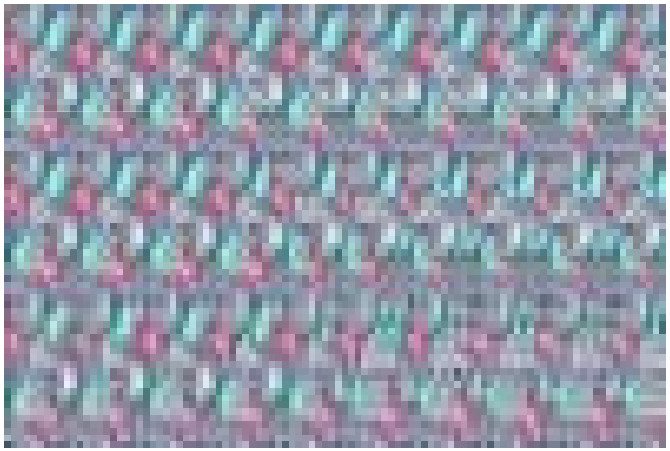
16. 5. 2019

Petra Konečná

Zajímavosti z kryptologie

VF

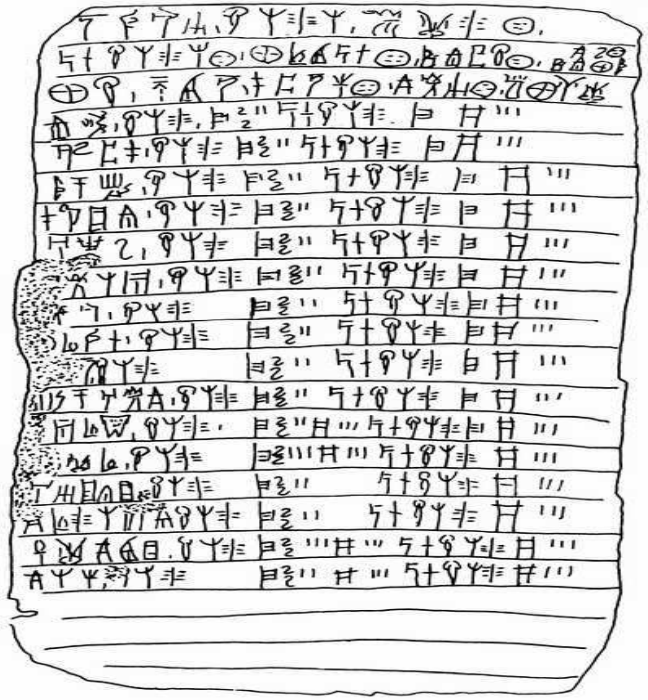
O co se (ne)jedná



http://commons.wikimedia.org/wiki/Category:Quick_Response_Codes
AutorScrawler

http://www.math.umn.edu/~rogness/visualization.shtml

O co se (ne)jedná



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	.	?

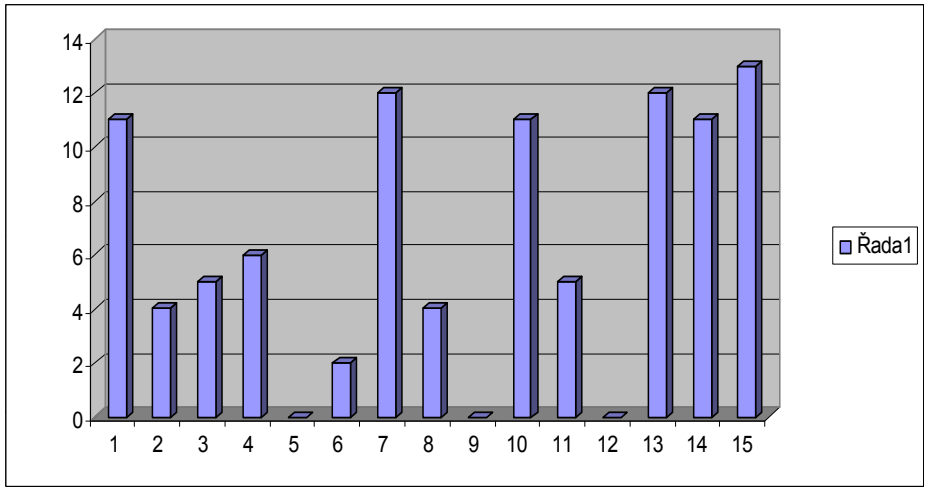
O co se (ne)jedná

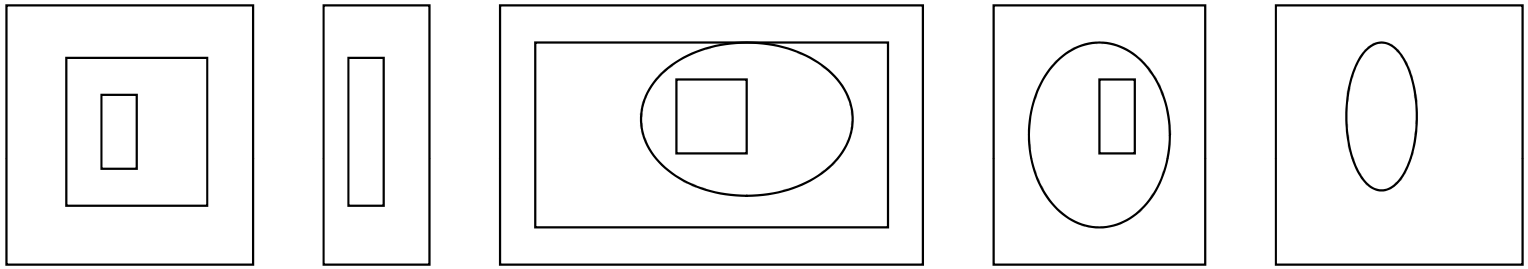
♫♪|♫♫♫|♫|♪♪|♫♪♫♪|♫♪♫|♫♪♫♫|♫♫♪♪♫♫
|♫|♫♫♫|♫|♪♫|♫♪♫|♫♪♫♫|♫♪|♪|♫♪|♪♪|
♪♪♪|♪♫♫♪|♪♫|♫|♫♪|♪|♫♫♪♪♫♫|♫♫♪♪|♪|
♪♪♫♫♪♪|

11233424

0010000000010100

O co se (ne)jedná





O co se (ne)jedná

- **Kódování**

  Zobrazení ze zdrojové abecedy do množiny všech slov nad kódovou abecedou.

  Stále se jedná o tzv. otevřenou zprávu, kterou příjemce čte

- **Kód**

  Množina všech kódových slov tj. obrazů zdrojových znaků v daném kódování.

- **Dekódování**

O co se (ne)jedná

Převedení čísla 2019 do binární číselné reprezentace.

Princip

$$a = b_3 \cdot 2^3 + b_2 \cdot 2^2 + b_1 \cdot 2^1 + b_0 \cdot 2^0$$

2019 ➡ 0010000000011011

a	$b_3\ b_2\ b_1\ b_0$
0	0 0 0 0
1	0 0 0 1
2	0 0 1 0
3	0 0 1 1
4	0 1 0 0
5	0 1 0 1
6	0 1 1 0
7	0 1 1 1
8	1 0 0 0
9	1 0 1 1

