický výklad luštění pomocí frekvenční analýzy.
2. Zavedení polyalfabetického šifrování.
3. Myšlenka šifrování kódů a nomenklatorních prvků.

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

JOHANNES TRITHEMIUS 1452-1516 (TABULA RECTA)

První písmeno zprávy
píšete tak, jak je (1.
řádek, posun 0).

Druhé písmeno
nahradíte písmenem z
2. řádku (posun o 1
místo).

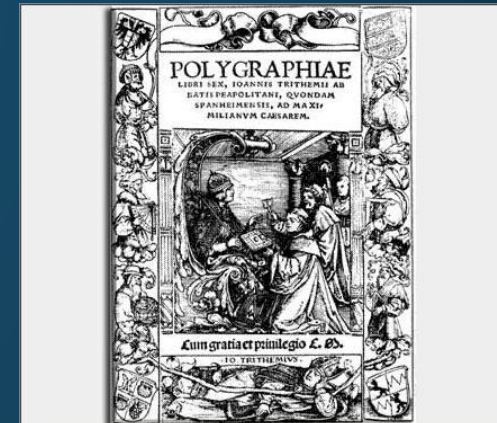
Třetí písmeno
nahradíte písmenem
ze 3. řádku (posun o 2
místa).

Takto pokračujete až k
poslednímu řádku, a
pak se případně vrátíte
na začátek.

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

- Německý benediktinský opat, učenec
- Autor **Polygraphie** (1508, tisk 1518).
- První tištěné dílo o kryptografii.
- **5. kniha** představuje slavnou **Tabula recta**.
- **Základ polyalfabetického šifrování.**
- Obsahuje různé metody utajování zpráv.
- Popisuje systém **Ave Maria**, kde jsou písmenům přiřazována celá slova.
- Dílo bylo po staletí vydáváno, opisováno a dále r

OKO
OLQ



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.

BLAISE DE VIGENÉRE

Francouz Blaise de Vigenère (1523-1596)

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

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	YZABCDEFGHIJKLMNOPQRSTUVX
Z	ZABCDEFGHIJKLMNOPQRSTUVWXY

Klíč:

OKNOOKNO

Otevřený text:

ALBATROS

Šifrový text:

OVOOHBBG

1553 - La cifra del. Sig. Giovan Battista Belaso

Zavedl tajný klíč pro volbu abecedy (dohoda na pořadí využití abeced)

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

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

1710 - Ital Giovani Sestri

Úprava Vigenérova systému (menší
chybovost při přípravě šifrového znaku
textu)...

V 19. století pojmenován podle obdobného
systému admirála Beuforta (se kterým se
někdy nesprávně zaměňuje)

A ABCDEFGHIJKLMNOPQRSTUVWXYZ
B BCDEFGHIJKLMNOPQRSTUVWXYZA
C CDEFGHIJKLMNOPQRSTUVWXYZAB
D DEFGHIJKLMNOPQRSTUVWXYZABC
E EFGHIJKLMNOPQRSTUVWXYZABCD
F FGHIJKLMNOPQRSTUVWXYZABCDE
G GHIJKLMNOPQRSTUVWXYZABCDEF
H HIJKLMNOPQRSTUVWXYZABCDEFG
I IJKLMNOPQRSTUVWXYZABCDEFGH
J JKL MNOPQRSTUVWXYZABCDEFGHI
K KLMNOPQRSTUVWXYZABCDEFGHIJ
L LMNOPQRSTUVWXYZABCDEFGHIJK
M MNOPQRSTUVWXYZABCDEFGHIJKL
N NOPQRSTUVWXYZABCDEFGHIJKLM
O OPQRSTUVWXYZABCDEFGHIJKLMN
P PQRSTUVWXYZABCDEFGHIJKLMNO
Q QRSTUVWXYZABCDEFGHIJKLMNO
...
W WXYZABCDEFGHIJKLMN OPQRSTU
X XYZABCDEFGHIJKLMN OPQRSTU
Y YZABCDEFGHIJKLMN OPQRSTU
Z ZABCDEFGHIJKLMN OPQRSTU

Klíč:

PAVELPAV

Otevřený text:

ALBATROS

Šifrový text:

LLGWICOX

SYSTÉM BEAUFORT

Sir Francis Beaufort (1774-1857)

- Anglický admirál a hydrograf.
- Známý především díky Beaufortově stupnici síly větru.
- Nabídl jednoduchý a levný systém šifrování telegrafních zpráv.
- Cena šifrovací pomůcky: 6 pencí.
- Určeno pro běžné každodenní použití.
- Součástí byla šifrovací tabulka, návod a pravidla pro tvorbu hesel.

