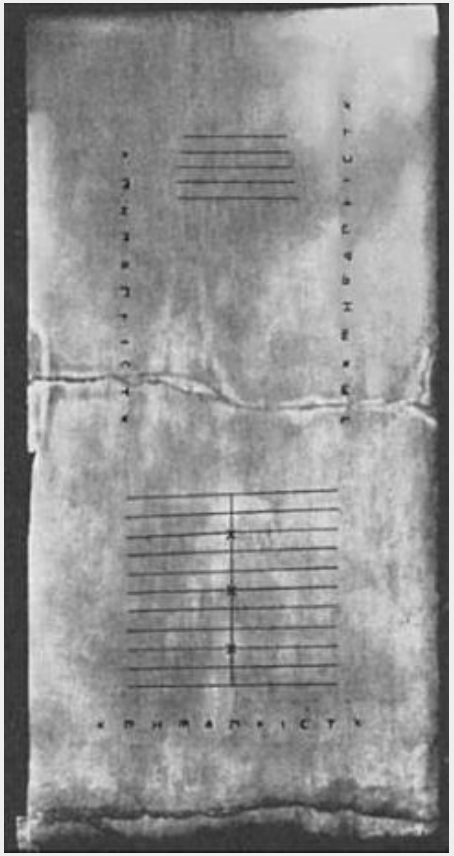
História počítačov

Miroslav Hájek

Počítadlo (Abakus)

Mezopotámia (2700 – 2300 p.n.l.)
Kamienky na kamenných doštičkách – 60 sústava



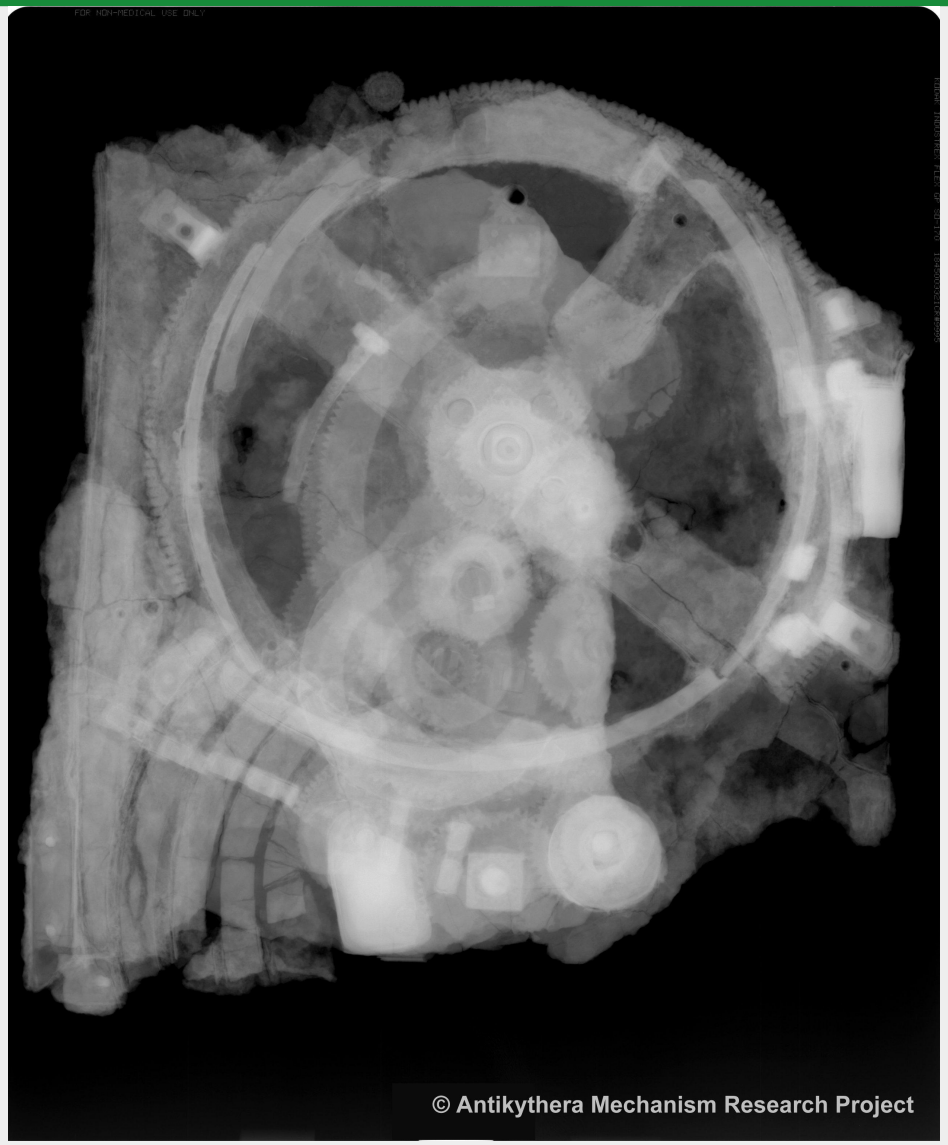
Salamis tablet (300 p.n.l.)
Antické Grécko

Príručný abakus (1. storočie)
Staroveký Rím

Mechanizmus z Antikythery

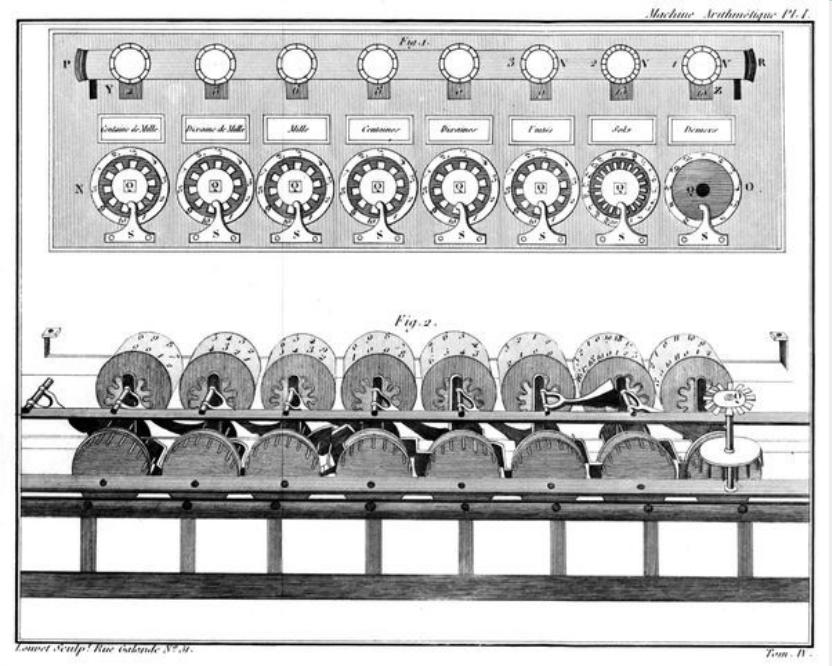
Analógový počítač z 150 – 100 p.n.l.

- Astronomické pozície
- Predpoveď zatmení
- Cyklus olympijskych hier

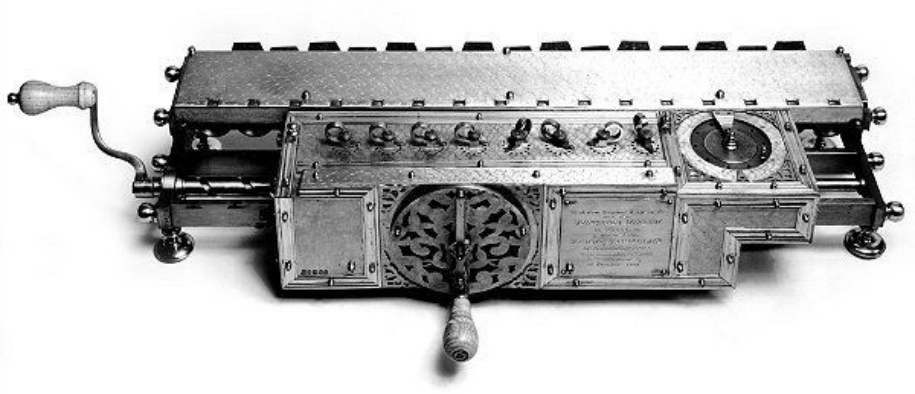


Mechanické kalkulátory

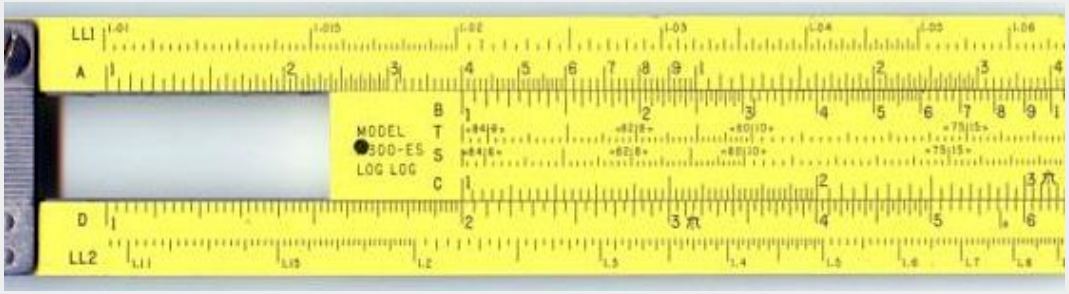
Schickardova kalkulačka (1623)



Paskalína (1645)