O co se (ne)jedná

- **Kryptografie**

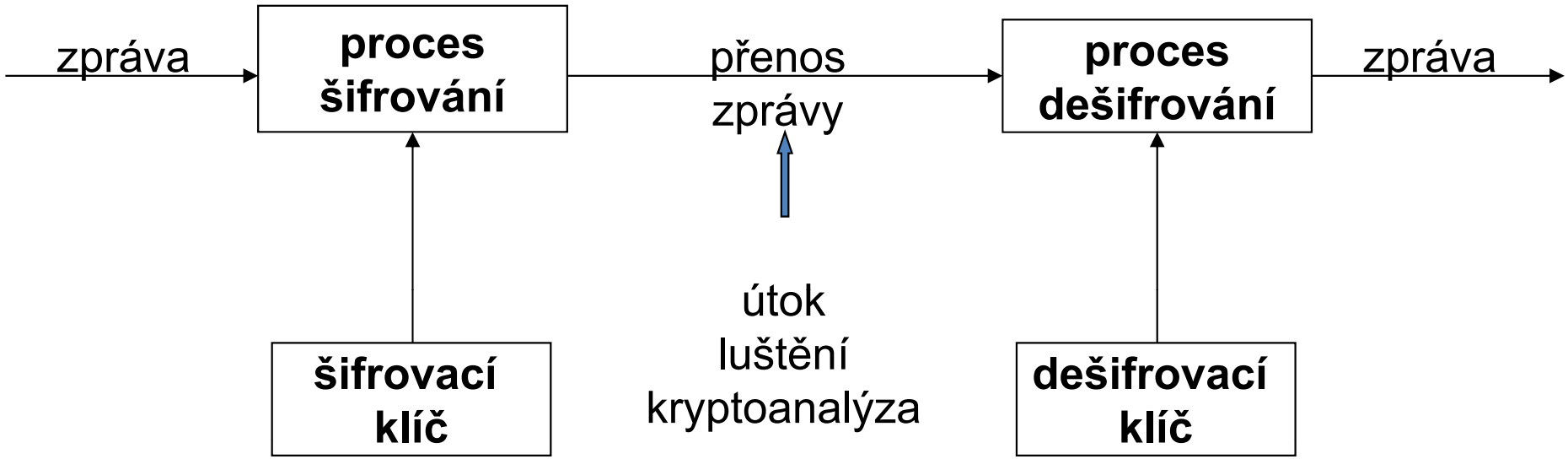
  Otevřený text převádíme na tzv. šifrový text (zkráceně šifra) za účelem utajení.

  Příjemce zprávy šifru zpětně dešifruje.

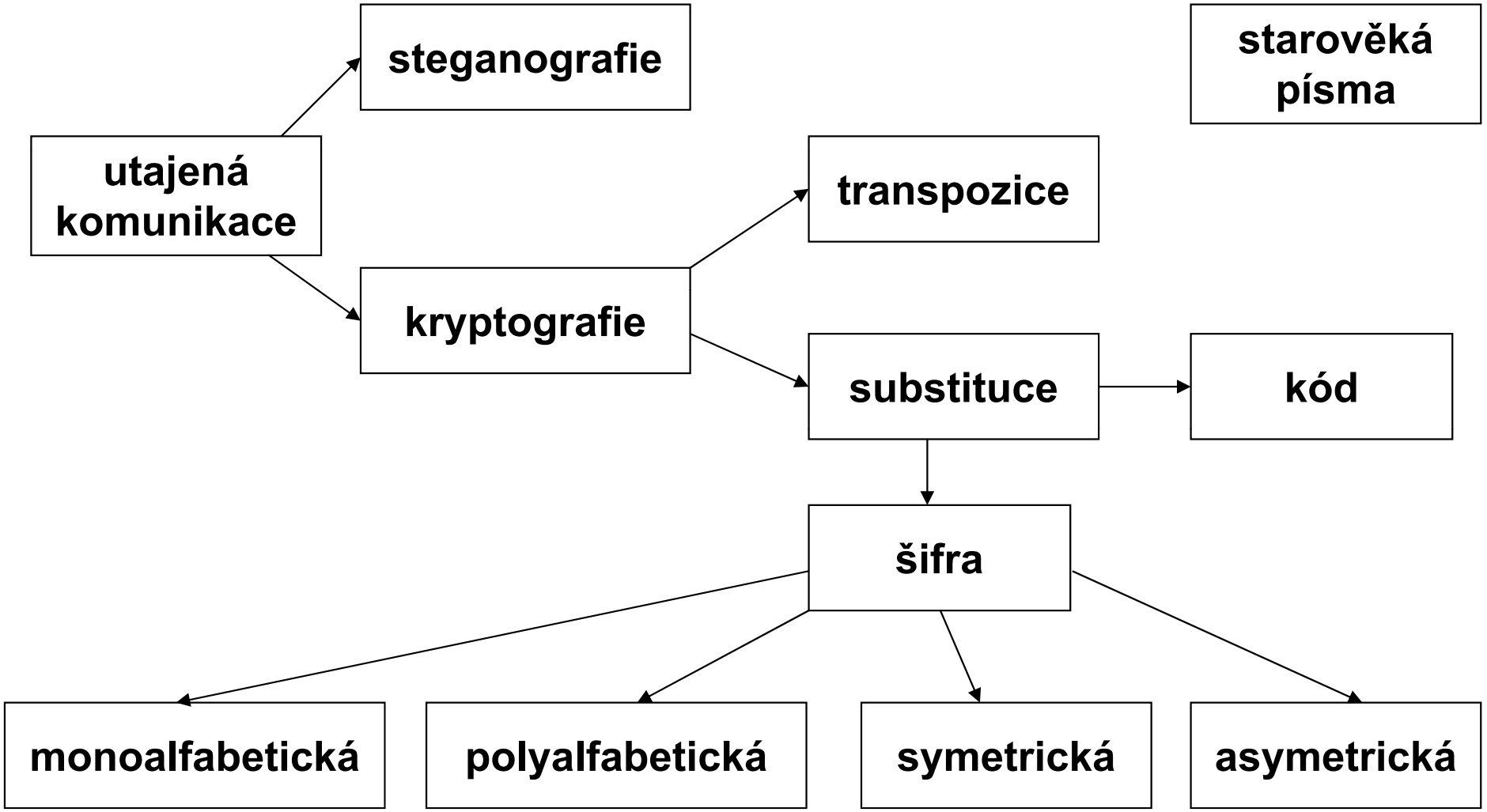
- **Kryptoanalýza**

  Útočník se snaží šifru vyluštit (= rozbít).

O co se (ne)jedná



Způsoby tajné komunikace



3000
př. n. l.

Hieroglyfy

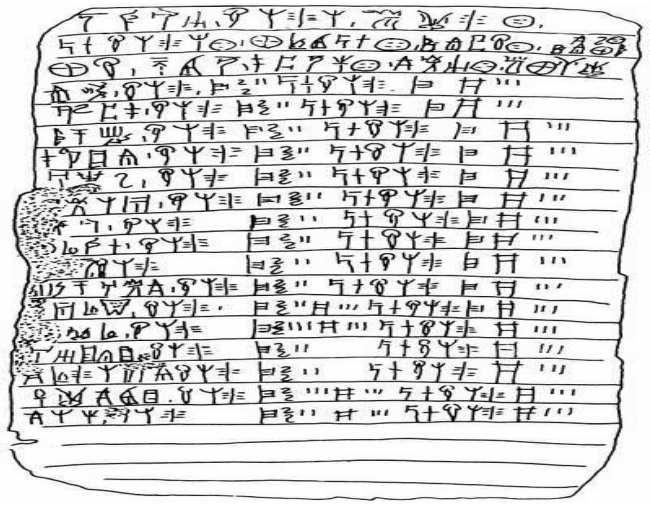
- vznik okolo roku 3000 př. n. l.
- používání asi do roku 400 n. l.
- 1400 let byly pro svět nečitelné
- považováno za obrázkové písmo
- 1799 nález Rosetské desky
- 1814 Thomas Young
- 1824 Jean-Francois Champollion

http://cs.wikipedia.org/wiki/Rosettsk%C3%A1_deska

3000 př. n. l

1700 př.n.l.

Lineární písmo

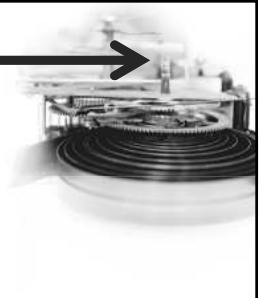


Lineární písmo B – hliněná tabulka

Disk z Faistu, kolem r.1600 př. n. l.

- Lineární písmo A (1750 – 1450 př. n. l.)
- Lineární písmo B (1300 – 1100 př. n. l)
- Arthur Evans (19./20. st.)

1700
př.n. l.



