

Šifrování – historické zajímavosti



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Prvopočátky

- Egypt
 - 1900 př.n.l.
- Mezopotámie
 - 1500 př.n.l.



ATBASH

- Substituční šifra
 - Židé, 500 př.n.l.
 - A je T, B je SH, atd.
 - V náboženských textech: Sheskakh je Bavel (babylon)

The ATBASH Cipher

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת
ת ש ר ק צ פ ע ס נ מ ל ב י ט ח ו ה ד ג ב א

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

Skytale

- Transpoziční šifra
 - Řecko, Sparta, 500 př.n.l.
- Počátky šifrování v armádě

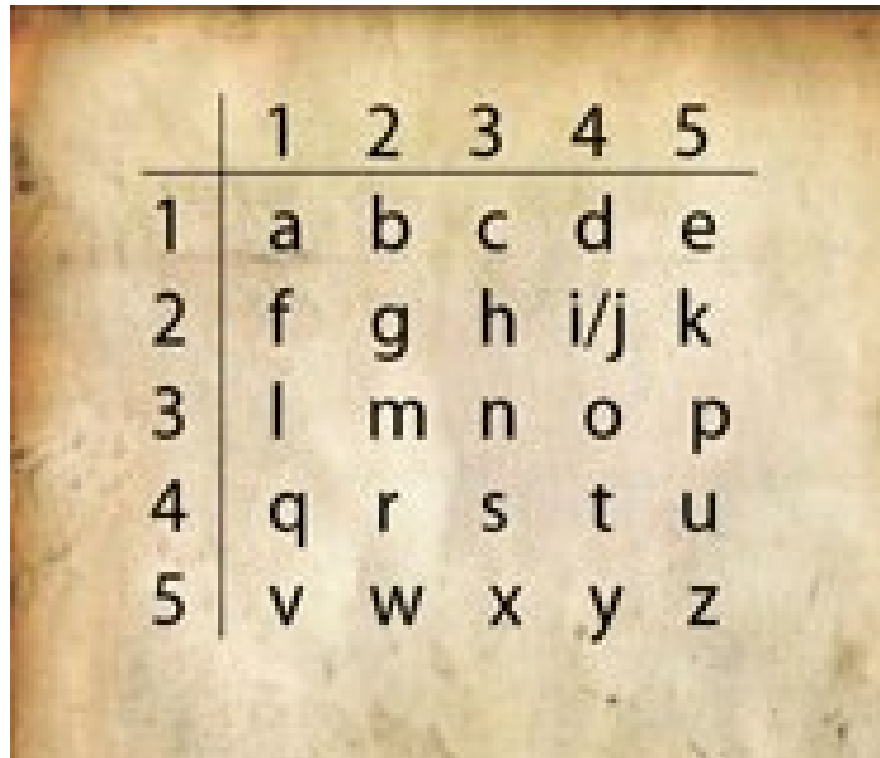


Steganografie



Polybiův čtverec

- Substituce + steganografie
 - Řecko, 200 př.n.l.



The image shows a photograph of a historical document, likely a manuscript, featuring Polybius's square cipher table. The table is a 5x5 grid of letters, with a vertical line separating the row numbers (1-5) on the left from the column letters (a-z) on the top. The letters are arranged in a specific order: Row 1: a, b, c, d, e; Row 2: f, g, h, i/j, k; Row 3: l, m, n, o, p; Row 4: q, r, s, t, u; Row 5: v, w, x, y, z. The document has a yellowed, aged appearance.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Ceasarova šifra

- Klasická monoalfabetická substituce s pevným posunem abecedy o 3
 - Řím, 50 př.n.l.
- Opravdu používaná Juliem Ceasarem

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

Kámasútra

- Indie, 4. století
- Šifrování jako prostředek k uchování tajemství milostné korespondence



Frekvenční analýza

- Základní statistické metody
 - Arabové
 - 9. století

[illegible]

ثم الأدلة - ولله الحمد - والعالي هو العلم به محمد وآل بيته ع

[illegible]

První šifrování v Čechách

- Jan Hus
- Jednoduchý
substituční systém
- ABECEDA →
BBFCFDB



Složitější substituce

- Polyalfabetická substituce
 - Leon Battista Alberti
 - 1467
 - různé substituce pro různé části zprávy
 - šifrovací zařízení