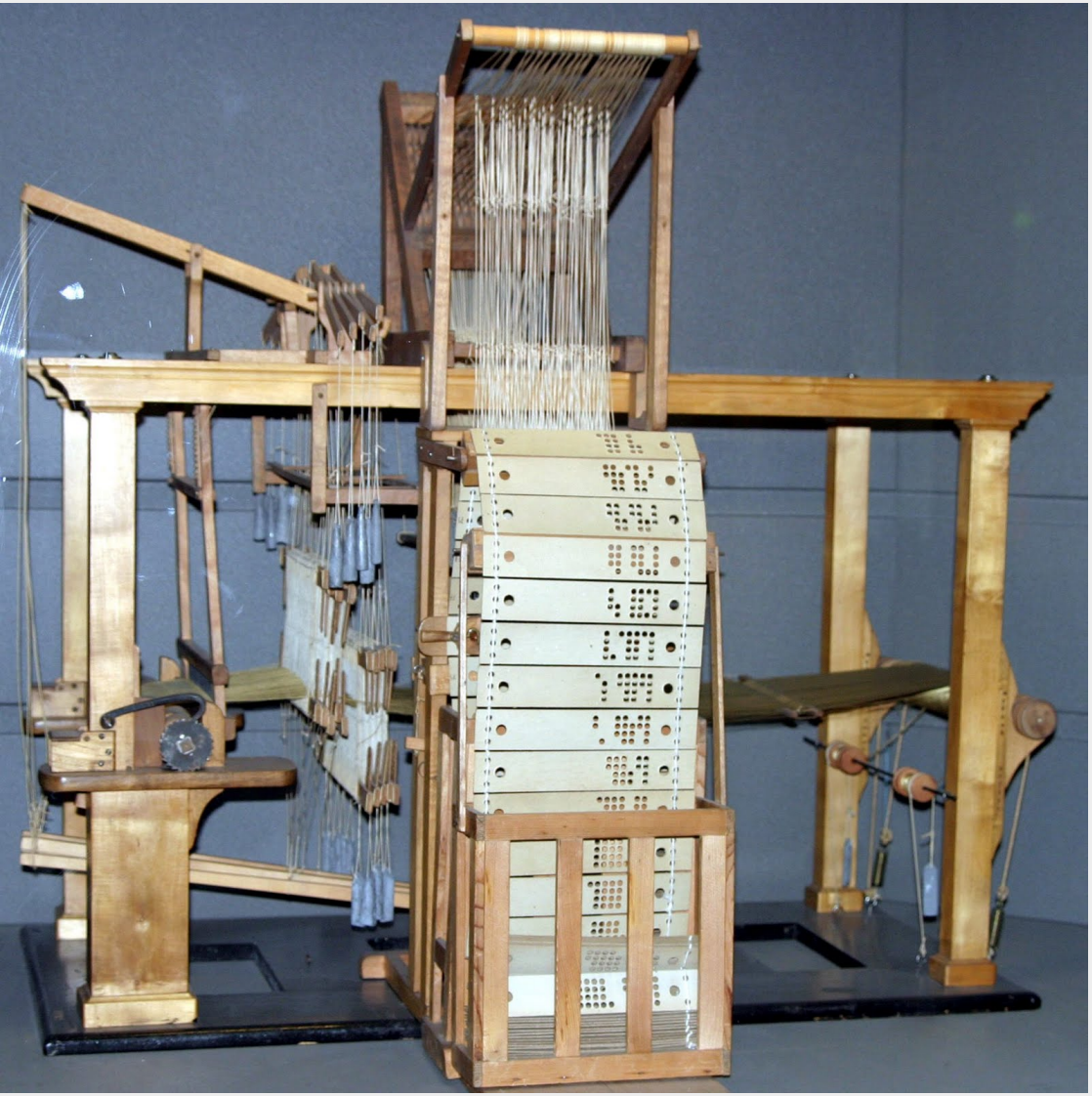


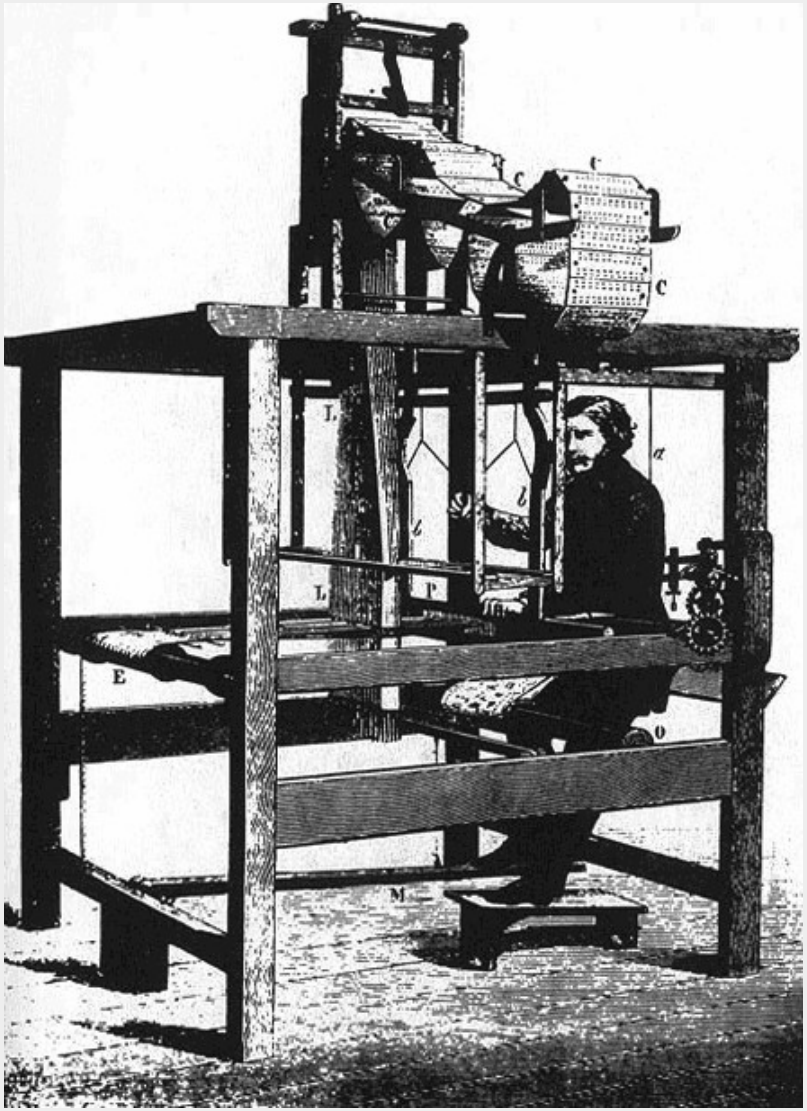
Leibnizova stupňovitá kalkulačka (1694)



Logaritmické pravítko - 1620
(William Oughtred)

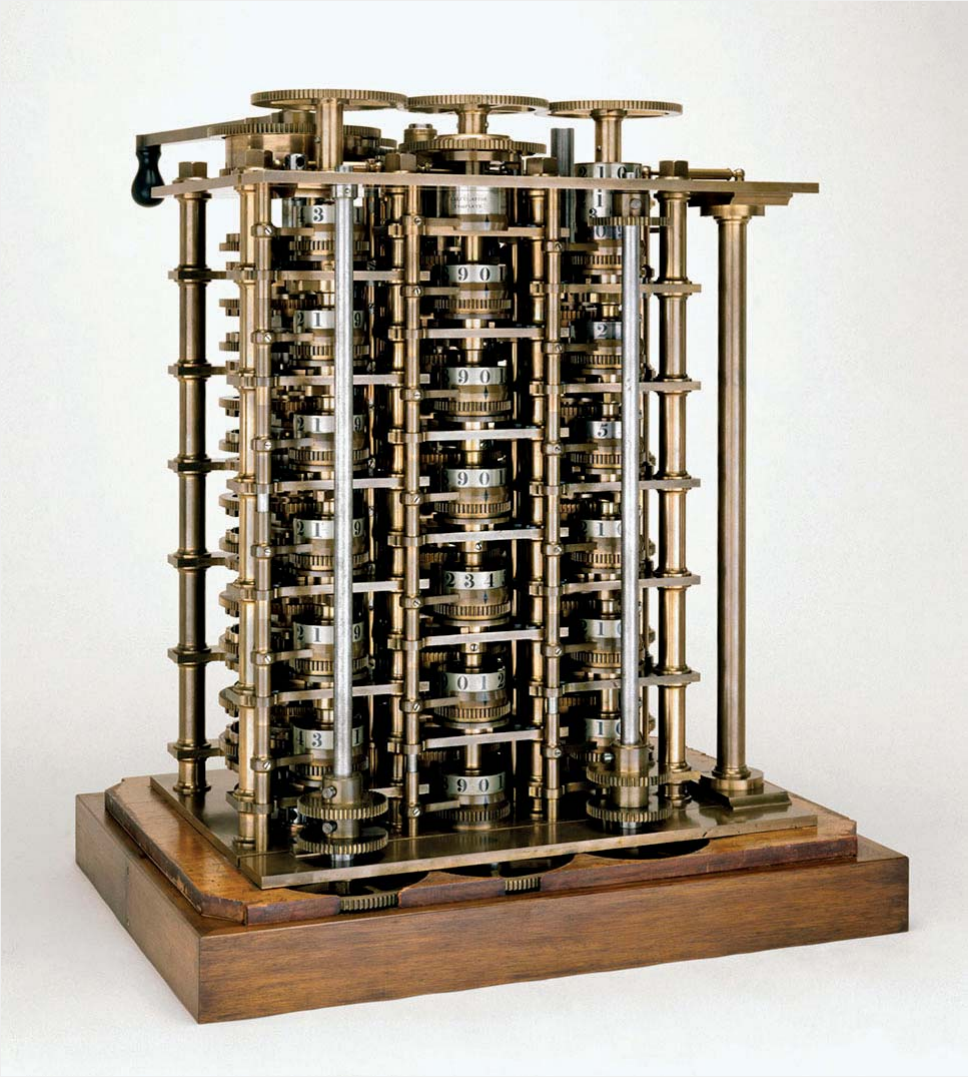
Jacquardove tkáčske krosná





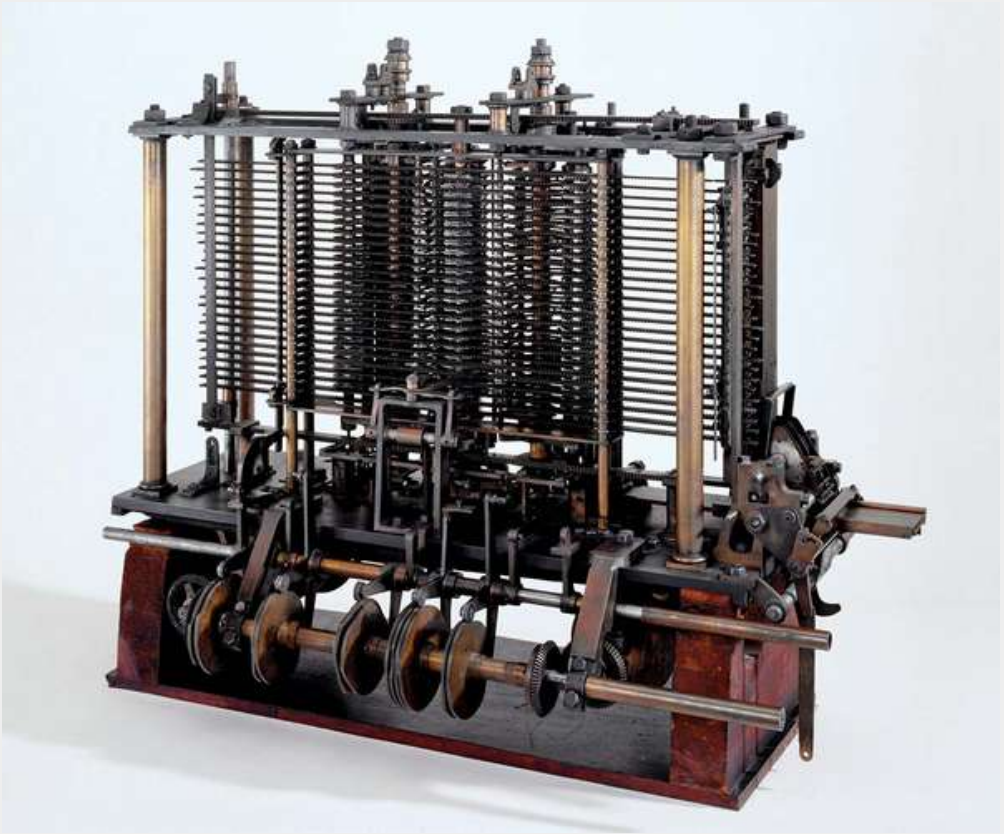
Vzorované tkanivá podľa vzoru - 1801

Babbageove počítacie stroje



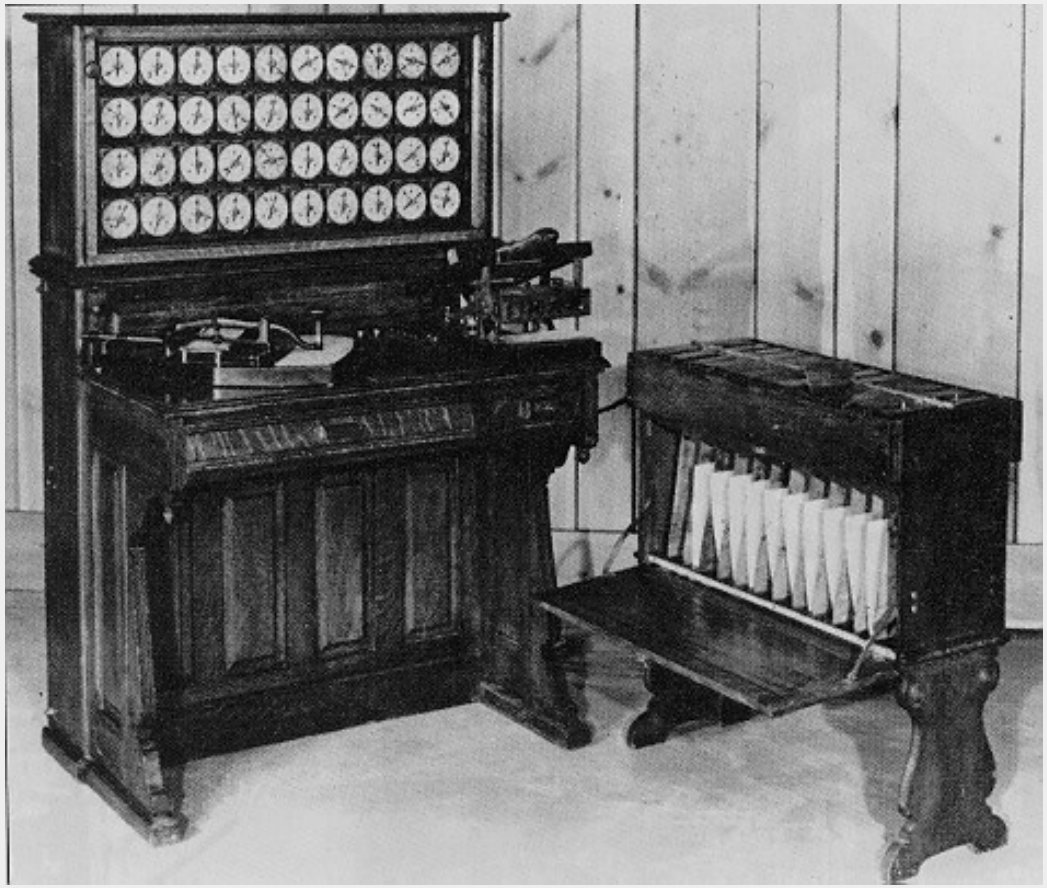
Diferenčný stroj (1820 - 33)