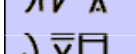
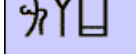
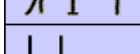
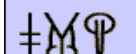
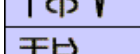
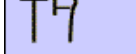
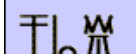
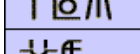
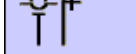
Lineární písmo

- Základní předpoklad – není na základě řečtiny
- 40. léta 20. st.
- **Alice Koberová** (1907 – 1950) - slabičné písmo
- **Michael Ventris** (1922 – 1956) – příbuznost se starou řečtinou
- **1953 John Chadwick + Michael Ventris** – rozluštění Lineárního písma B

1700
př.n. l.

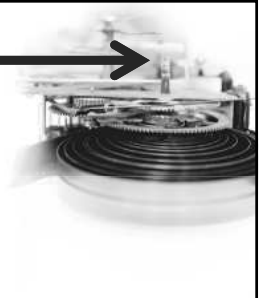
Lineární písmo

Ventrisova tabulka

následnost znaků	transkripce	Mykénská řečtina	Klasická řečtina	význam slova
	ku-mi-no	*kuminon	kuminon	kmín
	ku-na-ja	*gunaia	gune	žena (gynekologie)
	ku-ru-so	*khrusos	khrusos	zlato (chryzantéma)
	pa-te	*pater	pater	otec
	pa-ma-ko	*pharmakon	pharmakon	lék (lékárnička)
	to-so	*toso	tosos	tak moc
	to-ra-ke	*thorakes	thorax	hruď
	qo-u-	*gwou-	bou-	kráva
	i-qo	*hikkwoi	hippos	kůň
	re-u-ka	*leuka	leukos	bílá (leukémie)
	re-a	*rea	rhis, rhino-	nos (plastika nosu)

Příklady slov v Lineárním písmu B

1700
př.n. l.



Písma starých civilizací

další rozluštěná písma

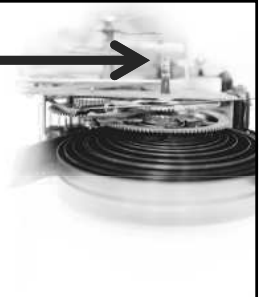
- babylonské klínové písmo
- turecké runy
- indické slabičné písmo brahmí

vybraná nerozluštěná písma

- Lineární písmo A
- Krétské hieroglyfy
- Rongorongo (Velikonoční ostrov)

1700 př.n.l.

500 př. n.l.



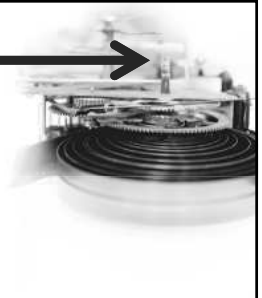
Steganografie

- ukrytí zprávy
- steganos = schovaný,
- graphein = psát
- psací destičky s voskem, zpráva tetovaná na hlavě otroka (Herodotos: Dějiny)

Čína – hedvábná kulička

obrazce Nazca (?)

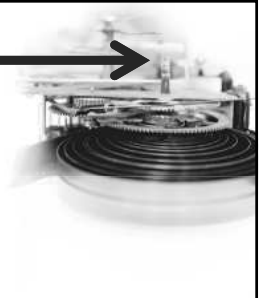
500
př.n.l.



Steganografie – tajné inkousty

- Roztok - bezbarvý za normálních podmínek
- Organické látky (moč, mléko, šťáva z citrusů či jiného ovocem ocet) – působením tepla zhnědnou
- Chemické látky (jiné než organické) – teplem, chemickou reakcí, UV zářením či infračerveným světlem

500
př.n.l.



Steganografie

Moderní metody steganografie

- Tajné inkousty (1. sv. válka)
- Fotografické metody – zmenšování (2. sv. válka)
- šumy ve zvukových i obrazových souborech
- Otevřené kódy

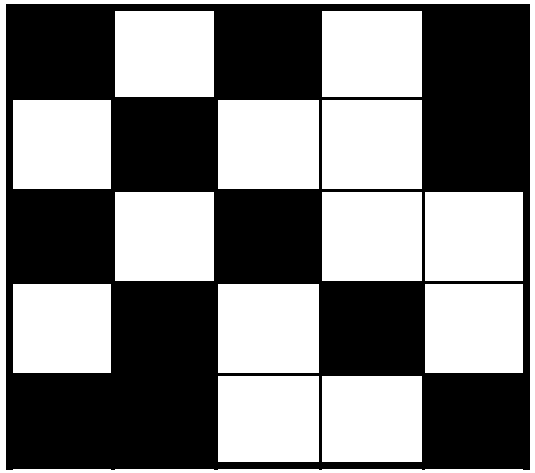
JAK S**E** **D**OSTANU D**N**ES **O**BJÍŽĎKOU S O**T**AKAREM DO **A**UTOOPRAVNY?

500
př.n.l.

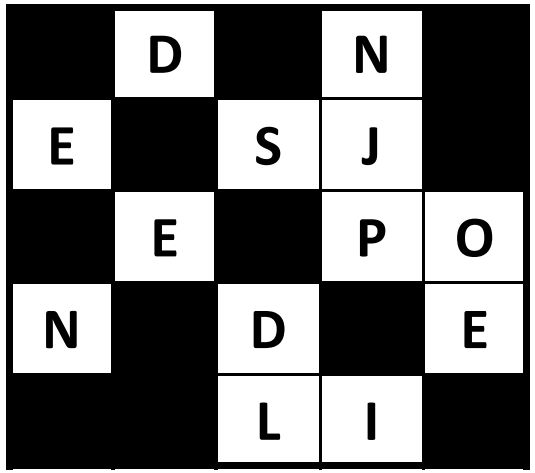
Steganografie

- šifrovací mřížka

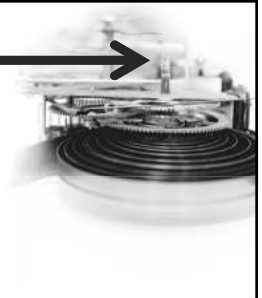
	D		N	
E		S	J	
	E		P	O
N		D		E
		L	I	



I	D	I	N	D
E	R	S	J	L
A	E	E	P	O
N	S	D	W	E
C	Z	L	I	K



500
př.n.l.



Transpozice

- permutace písmen otevřeného textu
- Skytala (Sparta, 500 př. n. l.)

- plot: SAAPSRSLTKKLEOEPO

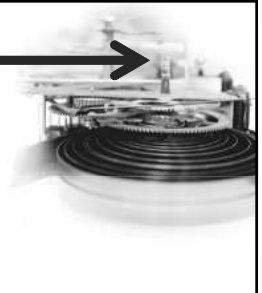
  S A A P S R S L T

  K K L E P E P O

- přesmyčky

  OT NINE LISPRI PEBEZCNA FRASI

500
př.n.l.

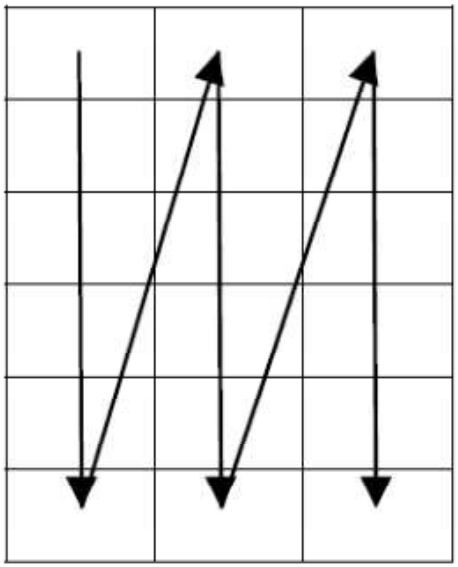


Transpozice

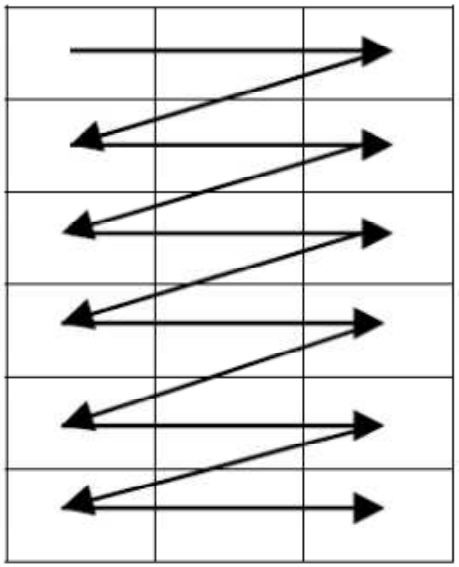
- Transpozice s využitím geometrického rozmístění.