Tabula recta (Vigenérova tabulka)

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

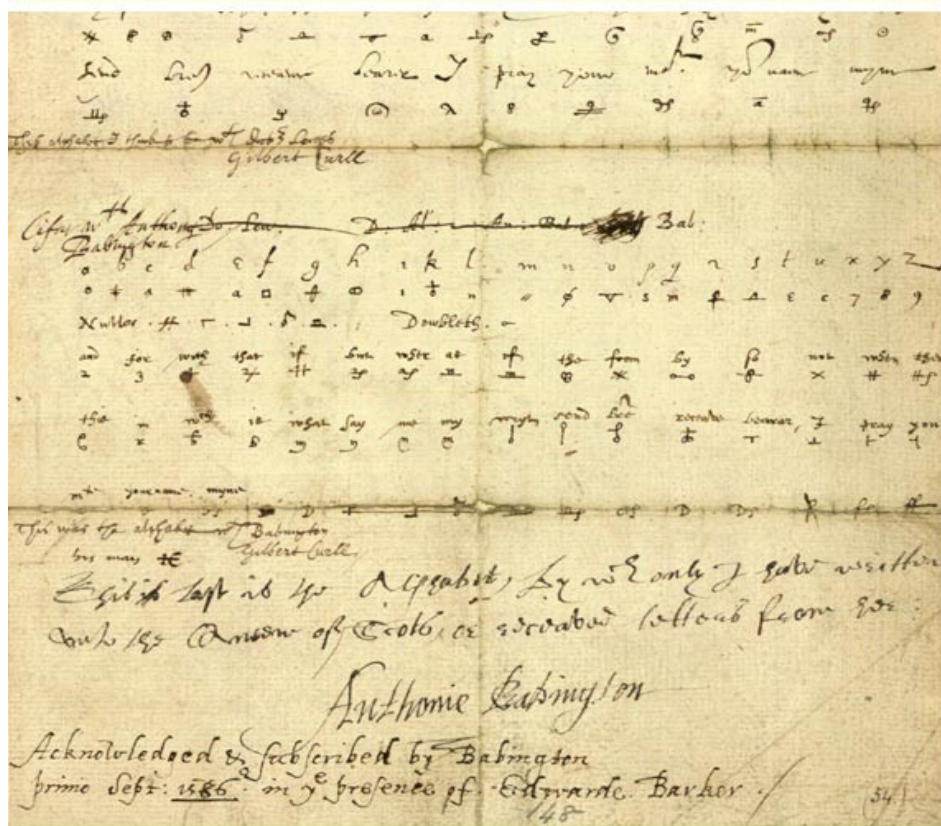
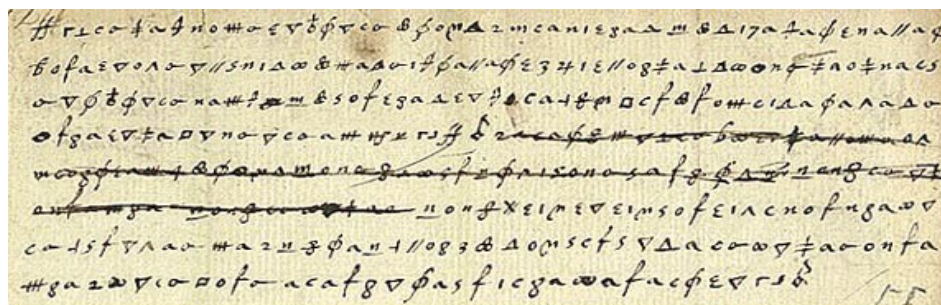
Šifrování podle hesla

- Polyalfabetická substituce
 - Giovan Batista Belaso, 1553
 - Vigenérova šifra
 - Metoda jejího rozluštění až v polovině 19. století

```
aliceabobmajitajemství  
tajnyklíctajnyklíctajn  
-----  
TLRPCKMWFASVRKUMOLTEV
```