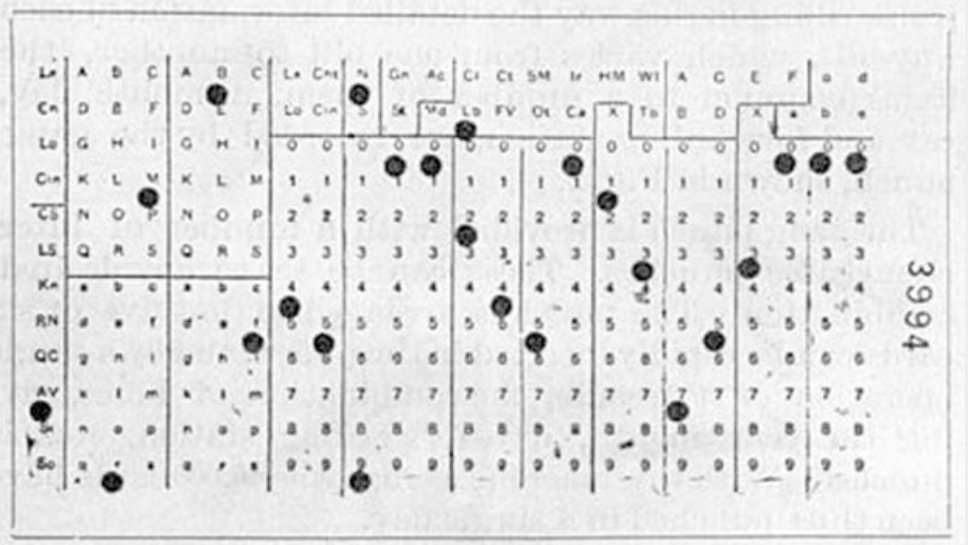
„The Analytical Engine weaves algebraic patterns, just as the Jacquard-loom weaves flowers and leaves“ - *Ada Lovelace*

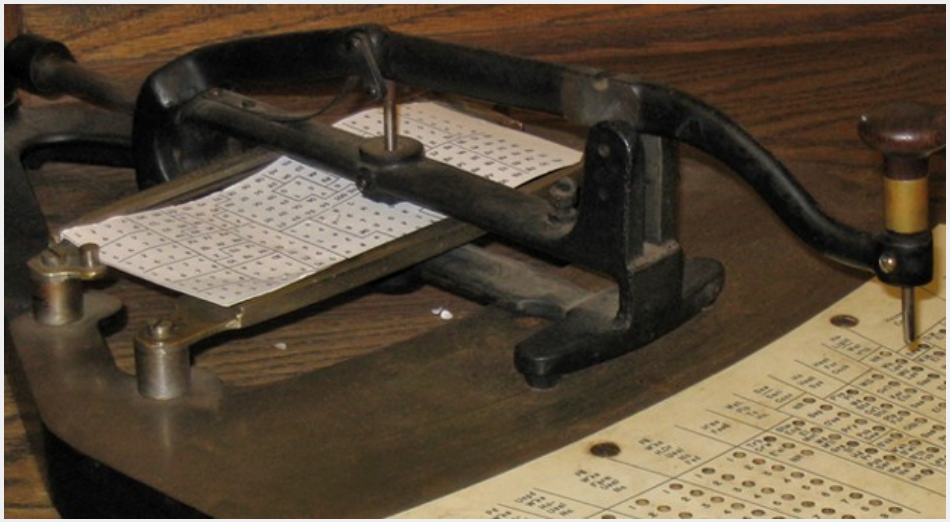


Časť nekončeného Analytického stroja (1910)

Holerithov tabelátor



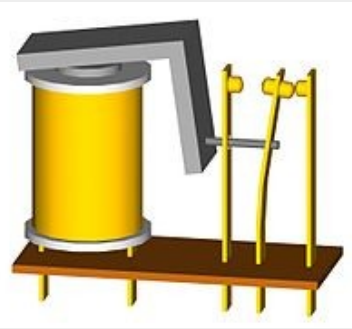




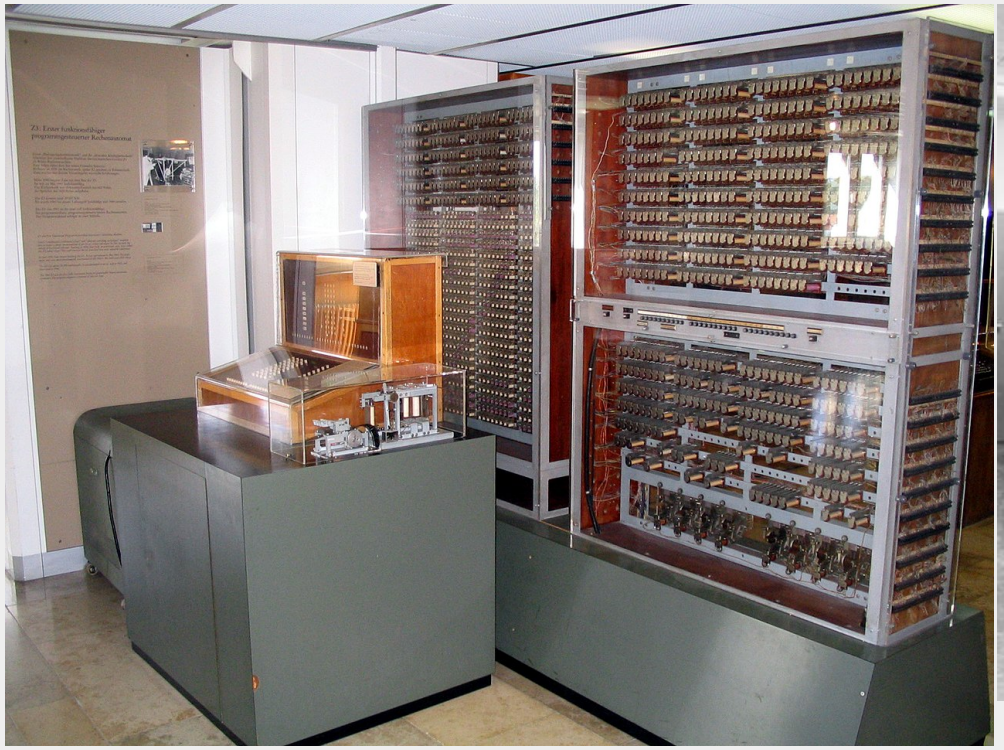
Sčítanie ľudu 1890 v USA

http://www.columbia.edu/cu/computinghistory/1890tabulator.html
https://www.ibm.com/ibm/history/ibm100/us/en/icons/tabulator/

Relé – 0. generácia (1930 - 1945)



Elektromechanické halové počítače



Konrad Zuse – Počítače Z1 – Z4

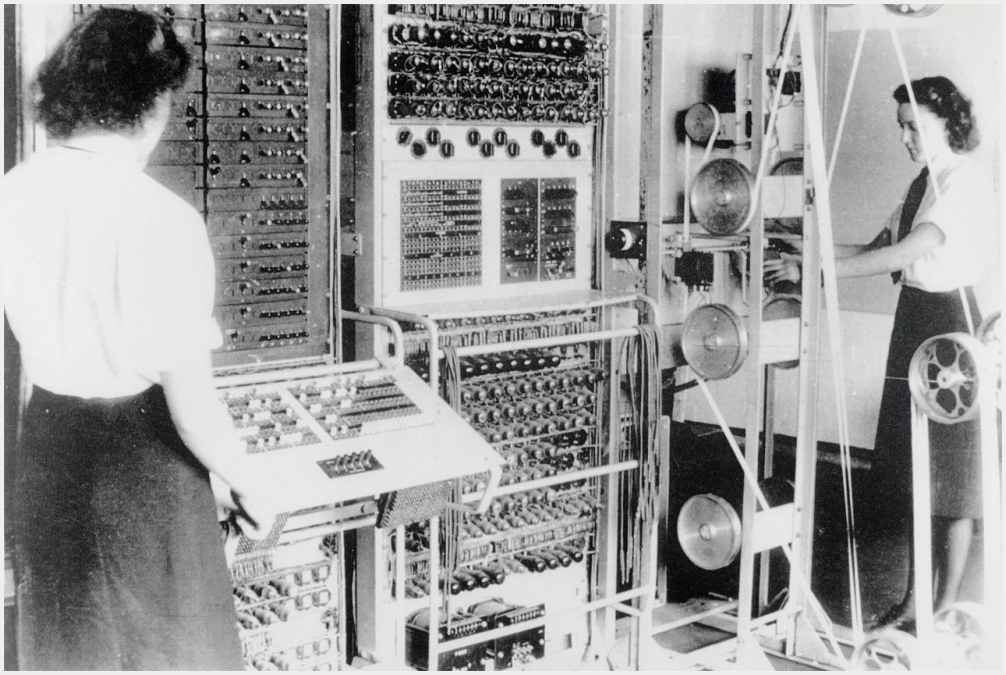
Z3: *cez 2000 relé, 5 Hz, 64 x 22 miestami, 4 kW*
Sčítanie: 0.8s, Násobenie: 3s

Harvard Mark I (1937)
IBM Automatic Sequence Controlled Calculator
Howard Aiken, Grace Hopper

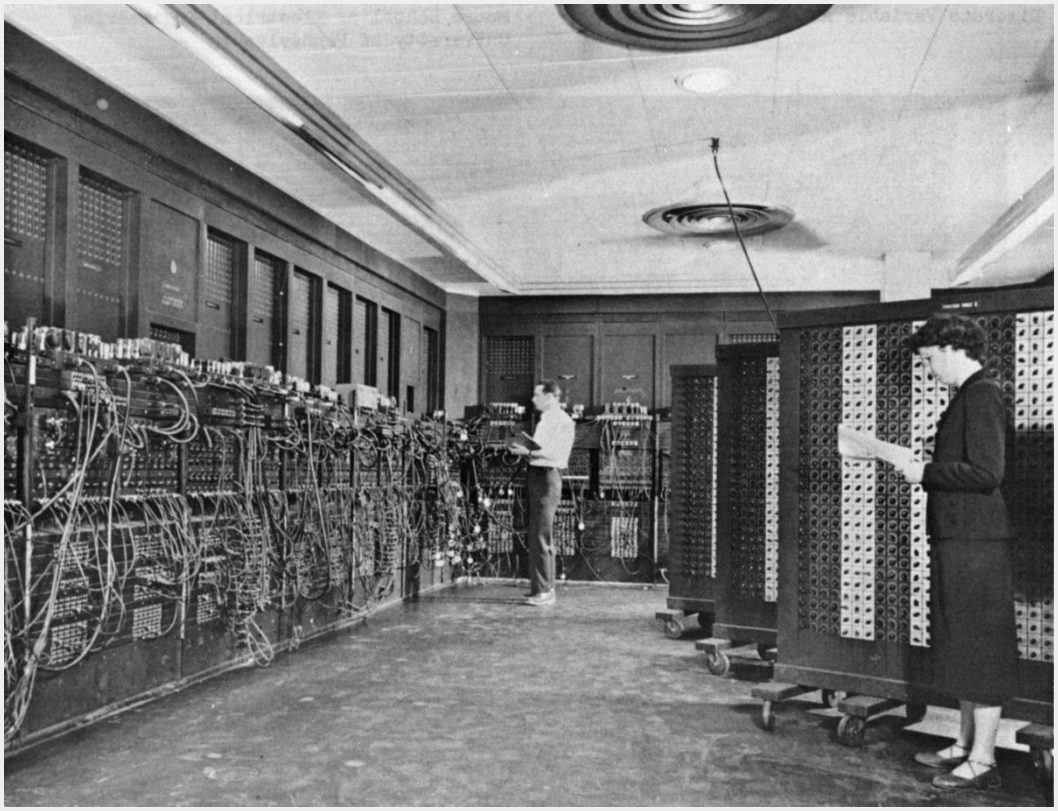
Pamäť pre 72 čísel s 23 desiatkovými ciframi
3 sčítania/s, Násobenie: 6s, Delenie: 15s, 4t