Otevřený text: TRANSPOZICNI SIFRA 3

Transpozice:

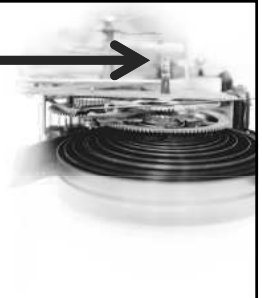


T	O	S
R	Z	I
A	I	F
N	C	R
S	N	A
P	I	3



Výsledná šifra: TOSRZIAIFNCRSNAPI3

500
př.n.l.



Transpozice

- Transpozice s využitím klíče.

Otevřený text: KRYPTOLOGIE JE VEDA O SIFRACH

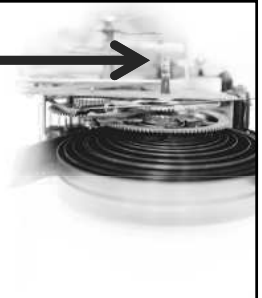
Transpozice dle klíče JCMF při vepisování zprávy po sloupcích:

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

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

Výsledná šifra: ORKEGARDICYAEHPOJXTSEYOIVZLF

500
př.n.l.



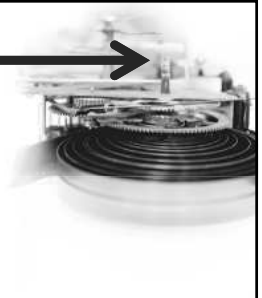
Transpozice

- Cardanova mřížka (zašifrován text Geronamo Cardano)

I3	F2		C2	**A1**	
	H3	**B1**	G3		F3
C1	G2	E2	E3	B2	**D1**
D3		**E1**			C3
F1	H2	**G1**	B3	**H1**	A2
I2	A3		D2		**I1**

E	**A**	A	**R**	**G**	A
C	**M**	**E**	**A**	C	**T**
R	**D**	**A**	**I**	**N**	**O**
K	E	**L**	F	G	**X**
A	**O**	**M**	**X**	**O**	**M**
A	**X**	H	**T**	I	**C**

500
př.n.l.

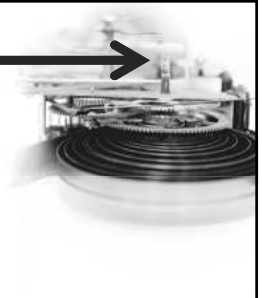


Transpozice

- klíč = určující permutace písmen.
- bezpečnost klíče

  počet možností seskupení zprávy = počet permutací
- bezpečnost transpoziční šifry roste s délkou zprávy
- slabina šifry = pravidelnost klíče, charakteristika jazyka.

500 př.n.l. 400 př.n.l.



Substituce

- substituce písmen abecedy otevřeného textu písmeny jiné abecedy (šifrová abeceda)
- **Kámasútra** (400 př. n. l.)

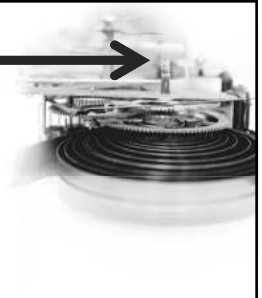
  umění Mlecchita – Vikalpa

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

SEJDEME SE V ZAHRADE ZA SOUMRAKU. BUDE BEZPECNO.

KZQBZEZKZNUXPJXBZUXKGMEJXVMAMBZAZUHZYFG

400 př. n.l. 200 př. n.l.



Polybiův čtverec

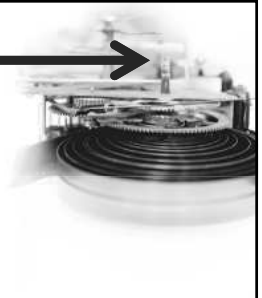
- řecký politik **Polybios** (cca 200 př.n.l.)

  dílo - Historiai (Dějiny)

	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

AHOJ →→ 11233424

200
př.
n.l.

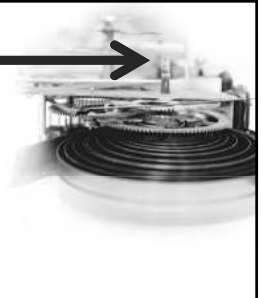


Polybiův čtverec

Možnosti vysílání Polybiova čtverce:

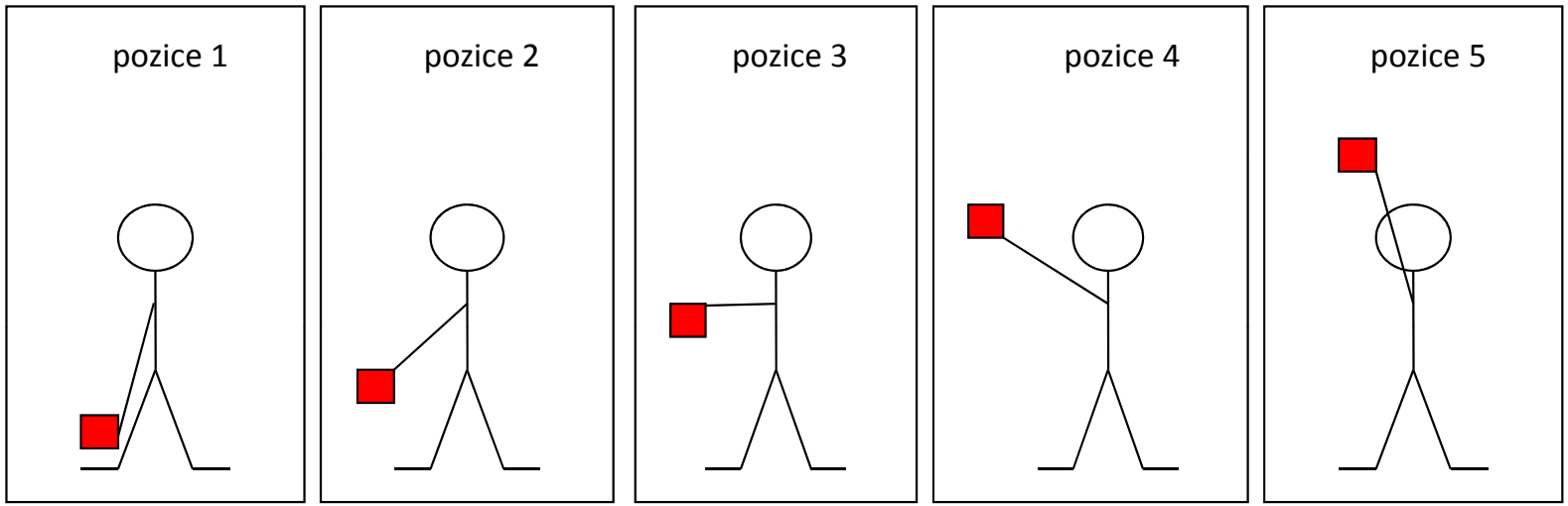
- hořící louče
- vlajková signalizace

200
př.
n.l.

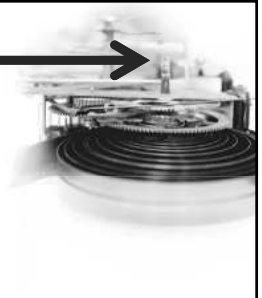


Polybiův čtverec

V každé ruce máme jinou vlajku (pro lepší rozlišitelnost na dálku). Na každé straně můžeme mít 5 poloh ruky = vlajky.