Marie Stuartovna

- Popravena kvůli rozluštěné šifře
 - 16. století



Baconova šifra

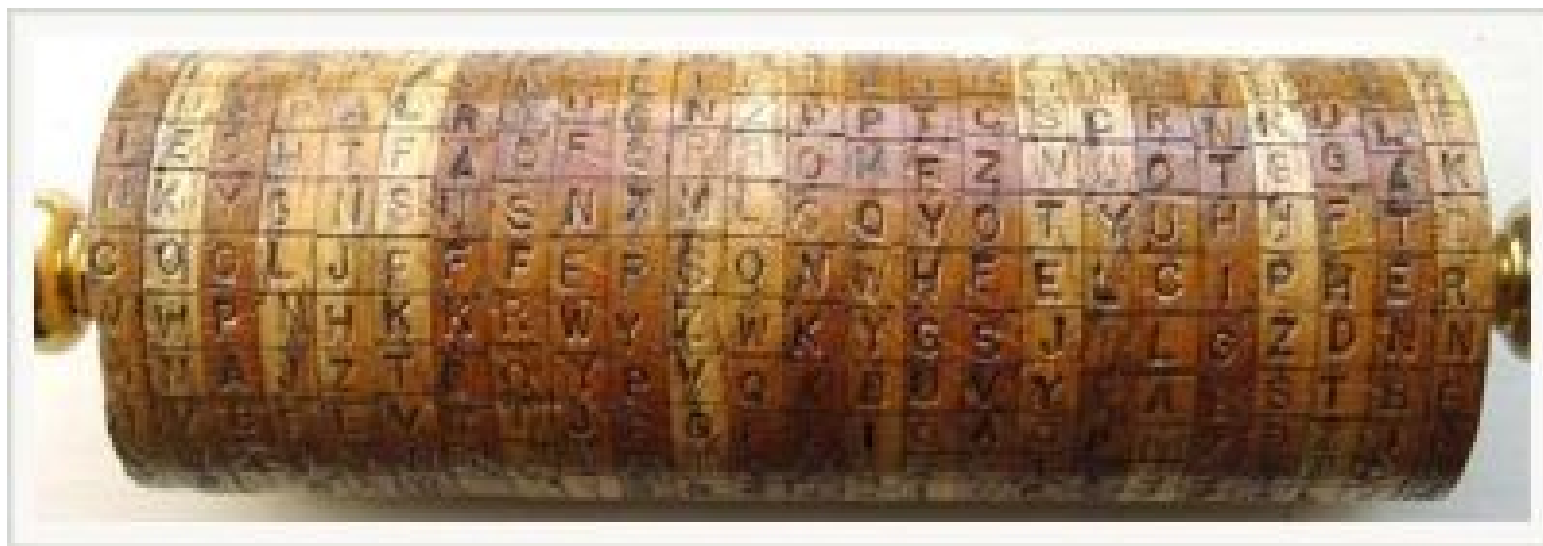
- Francis Bacon,
 - 16-17 století
- 5 bit binární kód
- Steganografie

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

- Jedno písmeno kodovano pomocí 5 znaků, na pet znaků se používaly dva různé fonty