Mainframe – 1. generácia (1945 - 1955)

Elektronické sálové počítače pre špeciálne použitie



COLOSSUS – 1943 (Bletchley park)
Max Newman, Tommy Flowers
Dešifrovanie nemeckej rádiovej komunikácie
1500 elektróniek, 6kW

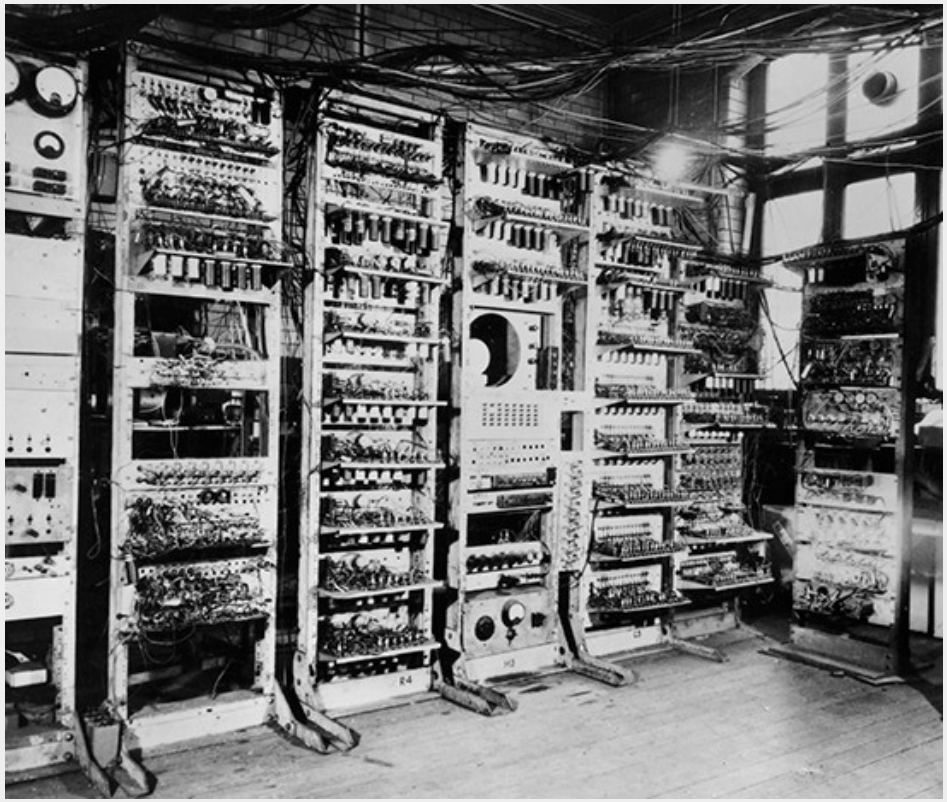


ENIAC – 1945
Electronic Numerical Integrator And Computer

- Výpočty palebných tabuliek pre delostrelectvo
- Desiatková sústava s 10 miestnymi číslami
- 17-tisíc elektróniek, 150kW, 300 op/s

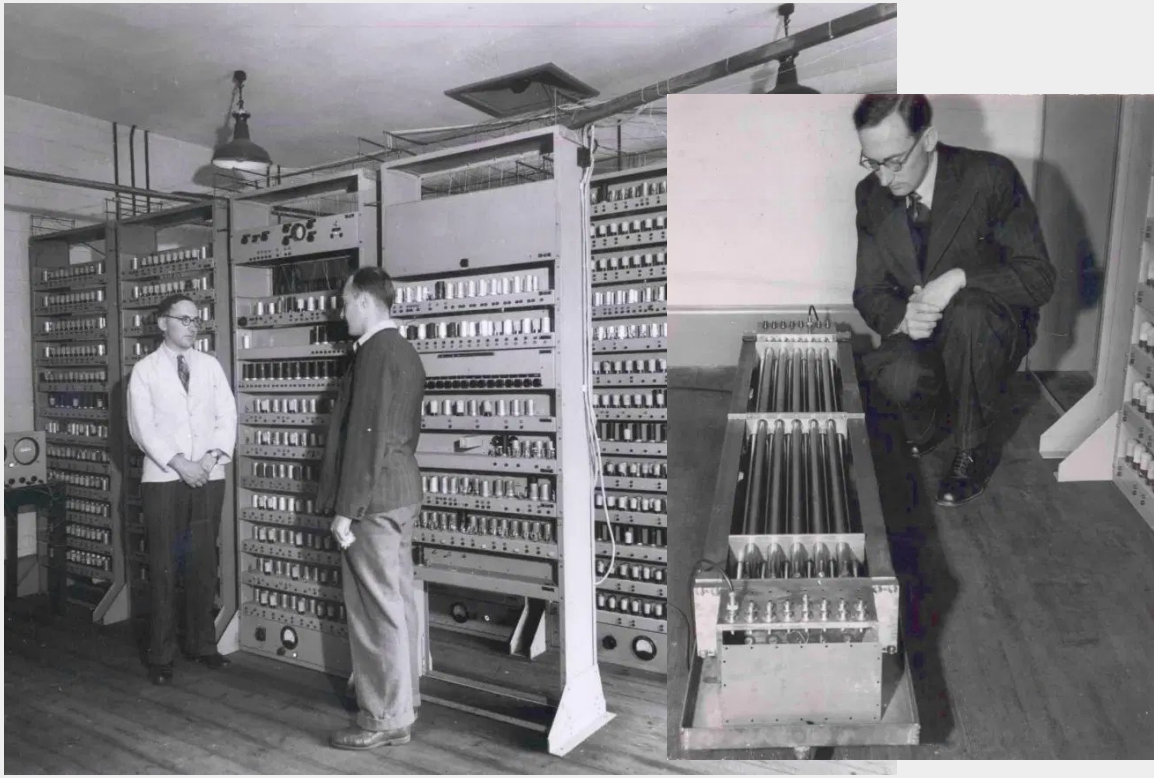
Mainframe – 1. generácia (1945 - 1955)

Elektronické programovateľné počítače



Manchester Mark 1

- August 1949
- Hľadanie Mersennových prvočísel: $2^n - 1$

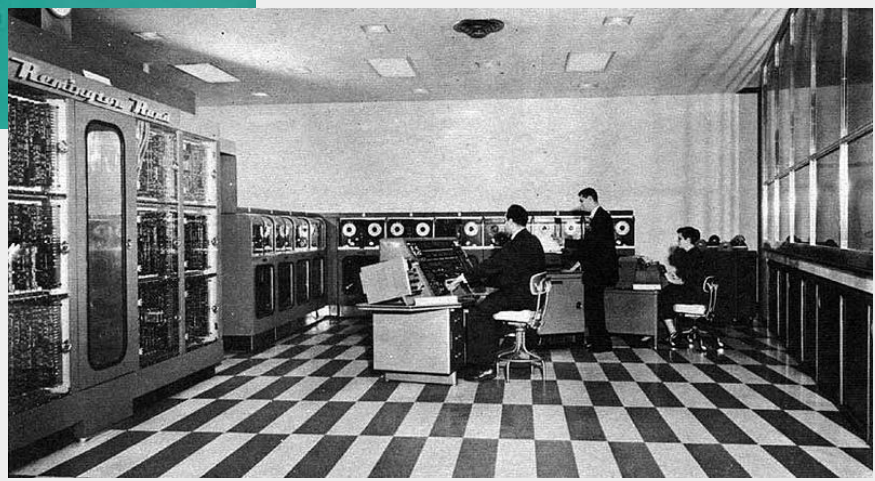


EDSAC (Electronic delay storage automatic calculator)

- Cambridge, UK
- Prvý program bežal 6.5.1949
- Pamäť z ortuťovej oneskorovacej linky

Mainframe – 1. generácia (1945 - 1955)

UNIVAC (UNIVersal Automatic Computer) – Prvý komerčne vyrábaný počítač (1951)

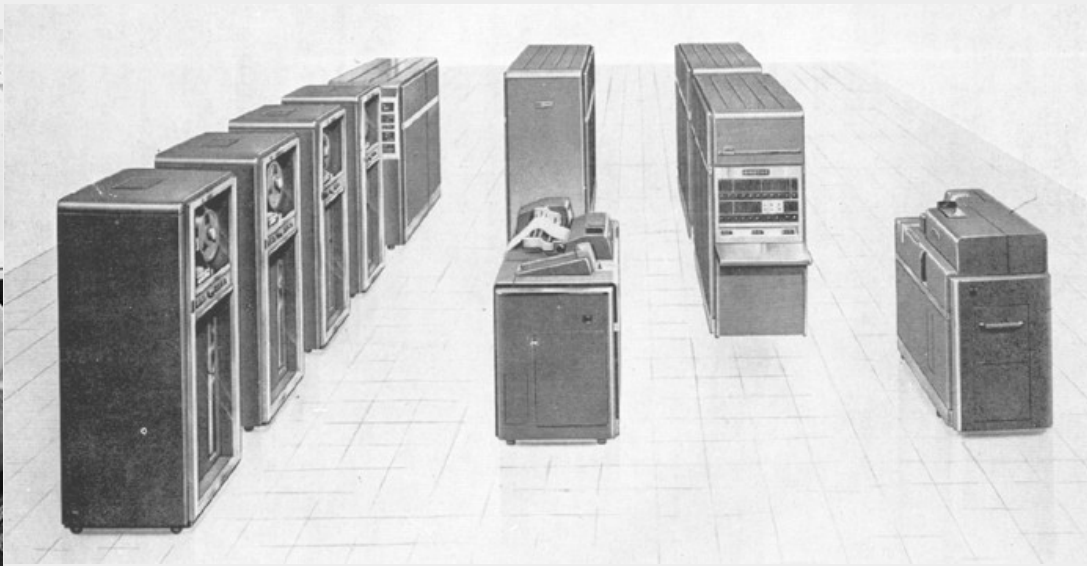


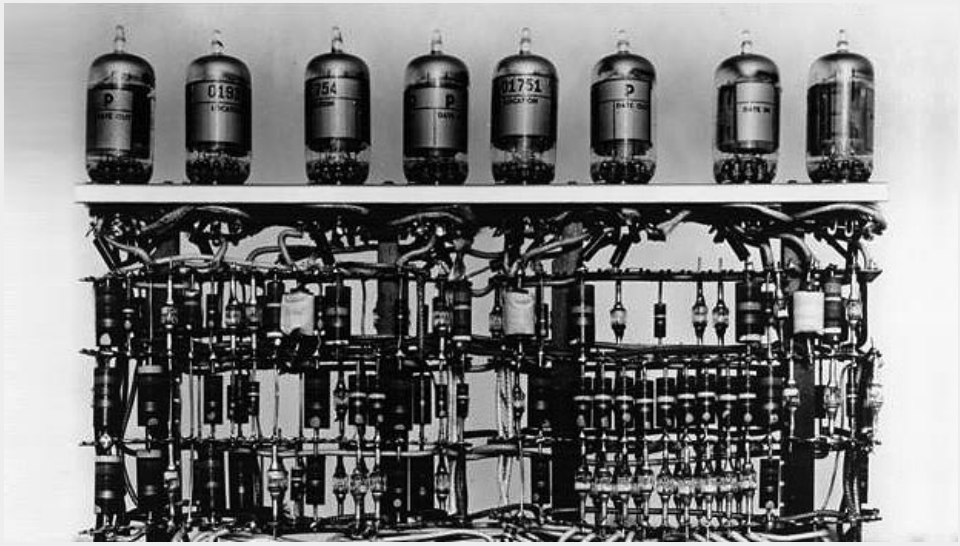
5000 elektróniek, 7,6 t, 125 kW, 1900 op/s
Súčet: 525 us, Násobenie: 2100 us (2,1ms)

Pamäť: 1000 x 12 bit (Oneskorovacia linka s ortuťou)
Prvý zákazník: United States Census Bureau

Mainframe – 1. generácia (1945 - 1955)

IBM 700 séria (1952)