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	WXYZABCDEFGHIJKLMNOPQRSTU
X	XYZABCDEFGHIJKLMNOPQRSTUV
Y	YZABCDEFGHIJKLMNOPQRSTUVW
Z	ZABCDEFGHIJKLMNOPQRSTUVWX

Klíč:

PAVEL PAVEL

Otevřený text:

DIGIF UTURE

Šifrový text:

MSQWG VHBNH

SVĚT CHCE ŠIFROVAT

Morseovka (1840-1844)

- Patent telegrafu.
- První dálková zpráva.
- Začátek telegrafické éry.

Černé komnaty

- Anglie (1844), Francie a Rakousko-Uhersko (1848).
- Zachycování a analýza komunikace.

Telegrafní kódy

- Francis O. J. Smith.
- Utajení obchodních a diplomatických zpráv.
- Kódové knihy až se 100 000 položkami.

Pětimístné skupiny

- Anglické předpisy z roku 1904.
- Šifrový text ve skupinách po pěti znacích.
- Budoucí standard kryptografické praxe.

POROVNÁNÍ SYSTÉMŮ

- Francouzský kryptolog známý pod pseudonymem de Viaris (Vlastním jménem **Marquis Gaëtan Henri Léon Viarizio di Lesegno**)
- Roku **1888** publikoval v časopise *Le Génie Civil* dvoudílnou studii.
- Později vyšla knižně pod názvem **Cryptographie**.
- Jako jeden z prvních popsal polyalfabetické šifry pomocí matematických a algebraických vztahů.
- Ukázal, že tyto systémy šifrování lze vyjádřit jednoduchým vzorcem nezávisle na použité pomůcce (tabulka, proužek, kotouč) a způsobu práce s touto pomůckou klíč / otevřený / šifrový text.

Tritheim, Vigenère , Gronsfeld

$$\text{Š} = \text{O} + \text{K}$$

$$\text{O} = \text{Š} - \text{K}$$

Beaufort

$$\text{Š} = \text{K} - \text{O}$$

$$\text{O} = \text{K} - \text{Š}$$

Varianta Beaufort

$$\text{Š} = \text{O} - \text{K}$$

$$\text{O} = \text{Š} + \text{K}$$

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

PÁD POLYALFABETICKÝCH ŠIFROVÝCH SYSTÉMŮ

Charles Babbage (1791-1871)

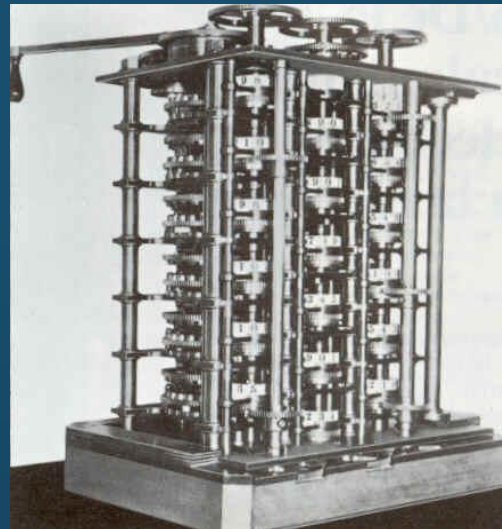
- Anglický matematik a vynálezce.
- Autor mechanických výpočetních strojů **Difference Engine No. 1** a **Difference Engine No. 2**.
- Zabýval se také kryptoanalýzou polyalfabetických šifer.
- Studoval útoky založené na předpokládaném slově (*probable word attack*).

Hlavní kryptologický přínos

- Kolem roku **1854** našel obecný postup pro luštění Vigenèrovy šifry s periodickým heslem.
- Metoda využívala analýzu vzdáleností mezi opakujícími se skupinami znaků v šifrovaném textu.
- Svůj objev nepublikoval.
- Byl objeven až později v jeho osobních poznámkách.