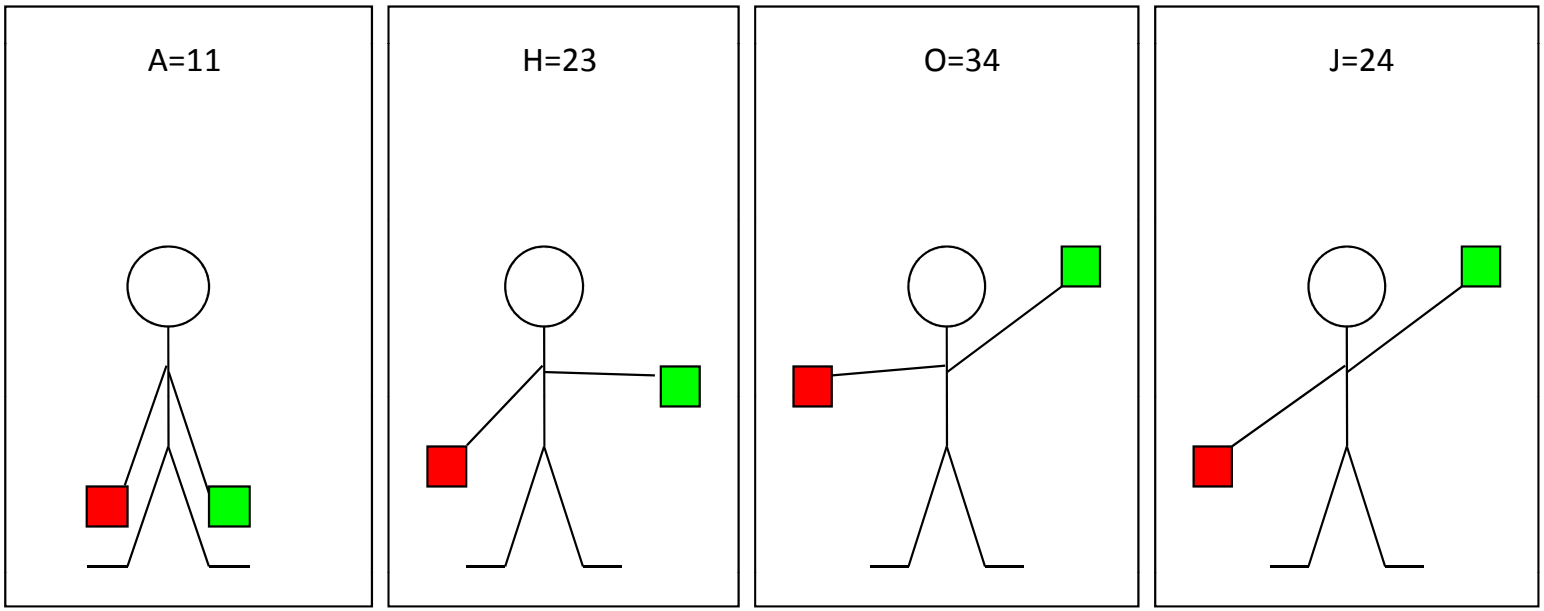


200
př.
n.l.

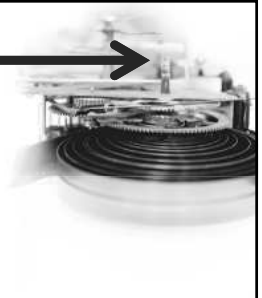


Polybiův čtverec

Například zpráva **AHOJ** by byla vysílána následovně:

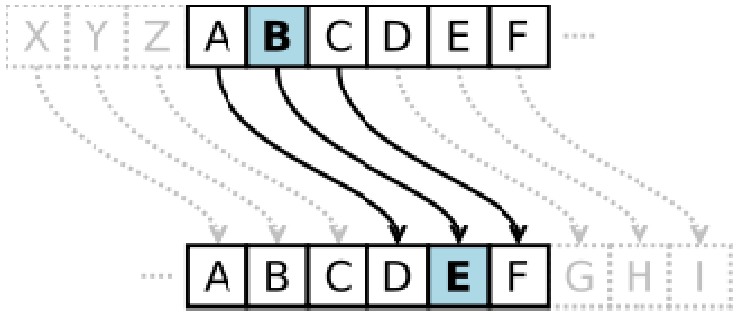


200 př.n.l. 50 n.l.



Substituce

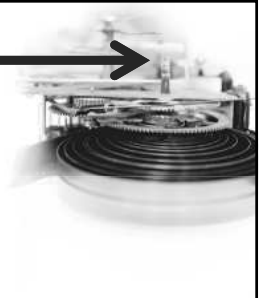
- **Caesarova šifra** (50 n.l.)



MYOLYVFDHVDYCDSLVNBRZDOFHJDOVNH

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

JULIUSCAESARZAPISKYOVALCEGALSKE



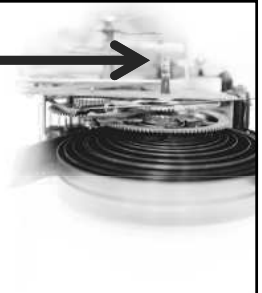
Substituce

- **Substituce s využitím klíčového slova**

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

- **Afinní šifra**

otevřená zpráva	x	$5x + 9$	$5x + 9\ (mod\ 26)$	šifra
M	12	69	17	R
O	14	79	1	B
D	3	24	24	Y
U	20	109	5	F
L	11	64	12	M

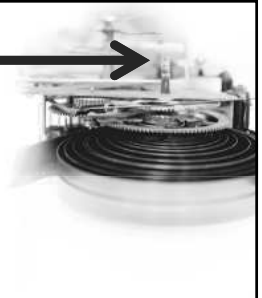


Substituce

- bezpečnost šifry = počet klíčů
- Caesarova šifra 26 klíčů
- Obecná substituční šifra 26! klíčů

50. n.l.

9. st. n.l.

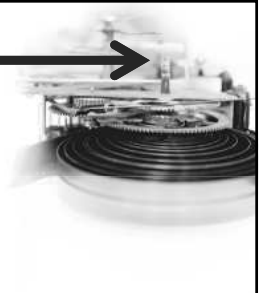


Frekvenční kryptoanalýza

- zlatý věk islámské civilizace (po roce 750 n.l.)
- časté používání šifer
- našli mechanismus na rozluštění zprávy bez znalosti klíče = jsou zakladateli kryptoanalýzy
- metody matematiky, statistiky a lingvistiky

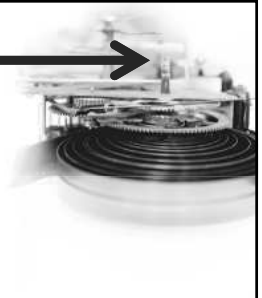
- vychází z relativní četnosti znaků v šifře a porovnává ji s četnostmi znaků otevřených textů daného jazyka

9. st.
n.l.



Charakteristika českého jazyka

písmeno	frekvence	písmeno	frekvence
A	8,6	N	6,8
B	1,7	O	8,0
C	3,3	P	3,2
D	3,6	Q	0,0
E	10,5	R	4,9
F	0,2	S	6,3
G	0,2	T	5,1
H	2,2	U	4,0
I	7,5	V	1,3
J	2,2	W	0,0
K	3,6	X	0,1
L	4,2	Y	2,8
M	3,5	Z	3,2



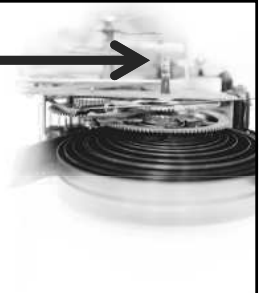
Frekvenční kryptoanalýza

MYOLYVFDHVDYCDSLVNBRZDOFHJDOVNH

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

Nejčetnější písmeno v šifře je D, v českém jazyce by mu mělo odpovídat písmeno E. Provedeme-li posun, dostaneme nesmyslnou zprávu NZPM...

Zkusíme tedy další písmeno s nejvyšší četností jako náhradu za E to je A, potom provedeme posun a získáme původní zprávu.

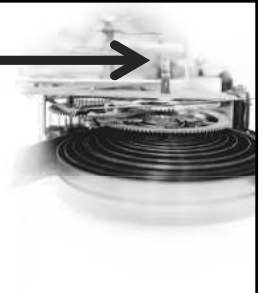


Frekvenční kryptoanalýza

Význam

Všechny doposud známé šifry byly od objevení metody kryptoanalýzy rozluštitelné.