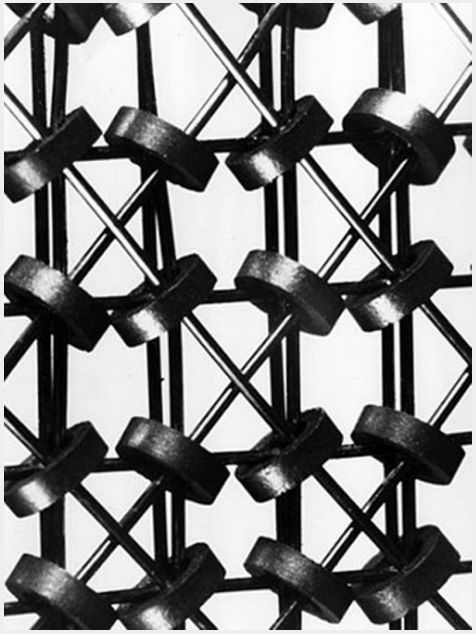


Zľava doprava:
4 x IBM 727 pre magnetické pásky
IBM 652 ovládacia jednotka
IBM 407 účtovnícky stroj (vpredu)
IBM 653 vysoko-rýchlostné úložisko
IBM 650 konzola (vpredu)
IBM 655 napájacia jednotka
IBM 555 pre dierne štítky

https://www.computerhistory.org/timeline/memory-storage/

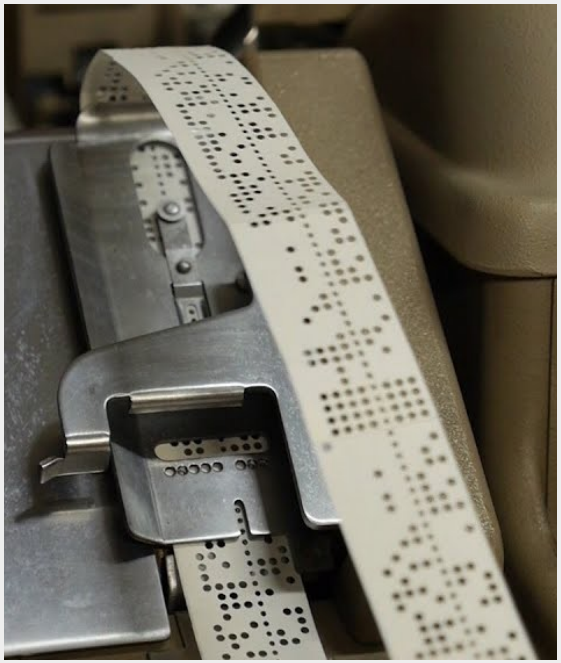
Pamätové média – 1. generácia

Williams–Kilburn
CRT pamäť - 1947

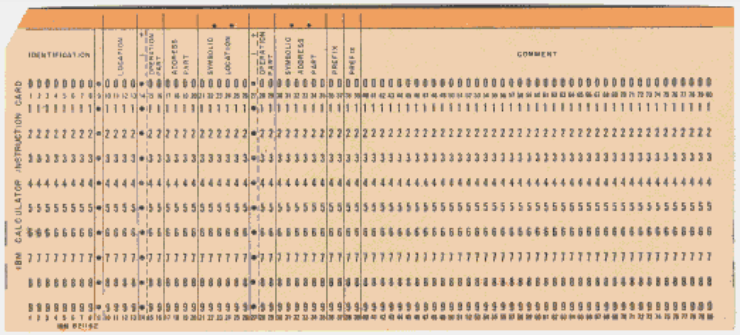


Feritová pamäť
(Core memory) - 1949

RAMAC – 1956
Magnetický pevný disk (5MB)



Dierna páska



Dierny štítok

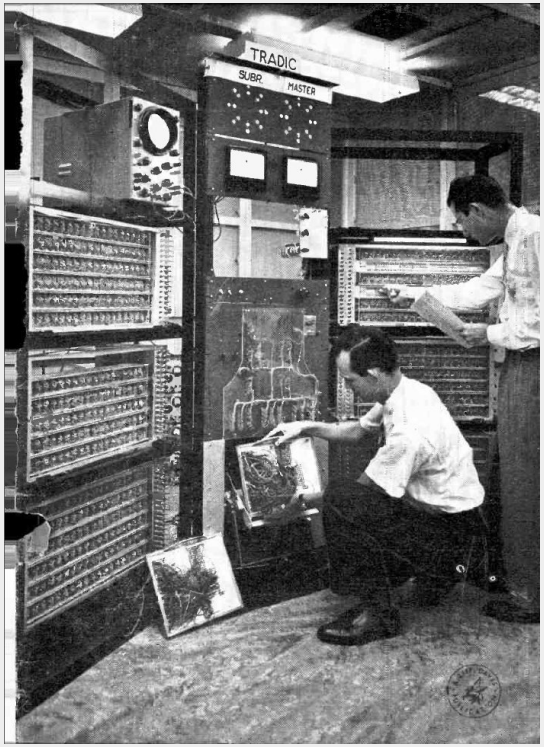
Lp.	Nr ścieżki 1	2	3	4	5	Litery	Cyfry i znaki
1	●	●	•			A	–
2	●		•		●	B	?
3		●	•	●		C	:
4	●		•		●	D	kto tam
5	●		•			E	3
6	●		•	●	●	F	wolny
7		●	•		●	G	wolny
8			•	●		H	wolny
9		●	•	●		I	8
10	●	●	•		●	J	dzwonek
11	●	●	•	●		K	(
12		●	•			L	)
13			•	●	●	M	.
14			•	●		N	,
15			•		●	O	9
16		●	•	●		P	0

Lp.	Nr ścieżki 1	2	3	4	5	Litery	Cyfry i znaki
17	●	●	•	●		Q	1
18		●	•		●	R	4
19	●		•	●		S	'
20			•		●	T	5
21	●	●	•	●		U	7
22		●	•	●	●	V	=
23	●	●	•			W	2
24	●		•	●	●	X	/
25	●		•	●		Y	6
26	●		•			Z	+
27			•		●	powrot karetki	
28		●	•			obrot wałka	
29	●	●	•	●	●	litery	
30	●	●	•		●	cyfry i znaki	
31			•	●		odstęp	
32			•				

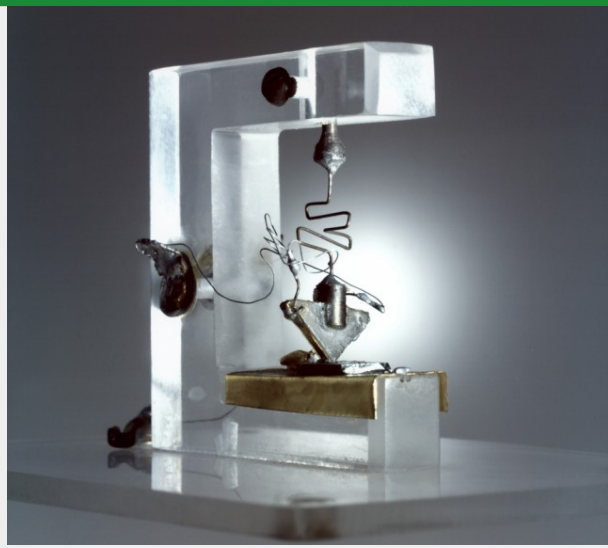
Skriňové počítače – 2. generácia (1955 - 1965)

Tranzistory a feritová pamäť

DEC PDP-1 (1959)
- 2700 tranzistorov
- 4096 x 18 bit
- $120 000
- 53 ks



TRADIC (1954)
- 700 transistorov
- 10 000 germániových diód



Prvý tranzistor - 1947
Bellové laboratória

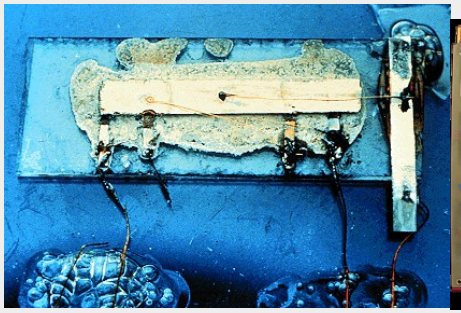
Minipočítače – 3. generácia (1965 - 1980)

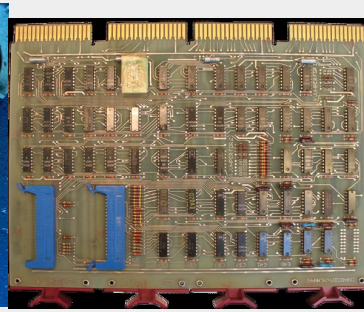
DEC PDP-7 (1965)

- 18-bitová zbernica
- RAM: 4 kB slov (do 64 kB)
- $72 000

Honeywell Level 6 (1975)

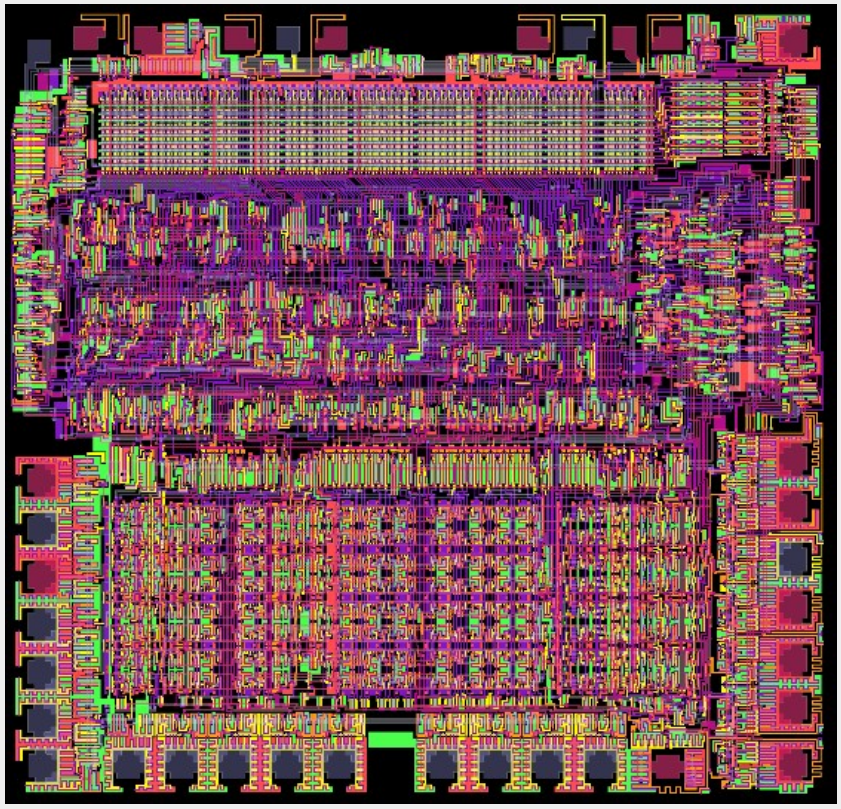
- 16-bitová zbernica
- RAM: 64kB slov MOS



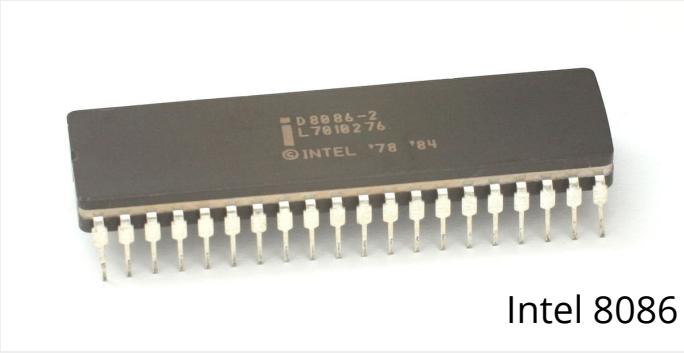


Integrovaný obvod

Mikropočítače – 4. generácia (1980 - dnes)



MOS Technology 6502



Intel 8086

3. generácia:

- SSI – Single scale integration (100 prvkov)
- MSI – Middle scale integration (1000 prvkov)
- LSI – Large scale integration (10 000 prvkov)

4. generácia:

- VLSI – Vysoká úroveň integrácie
  100 000 prvkov / cm^2 - Intel 8086
- ULSI – Ultra vysoká úroveň integrácie
  64-bitové viac-jadrové procesory

IBM PC (1981)