Friedrich Wilhelm Kasiski (1805-1881)

- Důstojník pruské armády.
- Roku **1863** vydal knihu *Die Geheimschriften und die Dechiffirkunst* (*Tajné šifry a umění je dešifrovat*).
- Publikoval obecnou metodu pro luštění Vigenèrovy šifry s periodickým heslem.
- Metoda vychází z hledání periody hesla pomocí opakujících se skupin znaků.
- Po určení délky hesla se problém redukuje na řešení několika monoalfabetických šifer.



Auguste Kerckhoffs (1835-1903)

- Roku **1883** vydal knihu *La Cryptographie Militaire* (Vojenská kryptografie).
- Zabýval se praktickými problémy vojenské kryptografie.
- Popsal metodu luštění polyalfabetických šifer s neperiodickým klíčem, pokud byl tentýž klíč použit opakovaně.
- Reagoval na nové požadavky doby:
 - masové využití polních šifer,
 - ochranu telegrafní komunikace,
 - jednoduchost a praktičnost šifrovacích systémů.

Kerckhoffsův princip

- Bezpečnost šifrového systému nesmí záviset na utajení algoritmu.
- Tajný má být pouze **klíč**.
- Šifrovací systém musí zůstat bezpečný i v případě, že protivník zná jeho konstrukci.
- Jedná se o druhý ze šesti Kerckhoffsových požadavků na vojenské šifry.
- Dodnes patří k základním principům moderní kryptografie.

HISTORIE ONE-TIME PADU

Franklin Miller (1842–1925)

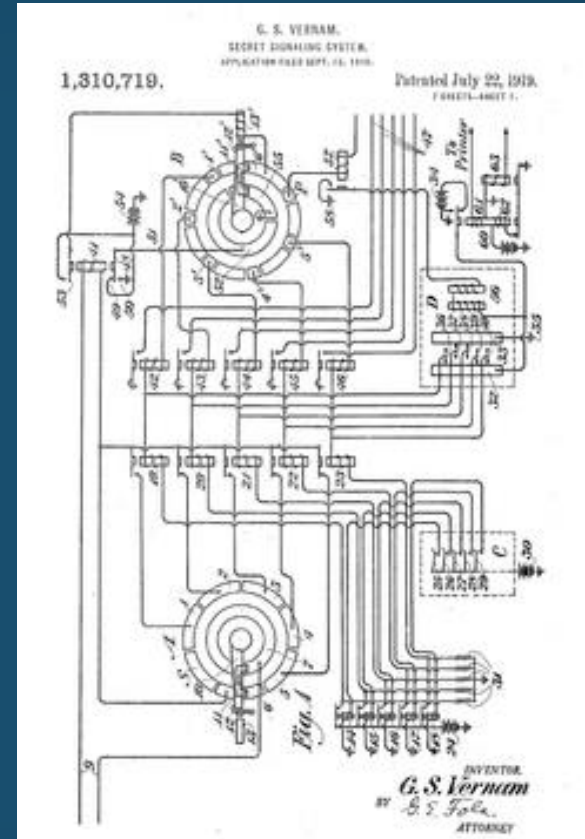
- 1882: první známý popis principu One-Time Padu
- o 35 let předchází Vernamovi
- čísla se nesmějí opakovat
- použitá čísla mají být vyřazena

Gilbert Sandford Vernam (1890–1960)

- inženýr AT&T Bell Laboratories
- dálkopisná šifra s klíčem na papírové pásce (1917)
- kombinace klíče a otevřeného textu znak po znaku
- patent USA č. 1 310 719 (1919)

Joseph Oswald Mauborgne (1881–1971)

- kapitán Signálního sboru armády USA
- kolem roku 1917 doplnil princip náhodného klíče
- klíč smí být použit pouze jednou
- vznik moderního One-Time Padu



Miller (1882)

První známý popis OTP



Mauborgne (1917)

Náhodný klíč použitý
pouze jednou



Vernam (1917, patent
1919)

Praktická a
patentovaná realizace

Historický Vernamův příklad (Baudot)

Šifrování:

otevřený text

A = ++---

klíčový znak

B = +--++

výsledný šifrový text

$G = -+-++$

Dešifrování:

přijatý znak

$G = -+-++$

znovu se zkombinuje se stejným klíčem

B = +--++

vznikne původní otevřený text $A = ++---$

V původním Vernamově popisu se pojem XOR nepoužívá. Interpretace Vernamovy šifry jako operace XOR je až pohledem moderní informatiky a digitální logiky.