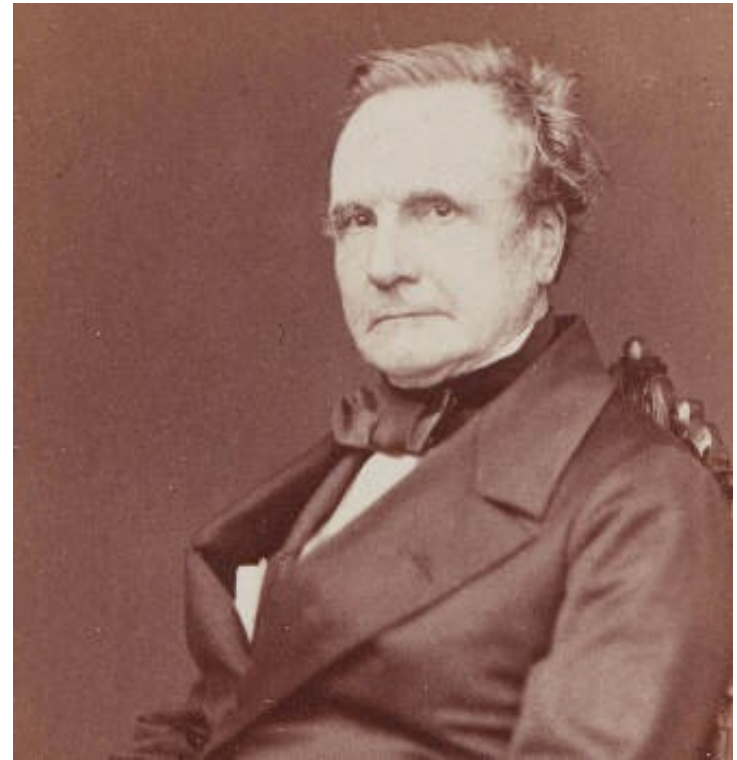
Jeffersonův váleček

- Americká občanská válka (1861 - 1865)
- Unie



Rozluštění Vigeněrový šifry

- Polovina 19. století
- Charles Babbage nebo Friedrich Kasiski?
- Babbage –
matematická notace



Playfair

- 1854
- Vymyslel Charles Wheatstone, popsal Lyon Playfair
- Používaná ještě za druhé světové války

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

Kerckhoffovy principy

- Principy v bezpečného šifrování
- Auguste Kerckhoff, 1883



Gold-Bug

- Příběh Edgara Allana Poa
- Úspěch povídky je založen na cetrálním kryprogramu
- Popularizace tématu šifrování



Legenda o Bealově pokladu

- Beale, hostinec, bedna, tři šifry a poklad
- Poklad nikdy nenalezen

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975,
14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485,
604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401, 370,
11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500,
538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283,
118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21,
24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131,
160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62,
116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568,
614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4,
30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461,
44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216,
728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5,
81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86,
36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985,
233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62,
194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895,
10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62,
31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31,
86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216,
548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56,
216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617,
84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18,
212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88,
612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132,
40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936,
447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216,
814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84,
221, 736, 820, 214, 11, 60, 760.

Šifrování veřejnosti

- Steganografie
- Pomocí špendlíku vypíchaná písmena v novinách



1.světová

- Rádio
- Playfair
- Kódové knihy



Mata Hari



Room 40

- Rozluštění šifry zařídilo zapojení USA do války

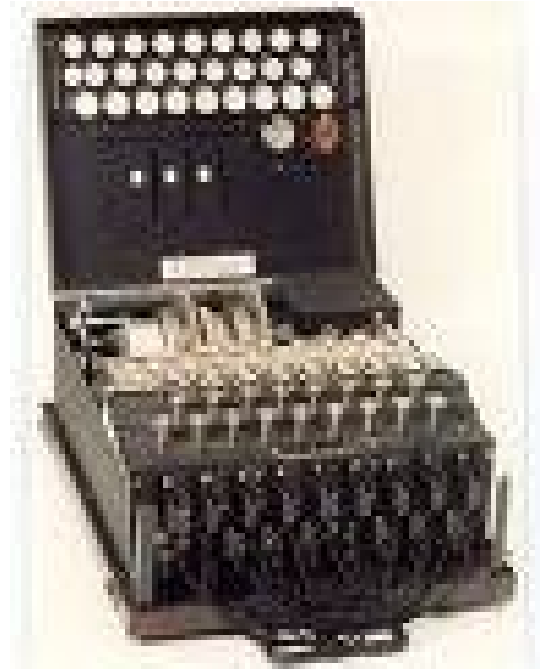


2. světová válka

- Posun od kryptologů-lingvistů ke kryptologům-matematikům
- Mechanizace šifrování
- Něco ale stále pořád tužka papír – playfair



Sigaba, Typex, Purple, Enigma



Enigma & Bomb

- Klávesnice
 - Tři rotory
 - Reflektor
 - Propojovací desky
 - Panel žárovek
-
- Stisk klávesy → rotory → reflektor → rotorz → propojovací deska → rozsvícení žárovky

Navajo

- Pseudošifra Američanů



Steganografie

- Tečka na konci věty



Současnost

- Rozvoj počítačů → velmi rychlý rozvoj kryptografie

Zdroje

- Šifry a hry s nimi. Tomáš Hanžl, Radek Pelánek, Ondřej Výborný. Portál, 2007.
- The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. David Kahn. 1996.