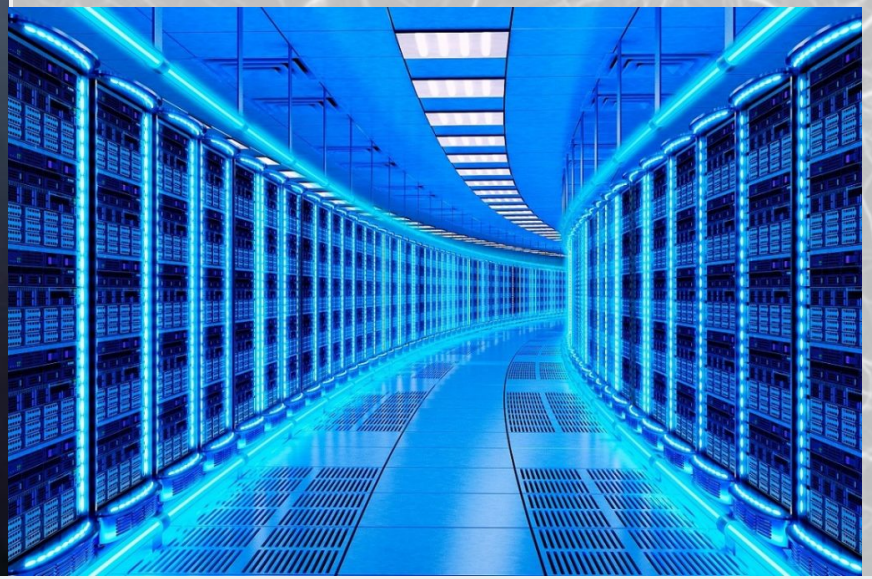
- *CPU: Intel 8088 (8/16-bit) @ 4.77 MHz*
- *RAM: 16 kB – 640 kB*
- *$1 565*

Mikropočítače – 4. generácia (1980 - dnes)

IBM PC, Apple Macintosh, Altair 8800, ZX Spectrum, Commodore 64, PMD-85

Budúcnosť – 5. generácia

- Kvantové počítače
- Umelá inteligencia
- Distribuované masívne paralelné počítanie



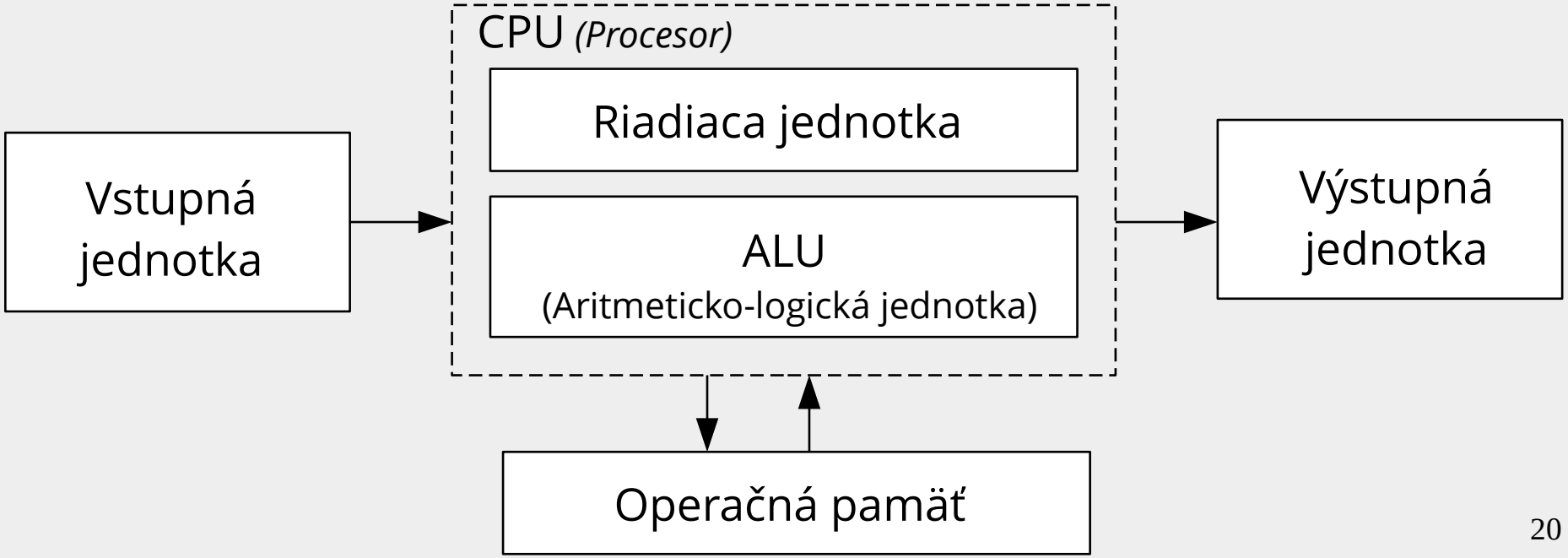
Komponenty počítačov

Miroslav Hájek
Gymnázium, Hubeného 23

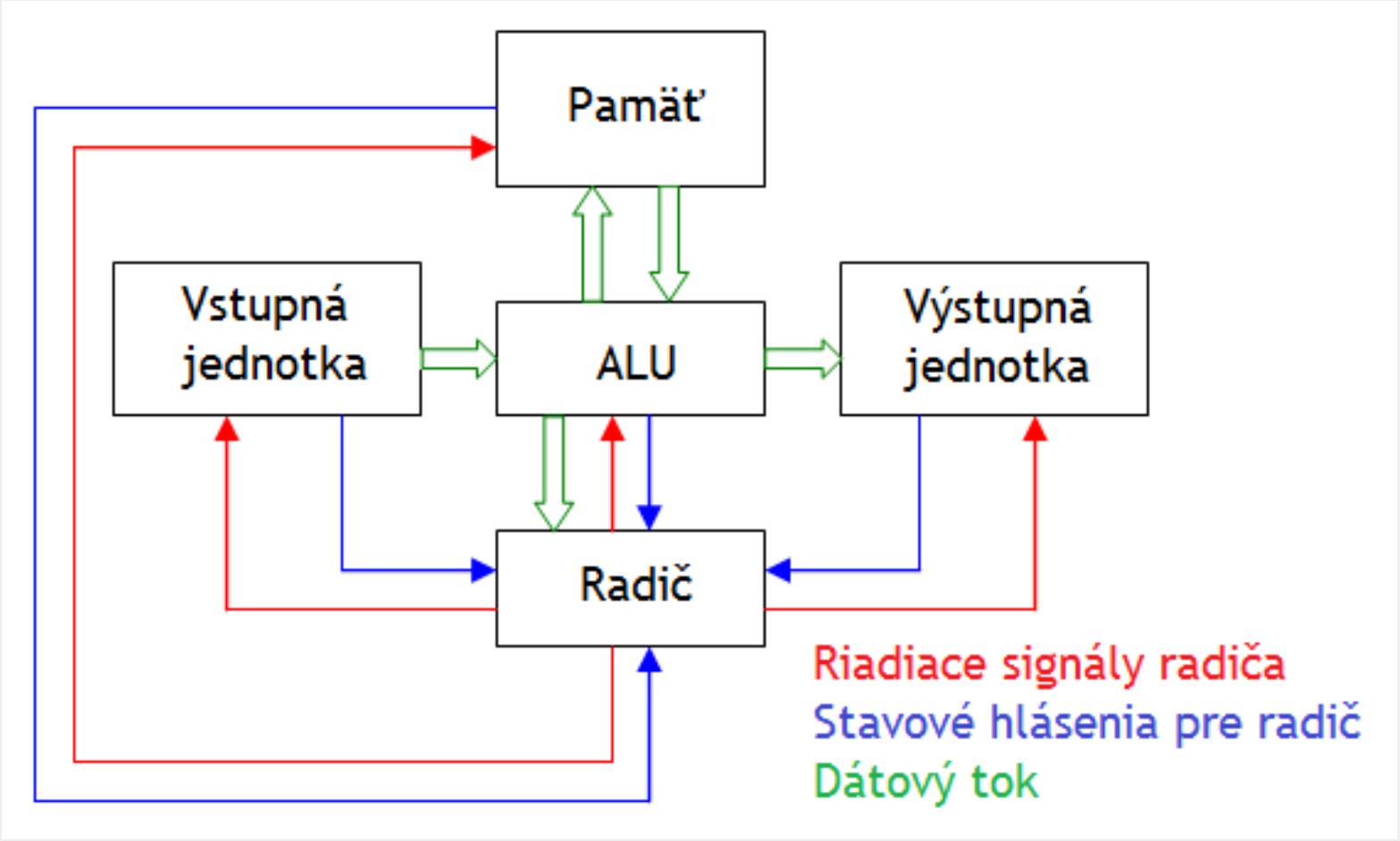
Bloková schéma počítača

Koncepcia počítača - Von Neumannova schéma

First Draft of a Report on EDVAC (1945)



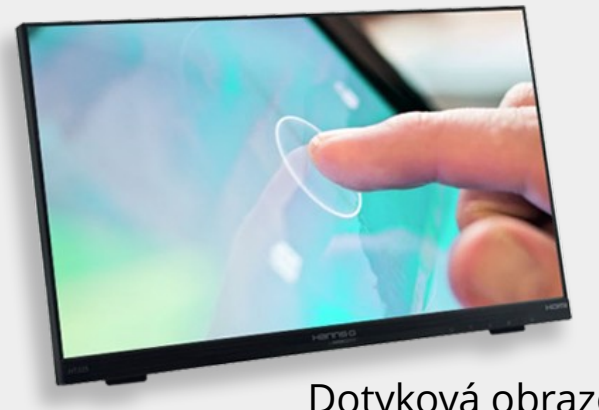
Bloková schéma počítača



Vstupné zariadenia (**H**uman **I**nterface **D**evice)

Klávesnica

Myš



Dotyková obrazovka

Joystick

Gamepad

Touchpad

Volant

Trackball

Čítačka otlačkov prstov

Ovládač gestami

Diaľkový ovládač

Vstupné zariadenia (Multimédia)

Grafický tablet (HID)

Webkamera

Skener

Mikrofón

Výstupné zariadenia

CRT monitor

LCD/OLED monitor

Tlačiareň
(ihličkové, atramentové, laserové 3D)

Dataprojektor

Sluchadlá

Reproduktory

Základná doska

V/V Rozhrania

USB, Keyboard and Mouse


USB Type A (male)


USB Type A (female)


USB Type B (male)


USB Type B (female)


USB Mini-A (male)


USB Micro-A (male)


USB Type C (male)


USB Type C (female)


USB 3.0 Type A (male)


USB 3.0 Type A (female)


USB 3.0 Type B (male)


USB 3.0 Micro B (male)


PS/2 (male)


PS/2 (female)

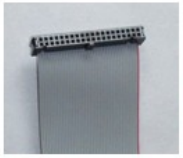

AT Keyboard (male)


AT Keyboard (female)

Storage / Disk


SATA Type A


e-SATA


IDE 40-pin Connector


IDE 40-pin Port


Thunderbolt


Firewire 400 1394a 6-pin


Firewire 400 1394a 4-pin


Firewire 800/3200 1394b/c

Power


IEC 320 C13/C14 Connector


IEC 320 C13 Socket (f)


IEC 320 C14 Plug (m)


IEC 320 C19 (f)


IEC 320 C20 (m)


IEC 320 C5 Connector


SATA Power Connector

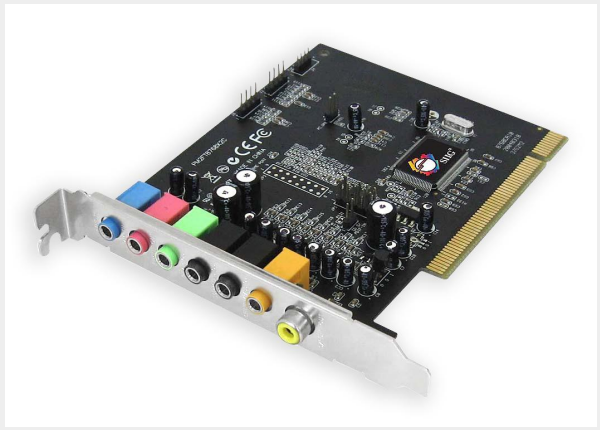

Molex 4-pin Connector

V/V Rozhrania

Rozširujúce karty pre PCI

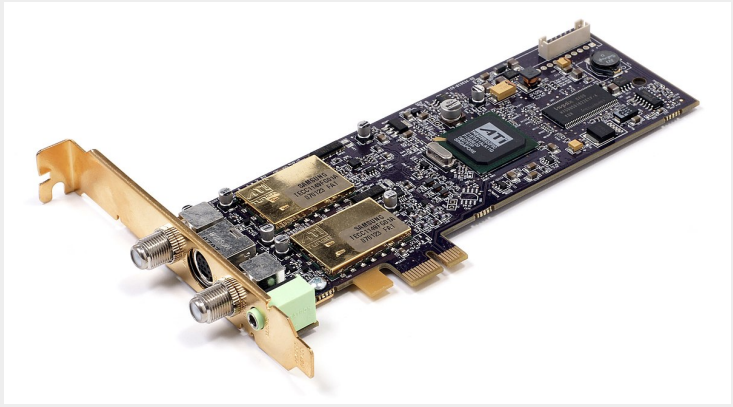
Grafická karta

Zvuková karta

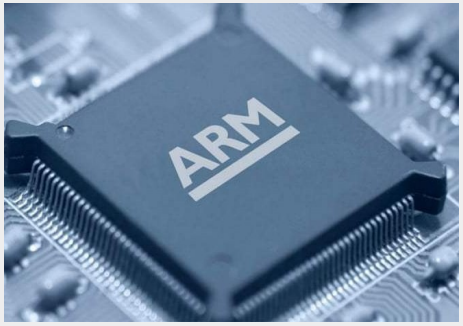


Sieťová karta (NIC)