Moderní interpretace pomocí XOR (binární zápis)

$$\check{S} = 0 \text{ XOR } K$$
$$O = S \text{ XOR } K$$

Modulární zápis (abeceda o 26 znacích)

Beaufortova varianta polyalfabetické šifry:

$$\check{S} = (K - O) \bmod 26$$
$$O = (K - \check{S}) \bmod 26$$

SYSTÉM BEAUFORT

A	ABCDEFHGHIJKLMNOPQRSTUVWXYZ		
B	BCDEFHGHIJKLMNOPQRSTUVWXYZ		
C	CDEFHGHIJKLMNOPQRSTUVWXYZAB		
D	DEFHGHIJKLMNOPQRSTUVWXYZABC		
E	EFGHGIJKLMNOPQRSTUVWXYZABCD		
F	FHGHIJKLMNOPQRSTUVWXYZABCDE		
G	GHGIJKLMNOPQRSTUVWXYZABCDEF		
H	HIJKLMNOPQRSTUVWXYZABCDEFG		
I	IJKLMNOPQRSTUVWXYZABCDEFGH		
J	JKLMNOPQRSTUVWXYZABCDEFGHI		
K	KLMNOPQRSTUVWXYZABCDEFHGHI		
L	LMNOPQRSTUVWXYZABCDEFHGIJK		
M	MNOPQRSTUVWXYZABCDEFHGIJKL		
N	NOPQRSTUVWXYZABCDEFHGIJKLM		
O	OPQRSTUVWXYZABCDEFHGIJKLMN		
P	PQRSTUVWXYZABCDEFHGIJKLMNO		
Q	QRSTUVWXYZABCDEFHGIJKLMNOP		
	...		
W	XYZABCDEFHGHIJKLMNOPQRSTUV	Klíč:	PAVEL PAVEL
X	XYZABCDEFHGHIJKLMNOPQRSTUVW	Otevřený text:	DIGIF UTURE
Y	YZABCDEFHGHIJKLMNOPQRSTUVWX	Šifrový text:	MSQWG VHNBI
Z	YZABCDEFHGHIJKLMNOPQRSTUVWXY		

Klíč:	PAVELPAVEL																																					
Otevřený text:	DIFIFUTURE													$0=K-\tilde{S}(\text{mod}26)$																								
Výsledný šifrový text je:	MSQWGVHBNH													$\tilde{S}=K-0(\text{mod}26)$																								
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													
Klíč											P			A			V			E			L			P			A			V			E			L
Hodn. K											15			0			21			4			11			15			0			21			4			11
Otevřený text											D			I			F			I			F			U			T			U			R			E
Hodn. 0											3			8			5			8			5			20			19			20			17			4
Šifrový text											12			18			16			22			6			21			7			1			13			7
Šifra											M			S			Q			W			G			V			H			B			N			H
$\tilde{S}=K-0(\text{mod}26)$																																						

Claude Elwood Shannon (1916 – 2001)

- zakladatel moderní **teorie informace**
- autor prací:
 - *A Mathematical Theory of Communication* (1948)
 - *Communication Theory of Secrecy Systems* (1949)
- zavedl pojem **redundance informace**
- položil teoretické základy moderní kryptologie
- matematicky analyzoval bezpečnost šifrovacích systémů
- dokázal, že **One-Time Pad** může dosáhnout **dokonalého utajení** (*perfect secrecy*)
(Ze samotného šifrovaného textu nelze získat žádnou informaci o otevřeném textu.)

One-Time Pad je dosud jediný prakticky známý kryptosystém s matematicky prokázaným dokonalým utajením (*perfect secrecy*).

Jeho bezpečnost nezávisí na výpočetním výkonu útočníka, a tedy ani na existenci **kvantových počítačů**.

One-Time Pad je bezpečný pouze tehdy, pokud:

- ✓ klíč je **skutečně náhodný**
- ✓ klíč není generován deterministickým algoritmem
- ✓ délka klíče je alespoň rovna délce zprávy
- ✓ každá část klíče je použita **pouze jednou**
- ✓ všechny možné klíče jsou stejně pravděpodobné
- ✓ klíč zůstane utajen před útočníkem

1466 Alberti → první polyalfabetická šifra
1882 Miller → první známý popis OTP
1917 Mauborgne → náhodný jednorázový klíč
1919 Vernam → praktická realizace a patent
1949 Shannon → důkaz perfect secrecy