Byla prolomena transpoziční i **monoalfabetická substituční šifra**



Frekvenční kryptoanalýza

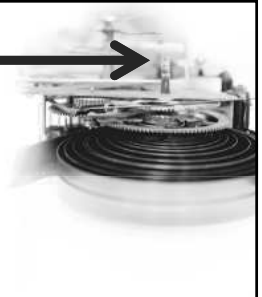
- **klamač** – bezvýznamná vsuvka, symbol sloužící pro zmatení kryptoanalytika

- **nomenklátor** – kombinace použití šifrové abecedy a kódových slov

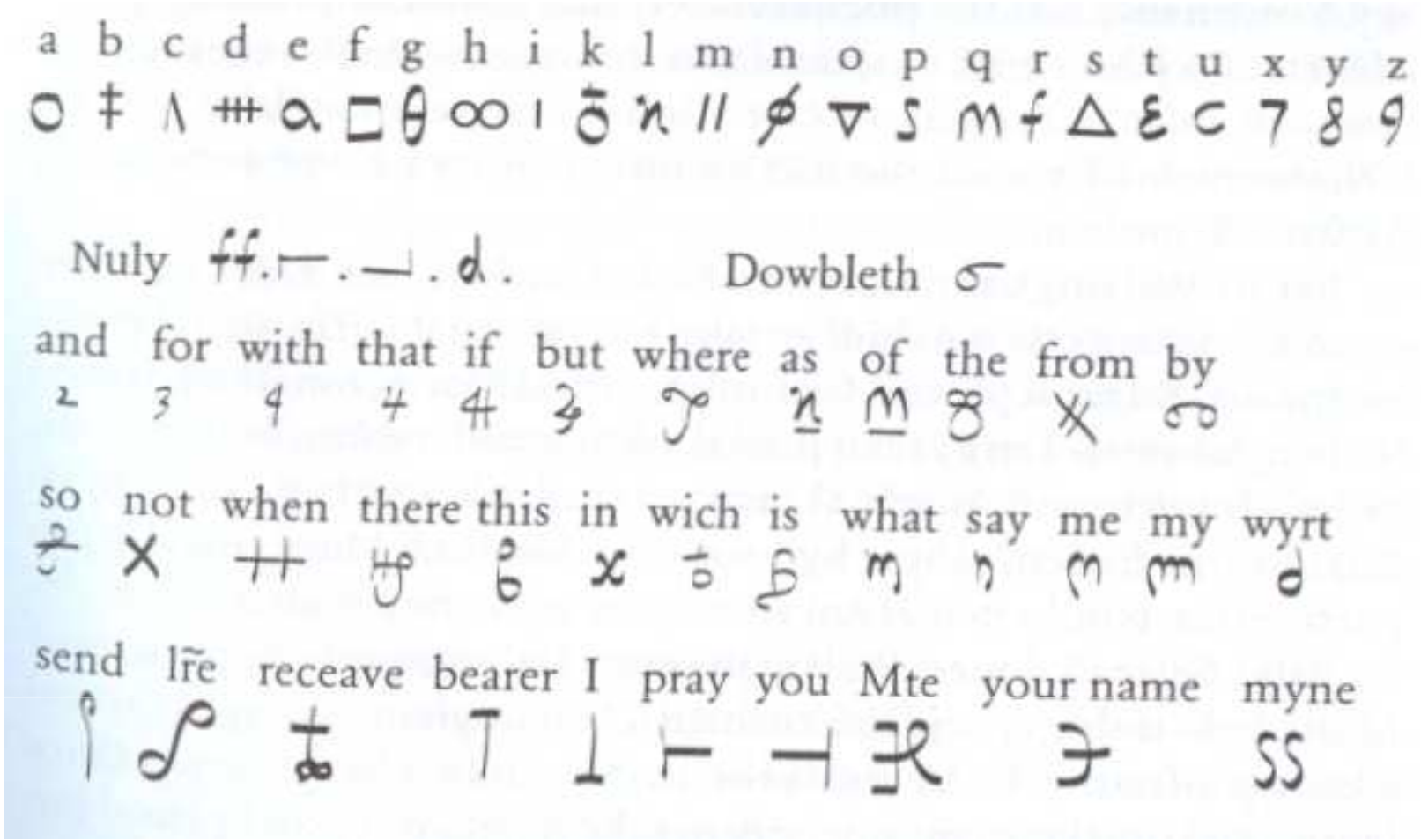
- **homofonní substituční šifra** – každé písmeno nahrazeno systémem reprezentantů, jejichž počet odpovídá frekvenci výskytu písmene v otevřeném textu

9. st. n.l.

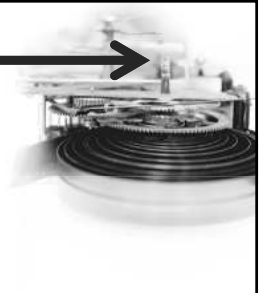
16. st. n.l.



Šifra Marie Stuartovny



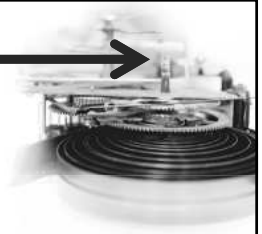
16. st.
n.l.



Polyalfabetická substituční šifra

- Leon Battista Alberti (1. pol. 15. st.)
- Johannes Trithemius
- Giovanni Porta

- Blaise de Vigenére – **Vigenérův čtverec** (1586)
- využití slovního klíče pro postupné změny šifrové abecedy
- vzniká **polyalfabetická substituční šifra**



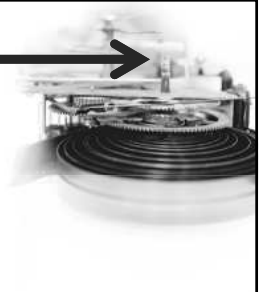
16. st.

n.l.

	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
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

16. st. n.l.

19 st. n.l.



Kryptoanalýza Vigenérovy šifry

- **Charles Babbage** (1854)
- **Friedrich Wilhelm Kasiski** (1863)

  postup:

  Hledáme opakující se sekvence znaků.

  Určujeme vzdálenosti mezi opakujícími se sekvencemi znaků.

  Hledáme jejich společné dělitele.

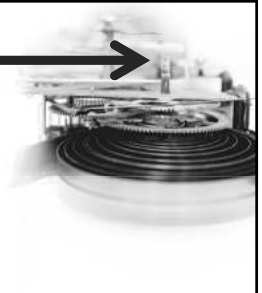
  Společní dělitelé jsou potencionálními délkami klíče.

  Rozdělíme text podle délky klíče do jednotlivých částí.

  Jednotlivé části jsou již monoalfabetickou substituční šifrou.

  Na každou část aplikujeme klasickou frekvenční kryptonalaýzu.

19 st.
n.l.



Morseovka

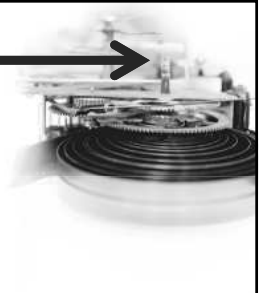
- **Samuel Finley Breese Morse** (1791 – 1872)

  americký vynálezce, malíř a sochař

- první telegrafické spojení mezi Washingtonem a Baltimorem (24.5.1844), „What hath God wrought“

- současný stav abecedy – 1918 – Philips (sjednocení americké a anglické verze)

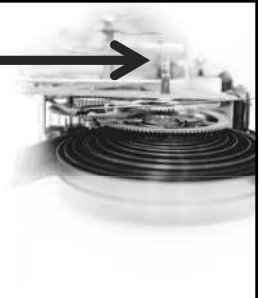
19 st.
n.l.



Morseovka

- Skupina symbolů používána v telegrafii;
- Kóduje znaky latinské abecedy, číslice a speciální znaky do kombinací krátkých a dlouhých signálů;
- Možnosti přenosu = akustický signál (pískání), elektrický signál (telegraf), optický signál (signalizace vlajkami, záblesky světla, záznam na papír a pod.)