Karta TV tunera

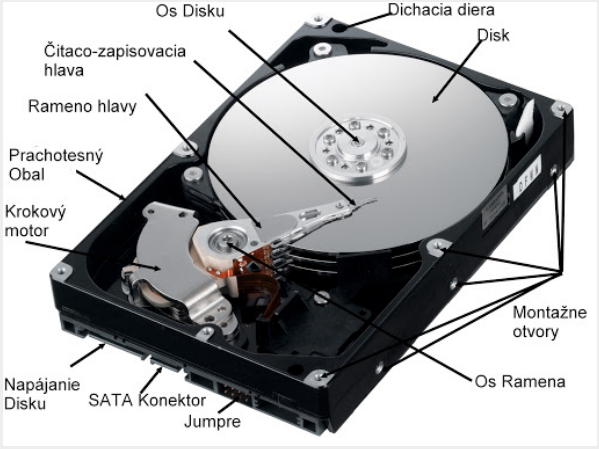


Procesor



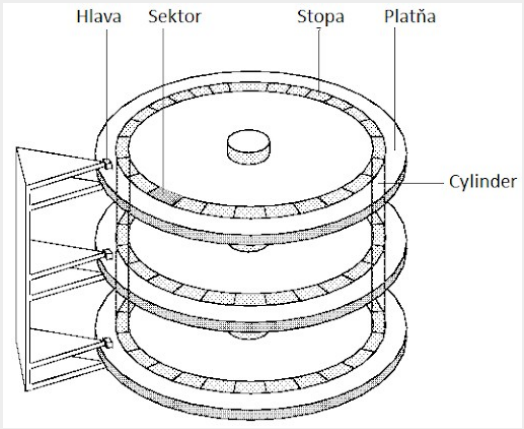
Výrobca a typ:
Intel, AMD, Qualcomm, Apple, ...
Pätica: LGA1155
Architektúra:
x86, x86-64, ARM, AVR, ...
Inštrukčná sada:
CISC, RISC
Počet jadier:
2, 4, 8
Šírka zbernica:
32-bit/64-bit
Taktovacia frekvencia:
1,6 – 4 GHz
Kapacita vyrovnávacej pamäte (Cache):
L1, L2, L3 (v kB)
Ďalšie: podporovaná RAM, Litografia (22 nm)

Pamäte



Magnetické média

- Pevný disk (HDD) - 1TB
- Disketa – 1,44 MB
- Magnetická páska



Optické disky

- CD – 700 MB (780 nm)
- DVD – 4,7 GB (650 nm)
- Blue-ray – 25 GB (405 nm)

Flash pamäte

- SSD (Solid-state drive)
- USB kľúče
- Pamäťové karty (SecureDigital, CompactFlash)

1. Vnútorné

2. Vonkajšie

I. RAM (Volatilná pamäť)

- **I. RWM (SRAM, DRAM)**
- **II. ROM (PROM, EEPROM)**

II. NVRAM

Digitalizácia informácie

Miroslav Hájek
Gymnázium, Hubeného 23

Teória informácie

Informatika je vedný odbor zaoberajúci sa získavaním, spracovaním, prenosom a uchovávaním údajov, dát a informácií.

Údaj (digitálne: dáta)
- Každá správa bez ohľadu na nový informačný obsah
- Písmená, čísla, slová, znaky, obrázky, zvuky a ich kombinácie

Informácia
- Správa prinášajúca nové poznatky a odstraňujúca nevedomosť
- ***Entropia (H)*** *- priemerný počet bitov potrebných na zakódovanie informácie (Shannon, 1949)*

Digitalizácia
- Proces prevodu analógových údajov na digitálne (číslicový tvar)
- Údajom sa priradí jedinečná kombinácia bitov

Kódovanie
- Proces jednoznačného priradenia každého znaku alebo postupnosti znakov daného súboru do iného súboru znakov
- Cieľom nie je utajovanie

Bit [b] - **bi**nary digi**t**
- jednotka informácie
- [0, 1], [Pravda, Nepravda]

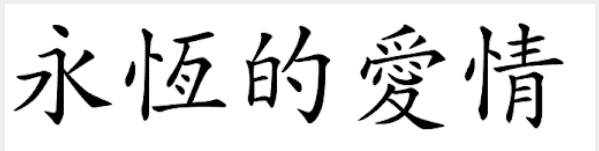
Bajt [B] – slabika
- zoskupenie **8 bitov**

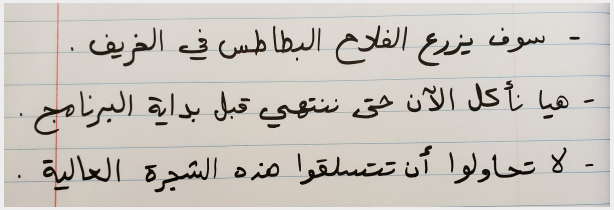
Kódy

Definície z KSSJ:

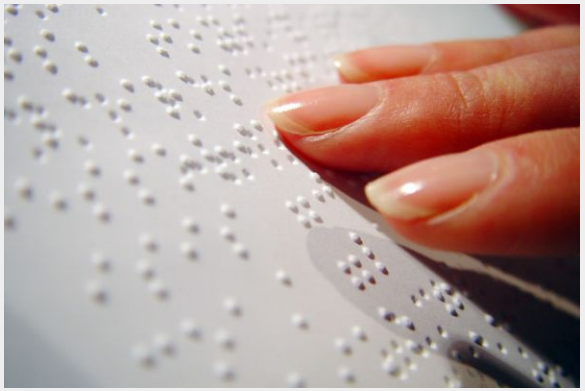
- „Systém znakov na prenášanie informácie: číselný kód“
- „Dohodnutý systém pravidiel na priradenie významu k znakom alebo signálom“

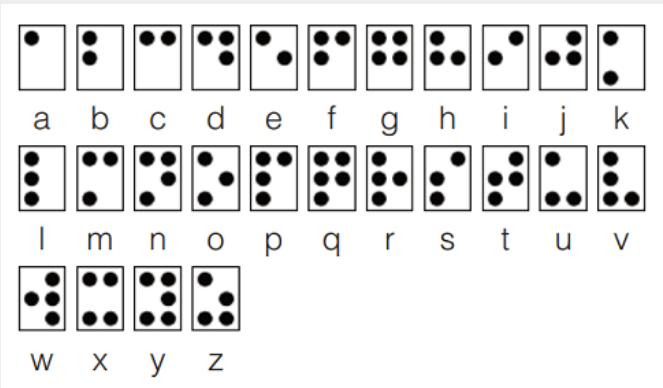
Abecedy





Braillovo písmo pre nevidiacich





Morseova abeceda (zvuk)

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

Piktogramy

Číselné sústavy

Desiatková (Decimálna) pozičná číselná sústava (0 - 9)

2985 = **1000** x 2 + **100** x 9 + **10** x 8 + **1** x 5

90 = **10** x 9 + **1** x 0

Rád	10^3	10^2	10^1	10^0
	1000	100	10	1
Číslo	2	9	8	5

Dvojková (Binárna) sústava (0, 1)

11001 = **16** x 1 + **8** x 1 + **4** x 0 + **2** x 0 + **1** x 1

Rád	2^4	2^3	2^2	2^1	2^0
	16	8	4	2	1
Číslo	1	1	0	0	1

Šestnásková (Hexadecimálna) sústava (0 – 9, A - F)

5C = **16** x 5 + **1** x 13

103 = **256** x 1 + **16** x 0 + **1** x 3

Rád	16^2	16^1	16^0
	4	2	1
Číslo	A	5	C

Prevody medzi sústavami

- **Z 10-sústavy na 2-sústavu**

```
12 : 2 = 6    zv. 0
6  : 2 = 3    zv. 0
3  : 2 = 1    zv. 1
1  : 2 = 0    zv. 1
```

$12_{10} = 1100_2$

Min. počet bitov pre číslo 12

$$\lceil \log_2 12 \rceil = \lceil 3.584962501 \rceil = 4\text{b}$$

- **Z 2-sústavy na 10-sústavu**

```
     2^3  2^2  2^1  2^0
x    1    1    0    0
-------------------------
     8  +  4  +  0  +  0  =  12
```

```
1182 : 2 = 591    zv. 0
591  : 2 = 295    zv. 1
295  : 2 = 147    zv. 1
147  : 2 = 73     zv. 1
73   : 2 = 36     zv. 1
36   : 2 = 18     zv. 0
18   : 2 = 9      zv. 0
9    : 2 = 4      zv. 1
4    : 2 = 2      zv. 0
2    : 2 = 1      zv. 0
1    : 2 = 0      zv. 1
```

$1182_{10} = 10010011110_2$

Princíp – prevod do dvojkovej sústavy

1. Vezmeme si desiatkové číslo (v binárnom tvare)
2. Pozrieme sa ako pomocou zvyšku po delení získavame bity
   - Delenie dvoma – **posun bitov** doprava o jedno miesto
   - Zvyšok po delení dvoma – **maska** na posledný bit

$$22_{10} = 10110_{2}$$

```
    10110
>>   1011
>>    101
>>     10
>>      1
>>
```

Prevody medzi sústavami

- **Z 10-sústavy na 16-sústavu**

```
84 : 16 = 5    zv. 4
5  : 16 = 0    zv. 5
```

$84_{10} = 54_{16}$

Min. počet hex-číslic pre číslo 84

$$\lceil \log_{16} 84 \rceil = \lceil 1.598079356 \rceil = 2$$

- **Z 16-sústavy na 10-sústavu**

```
      16²  16¹  16⁰
  x    5    3    C
-------------------
      1280 + 48 + 13 = 1341
```

- **Medzi 2-sústavou a 16-sústavou**

$$2^4 = 16$$

1001110101100010110

↓

100 1110 1011 0001 0110

4 E B 1 6

↓

$1001110101100010110_{10} = 4EB16_{16}$

Násobky jednotiek

IEC prefix		Representations				Customary prefix	
Name	**Symbol**	**Base 2**	**Base 1024**	**Value**	**Base 10**	**Name**	**Symbol**
kibi	Ki	2^{10}	1024^{1}	1024	$= 1.024 \times 10^{3}$	kilo	k[13] or K
mebi	Mi	2^{20}	1024^{2}	1 048 576	$\approx 1.049 \times 10^{6}$	mega	M
gibi	Gi	2^{30}	1024^{3}	1 073 741 824	$\approx 1.074 \times 10^{9}$	giga	G
tebi	Ti	2^{40}	1024^{4}	1 099 511 627 776	$\approx 1.100 \times 10^{12}$	tera	T
pebi	Pi	2^{50}	1024^{5}	1 125 899 906 842 624	$\approx 1.126 \times 10^{15}$	peta	P
exbi	Ei	2^{60}	1024^{6}	1 152 921 504 606 846 976	$\approx 1.153 \times 10^{18}$	exa	E
zebi	Zi	2^{70}	1024^{7}	1 180 591 620 717 411 303 424	$\approx 1.181 \times 10^{21}$	zetta	Z
yobi	Yi	2^{80}	1024^{8}	1 208 925 819 614 629 174 706 176	$\approx 1.209 \times 10^{24}$	yotta	Y