Chyba stejný klíč, opakování klíče, část klíče použita více krát:

$$\text{Š}_1 = \text{O}_1 \oplus \text{K}$$

$$\text{Š}_2 = \text{O}_2 \oplus \text{K}$$

$$\text{Š}_1 \oplus \text{Š}_2 = \text{O}_1 \oplus \text{O}_2 \quad (\text{protože } \text{K} \oplus \text{K} = 0)$$

- útočník získá vztah mezi oběma otevřenými texty
- stačí znát, odhadnout nebo otestovat pomocí slovníkového útoku jeden text (nebo jeho část)
- následně lze odvodit druhý text (nebo jeho část)

ETCRRM-II: ONE-TIME PAD V PRAXI

norský kryptografický systém ETCRRM-II
používán v komunikačních systémech NATO
po kubánské krizi byla mezi USA a SSSR vybudována tzv. horká
linka, byla uvedena do provozu 30. srpna 1963
šifrování využívalo jednorázové klíčové pásky (One-Time Pad)
po použití byla klíčová páska automaticky zničena
zabránilo se tak opětovnému použití stejného klíče

Původní teletype s ETCRRM byl postupně nahrazen:
1980 nahrazen systémem Siemens M-190
1986 faxovým spojením
2008 zabezpečeným počítačovým systémem založeným na výměně
zpráv prostřednictvím zabezpečené elektronické komunikace.

Zajímavé je, že slavný „červený telefon“ nikdy neexistoval.
Od počátku šlo o textovou komunikaci, nikoliv o telefonní hovor.



Použití – československý šifrátor Šifrovací stroj ŠD –3



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.

ČÍSELNÉ STANICE

Nikdo neví, kdo právě poslouchá. Stačí obyčejný krátkovlnný přijímač a správný jednorázový klíč.

Číselné stanice (Numbers Stations)

- krátkovlnné rádiové stanice vysílající série čísel, písmen nebo znaků Morseovy abecedy
- zprávy jsou často předčítány syntetickým nebo nahraným hlasem
- aktivní jsou již od období druhé světové války (DOSUD !)
- signál lze přijímat na velmi velké vzdálenosti po celém světě
- vysílání bývá pravidelné i nepravidelné podle potřeby
- předpokládá se souvislost především se zpravodajskými službami
- některé (většina) stanic využívá šifrování typu **One-Time** Pad (a specifické převody otevřených textů na číselné posloupnosti)

Charakteristické vlastnosti

- ✓ anonymní příjemce
- ✓ celosvětový dosah krátkých vln
- ✓ jednoduchý příjem běžným rádiem
- ✓ velmi obtížné (nemožné) určování adresáta zprávy

The Conet Project

ČÍSELNÉ STANICE 2

- Akin O. Fernandez začal od roku 1992 systematicky nahrávat vysílání číselných stanic
- v roce 1997 vydal soubor 4 CD:
 - *The Conet Project: Recordings of Shortwave Numbers Stations*
- The Conet Project představuje nejznámější veřejně dostupný archiv vysílání číselných stanic.
- v roce 1999 byla nahrávková kolekce zpřístupněna online
- po roce 2000 začala řada tradičních číselných stanic postupně utichat

Číselné stanice dnes

- některé stanice vysílají dodnes
- systematické monitorování zajišťuje komunita radioamatérů a výzkumníků
- aktuální přehled vysílání: **Priyom.org**

Priyom.org › Military Stations

Military Stations

Table of contents:

- › Belarus
- › Bulgaria
- › France
- › Israel
- › Russia
 - › Russian Ground Forces
 - › Russian Air Force
- › United Kingdom

TIME	STN.	FREQ.	MODE	REMARKS
------	------	-------	------	---------

Thursday, 1 October

00:00	V13	15388kHz	USB/AM	[Target: East Asia]
00:00	V13	15890kHz	USB/AM	[Target: East Asia]
00:00	V13	18040kHz	USB/AM	[Target: East Asia]
01:00	F06a	17532kHz	RTTY	[Target: Pacific]
01:00	V13	18040kHz	USB/AM	[Target: East Asia]
01:00	V13	19052kHz	USB/AM	[Target: East Asia]
01:00	V13	20025kHz	USB/AM	[Target: East Asia]
01:15	F06a	16351kHz	RTTY	[Target: Pacific]
01:30	F06a	14428kHz	RTTY	[Target: Pacific]
02:00	V32	7910kHz	USB	
02:00	V13	8169kHz	USB/AM	[Target: East Asia]
02:00	V13	8300kHz	USB/AM	[Target: East Asia]
02:30	F01	13370kHz	RTTY	[Target: Pacific]