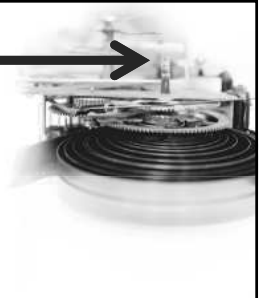
19 st.
n.l.



Morseovka

A	• -	akát
B	- •••	blýskavice
C	- • - •	cílovníci
D	- ••	dálava
E	•	erb

19 st.
n.l.

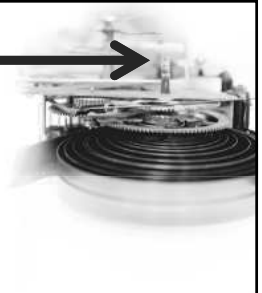


Morseovka

- Při volbě kódování byly znaky voleny tak, aby nejfrekventovanějším písmenům (v angličtině) odpovídaly nejkratší sekvence teček a čárek.

- Zdrojovou abecedou je A = {a, b, c, d, e, f, g, h, ch, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z} a kódovou abecedou je tříznaková množina B = (- , •, /)

19 st.
n.l.

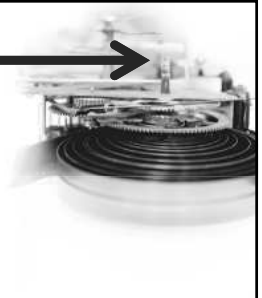


Morseovka

- **Signál SOS** (•••/ - - - / •••) je nejznámější tísňový signál vysílaný v Morseově abecedě oficiálně přijat v platnost v Německu 1905.

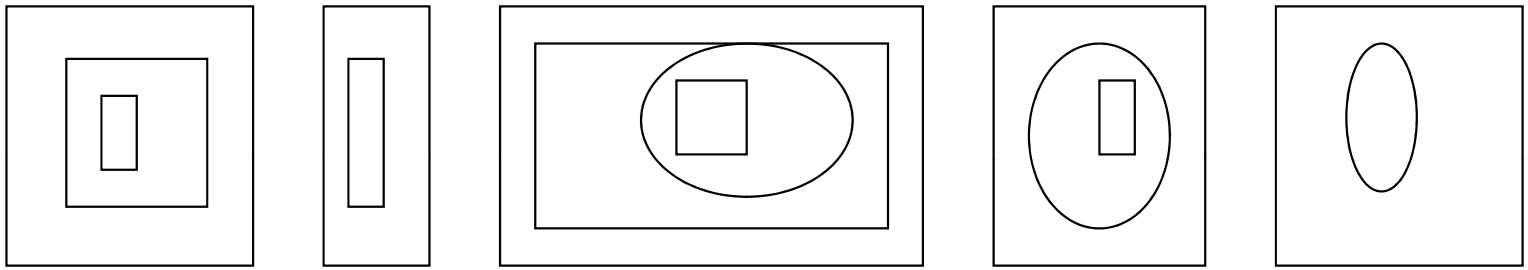
- Často se tvrdí, že SOS je akronymem pro anglickou větu Save Our Souls (Spaste naše duše), ale nebylo tomu tak.

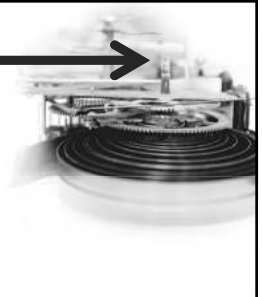
19 st.
n.l.



Morseovka

♫♪|♫♫♫|♫|♪♪|♫♪♫♪|♫♪♫|♫♪♫♫|♫♫♪♪
♫♫|♫|♫♫♫|♫|♪♫|♫♪♫|♫♪♫♫|♫♪|♪|♫♪|
♪♪|♪♪♪|♪♫♫♪|♪♫|♫|♫♪|♪|♫♫♪♪♫♫|♫♫♪♪
|♪|♪♪♫♫♪♪|





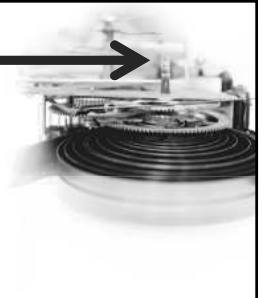
Vernamova šifra

- Vernamova šifra = jednorázová tabulková šifra
- délka klíče odpovídá délce zprávy
- použití náhodně generovaných klíčů a pouze jedenkrát
- absolutně bezpečná šifra
- nepraktické, náročné pro použití

ADFGVX

- německá šifra
- začala se používat v roce 1918
- příklad smíšené šifry

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

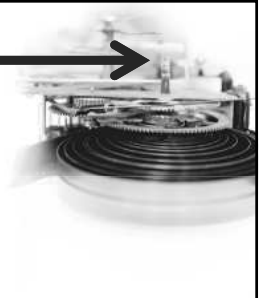


ADFGVX

- ZAJIMAVOSTIZKRYPTOLOGIE

Z	A	J	I	M	A	V	O	S	T	I
VD	AX	FF	DD	AF	AX	GG	FV	DA	GD	DD

Z	K	R	Y	P	T	O	L	O	G	I	E
VD	AV	DG	VA	FX	GD	FV	FG	FV	FA	DD	AD

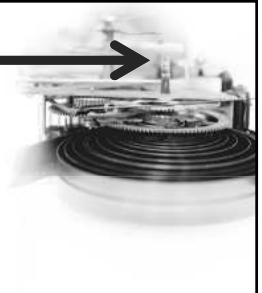


ADFGVX

- klíč = JARO

J	A	R	O
V	D	A	X
F	F	D	D
A	F	A	X
G	G	F	V
D	A	G	D
D	D	V	D
A	V	D	G
V	A	F	X

J	A	R	O
G	D	F	V
F	G	F	V
F	A	D	D
A	D		



ADFGVX

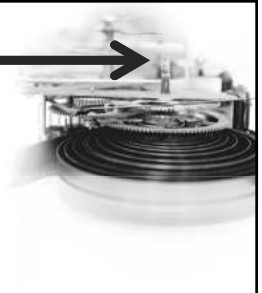
- výsledná šifra:

  DFFGADVADGADVFAGDDAVGFFAXDXVDDGXVVDADA
  FGVDFFFD

- kryptoanalýza - Georges-Jean Painvin

Šifrovací stroje

- šifrovací disk (16. st.)
- šifrovací stroje s otáčivými disky
- **Enigma** – A. Scherbius
- velký význam pro kryptoanalýzu práce v Bletchley Park



Kódy v kryptologii

- substituce, náhrada celých slov, vět, příkazů
- nutná znalost celé kódové knihy

- **kód Navaho**

  bojové letadlo – kolibřík – da-he-tih-hi

  ponorka – železná ryba – besh-lo

  A (ant – mravenec – wol-la-chee)

  B (bear – medvěd – shush)