Current prefixes:

- › E - English language voice broadcasts
- › G - German language voice broadcasts
- › S - Slavic language voice broadcasts
- › V - Voice broadcasts in all other languages
- › M - Morse code

Příklad použití

- otevřený text se nejprve převedl do číselné podoby pomocí **jedno- nebo dvoumístné číselné záměny**
- k takto získanému číselnému textu se přičetla **jednorázová klíčová sekvence (heslo)**
- výsledkem byl šifrový text určený k přenosu

Ukázka

- použita je jedna z převodových tabulek západoněmecké zpravodajské služby **BND (Bundesnachrichtendienst)**
- tabulka byla opakovaně využívána během období studené války

PRIJEDE KONTAKT. PRIPRAVTE ZBOZI NA STREDU.

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

	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	.	,

Eingabe - Klartext bei Verschlüsselung bzw. chiffrierter Text
PRIJEDE KONTAKT. PRIPRAVTE ZBOZI NA STREDU.

Operation - Methode und Variante wählen

Eingabe mit Dein-Star enkodieren
Eingabe mit Dein-Star dekodieren
Eingabe mit AEINRST enkodieren
Eingabe mit AEINRST dekodieren
Eingabe mit Ei-Strand enkodieren
Eingabe mit Ei-Strand dekodieren
Eingabe mit Stein-Rad enkodieren
Eingabe mit Stein-Rad dekodieren
Eingabe mit AEIOU enkodieren
Eingabe mit AEIOU dekodieren
Eingabe mit Za-Owies enkodieren
Eingabe mit Za-Owies dekodieren
Eingabe mit Karten-Kosak enkodieren
Eingabe mit Karten-Kosak dekodieren

ausführen

Ausgabe - Ergebnis der Berechnung / (De)-Chiffrierung / (D

50924 51015 84649 37846 75858 50925 09853 71585 74049 5725

HESLO PRO OTP



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

OT	PRIJEDE KONTAKT. PRIPRAVTE ZBOZI NA STREDU.																																																														
OT (číslený)	5	0	9	2	4	5	1	0	1	5	8	4	6	4	9	3	7	8	4	6	7	5	8	5	8	5	0	9	2	5	0	9	8	5	3	7	1	5	8	5	7	4	0	4	9	5	7	2	5	8	3	8	5	8	6	7	9	1	0	5	2	5	8
Heslo	1	4	3	5	8	8	9	7	5	3	2	4	1	3	3	4	0	1	6	9	2	6	7	9	9	7	6	9	0	9	2	2	7	6	4	1	2	3	1	4	8	5	8	3	3	2	7	3	8	5	1	2	5	3	6	4	8	8	7	7	4	7	6
ŠT	6	4	2	7	2	3	0	7	6	8	0	8	7	7	2	7	7	9	0	5	9	1	5	4	7	2	6	8	2	4	2	1	5	1	7	8	3	8	9	9	5	9	8	7	2	7	4	5	3	3	4	0	0	1	2	1	7	9	7	2	6	2	4

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



Typický průběh vysílání číselné stanice

- úvodní znělka, hudba nebo charakteristický signál
- oznámení počtu číselných skupin a identifikace zprávy
- vlastní zpráva tvořená **pětimístnými číselnými skupinami**
- skupiny jsou vysílány hlasem v jazyce používaném stanicí
- začátek zprávy bývá označen identifikační skupinou (např. **19**)
- konec zprávy může být označen skupinou **99999** nebo slovem „**konec**“
- po odvysílání všech zpráv následuje odhlášení stanice



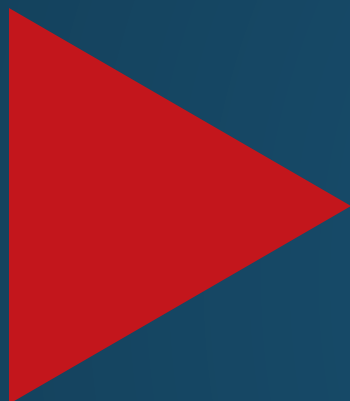
***Předehra* 13 19 13 19**

64272 30768 08772 77905 91547 26824

21517 83899 59872 74533 40012 17972

62430 konec 99999 konec vysílání

[illegible]



Děkuji za pozornost

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