Dělení šifry podle klíče

- **symetrická šifra** – symetrický klíč

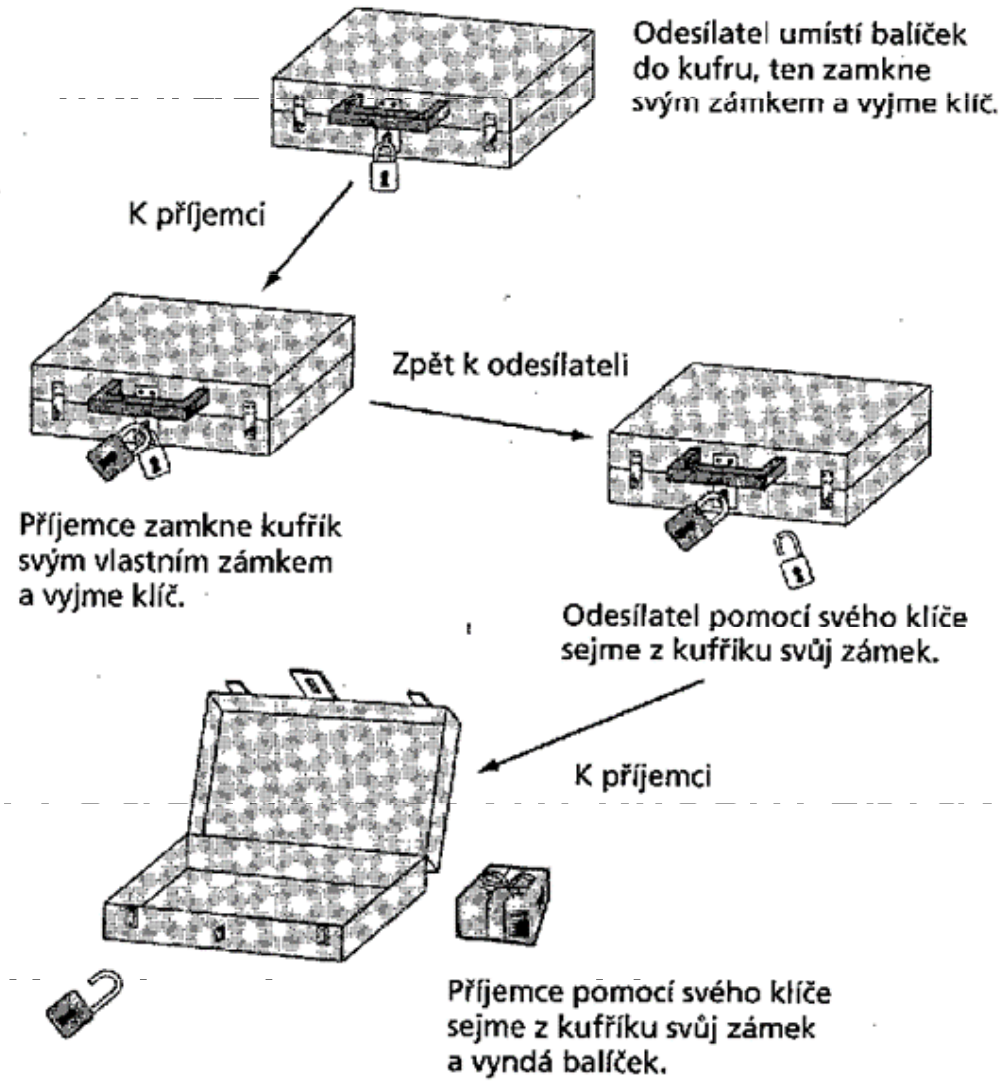
- **asymetrická šifra** – asymetrický klíč

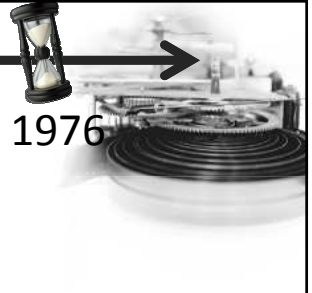
Správa klíčů

Problémy: ní,

Jak se dá

1. Osoba pošle osobě B.
2. Osoba ou svým klíčen
3. Osoba a pošle osobě
4. Osoba a může číst.





Správa klíčů

K čemu by se dal tento postup využít:

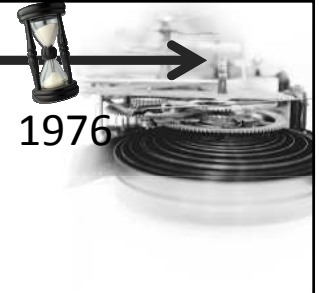
Výměna informací pro distribuci tajného klíče.

Kde je problém:

Skládání šifer není obecně komutativní.

Co se využívá:

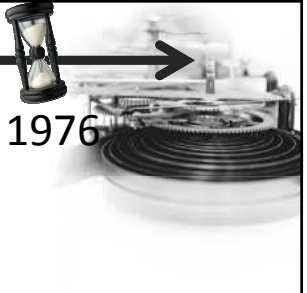
Princip jednosměrných funkcí.



W. Diffie, M. Hellman (1976)

- odstranění základního problému při předávání tajného klíče
- Postup: (O je odesílatel, P je příjemce, m a g mají dané vl.)

1. O i P si veřejně sdělí: $f(x) \equiv g^x \pmod{m}, \quad g < m$
2. O si zvolí tajné číslo *A*, P si zvolí tajné číslo *B*
3. O provede: $\alpha \equiv g^A \pmod{m},$
   P provede: $\beta \equiv g^B \pmod{m},$
4. Po veřejné výměně čísel α, β:
   O provede: $k \equiv \beta^A \pmod{m},$
   P provede: $k \equiv \alpha^B \pmod{m},$
5. Obě hodnoty jsou stejné $k \equiv \beta^A \pmod{m} = \alpha^B \pmod{m}.$

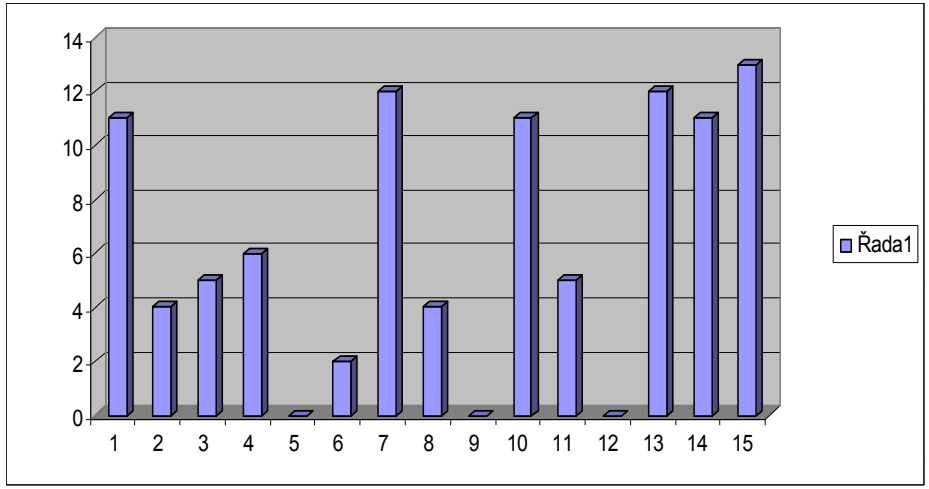


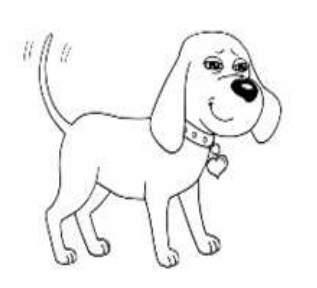
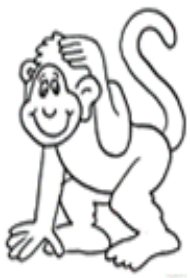
RSA kryptosystém

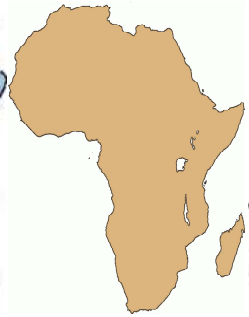
- nejrozšířenější metoda šifrování s veřejným klíčem
- založená na velkých prvočíslech
- bezpečnost založena na složité (nereálné) faktorizaci velkých čísel
- 1977 Rivest, Shamir a Adleman
- spolehlivá proti současným útokům
- použití: elektronický podpis, předávání klíčů u symetrických kryptosystémů

???

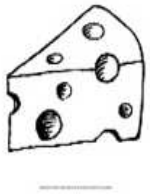
- **Tak se vyzkoušejme – jde nám to?**
- **Aktualni pocasi v Adamove: polojasno, eventualne zatazeno, anomalie misty.**



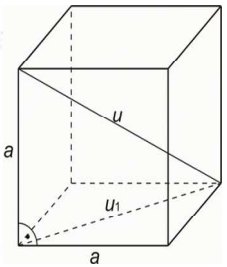



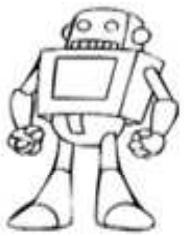


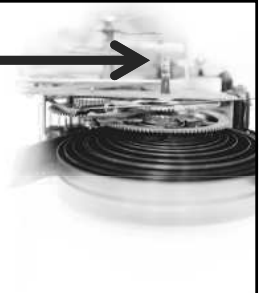






u
a
u_1
a



- Děkuji za pozornost.