Aritmetika v binárnej sústave

Súčet

```
  0101 (5)
+ 1010 (10)
-----------
  1111 (15)


  1001 (9)
+ 1011 (11)
-----------
 10100 (20)
```

Násobenie

```
    1000 (8)
x   0011 (3)
-------------
    1000
   1000
  0000
0000

-------------
0011000 (24)
```

A	B	+	-	x
0	0	0	0	0
0	1	1	1	0
1	0	1	1	0
1	1	0	0	1

Logické operácie

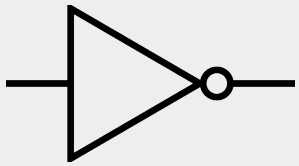
$\neg A = \overline{A}$ $A \wedge B = A \cdot B$ $A \vee B = A + B$ $A \oplus B$

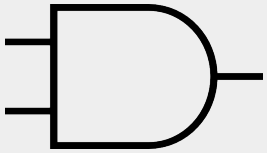
A	NOT
0	1
1	0

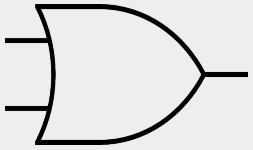
A	B	AND
0	0	0
0	1	0
1	0	0
1	1	1

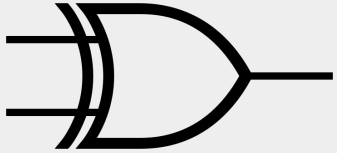
A	B	OR
0	0	0
0	1	1
1	0	1
1	1	1

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0









Kódovanie textu

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(	72	48	H	104	68	h
9	09	Horizontal tab	41	29	)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

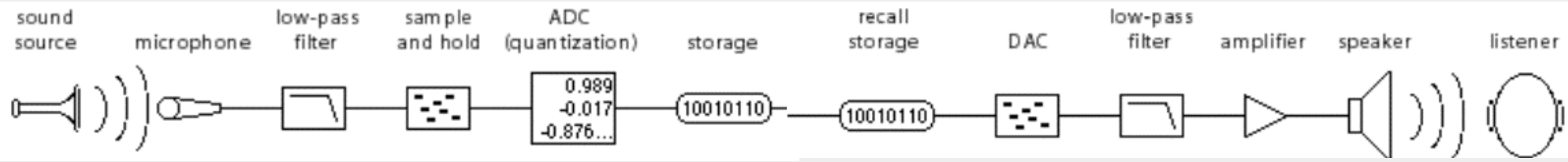
Proces:

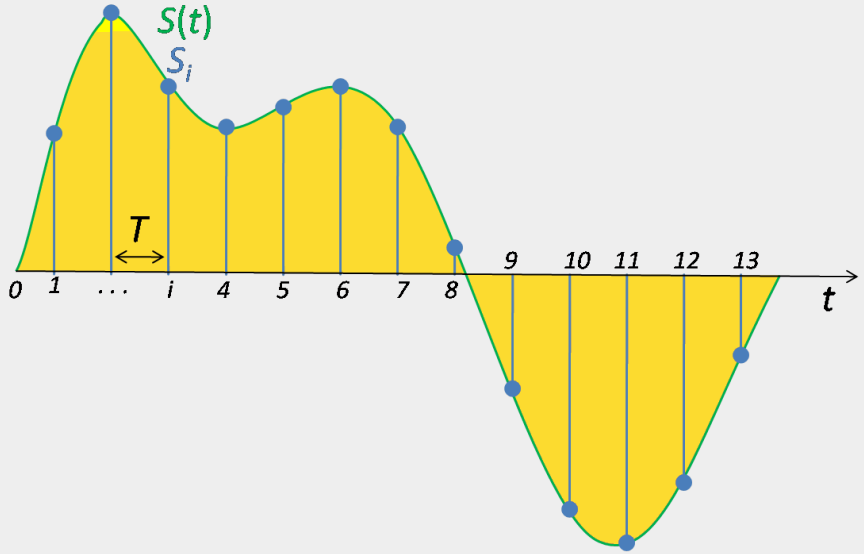
1. Text je rozdelený na jednotlivé znaky
2. Znaky sú prekódované podľa dohodnutej kódovacej tabuľky na čísla

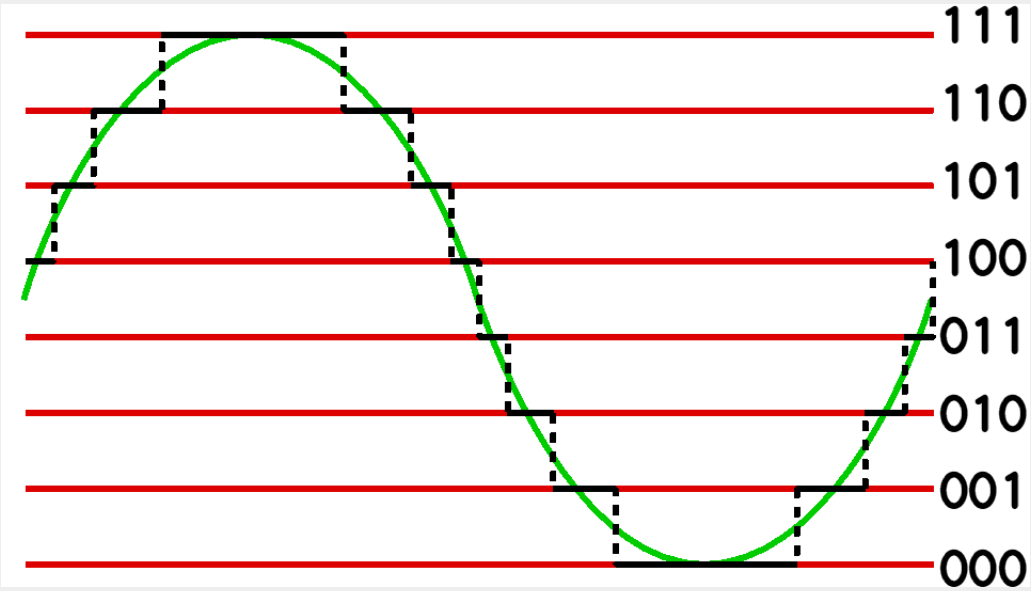
Kódovacie tabuľky:

- EBCDIC (Extended Binary Coded Decimal Interchange Code)
- ASCII (American Standard Code for Information Interchange)
  - 7-bitové kódy (0 - 127)
  - +1 bit na národné abecedy - kódové stránky
- Unicode (UTF-8, UTF-16, UTF-32)

Kódovanie zvuku







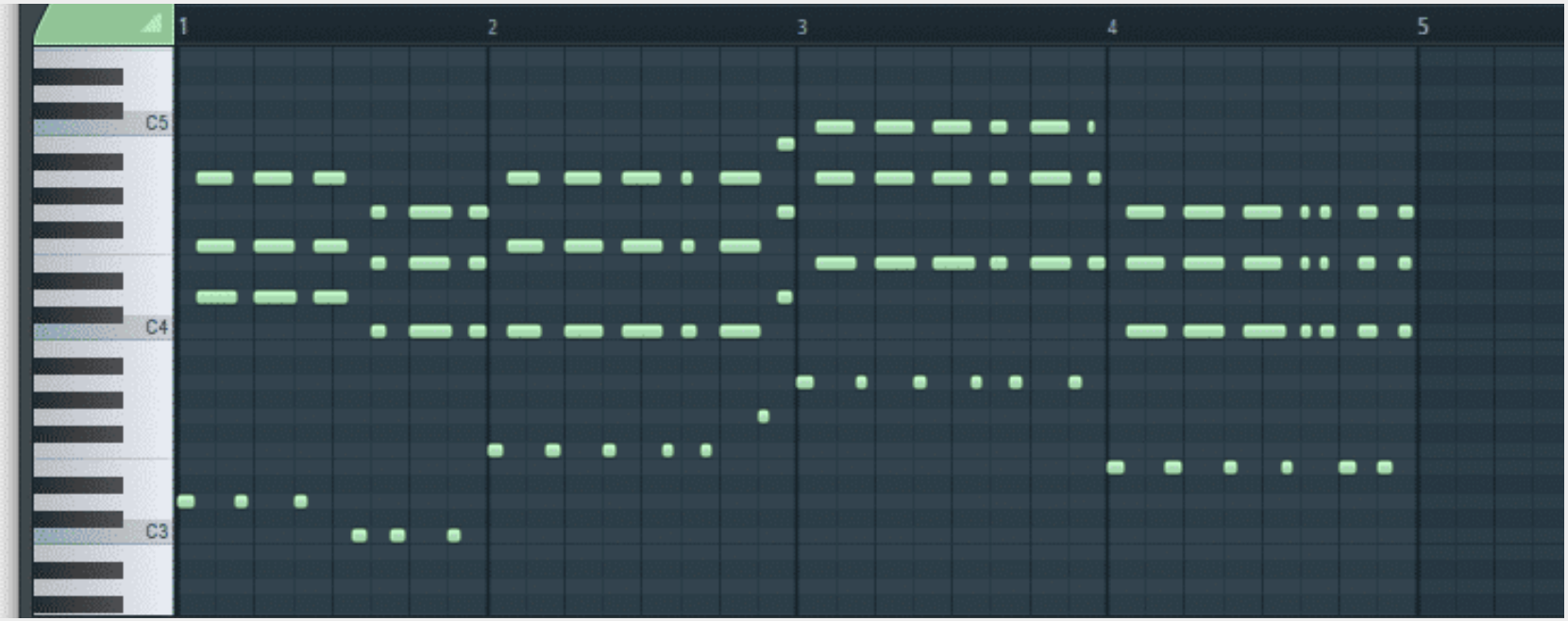
1. **Vzorkovanie** – vzorkovacia frekvencia (44,1 kHz)
2. **Kvantovanie** – bitová hĺbka (8 – 32 bitov)
3. **Kódovanie**

Nyquistova–Shannonova veta o vzorkovaní
„Presná rekonštrukcia spojitého, frekvenčne obmedzeného signálu z jeho vzoriek je možná len vtedy, ak bola vzorkovacia frekvencia vyššia než dvojnásobok najvyššej harmonickej zložky vzorkovaného signálu.“

Veľkosť nekomprimovaného zvuku (B)
Napr.: 48 000 Hz x 16 b x 10 s = 7,32 Mb (0,92 MB)

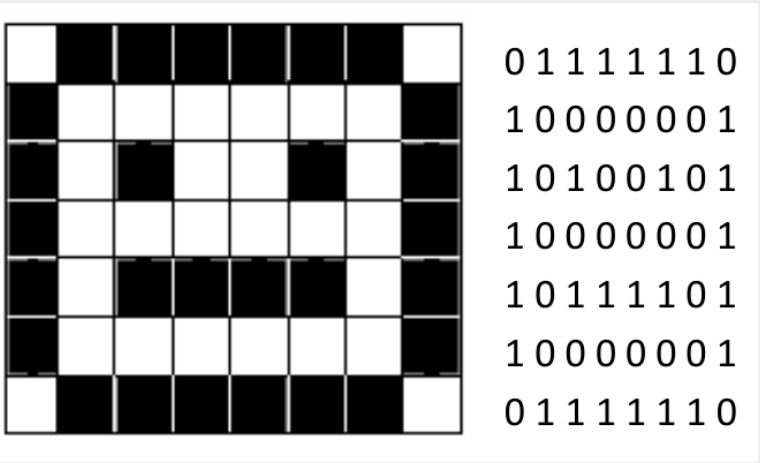
Hudobné súbory MIDI

8.1:000	0:00:16.800	12	Note On	C	3	126	2:257
8.1:000	0:00:16.800	12	Note On	C	5	126	2:257
8.1:000	0:00:16.800	12	Note On	E	5	126	2:257
8.1:000	0:00:16.800	12	Note On	G	5	126	2:257
8.1:000	0:00:16.800	16	Note On	E	5	126	3:001
8.1:000	0:00:16.800	16	Note On	G	5	126	3:001
8.1:000	0:00:16.800	16	Note On	C	6	126	3:001
8.1:000	0:00:16.800	11	Note On	C	3	126	3:001
8.1:000	0:00:16.800	13	Note On	C	3	126	1:001
8.1:000	0:00:16.800	10	Note On	C	3	126	2:001
8.1:000	0:00:16.800	10	Note On	B	4	126	0:129



Kódovanie obrázkov

Rastrové obrázky



Rozlíšenie:

- Obrazové body - pixely (napr. 600x400)

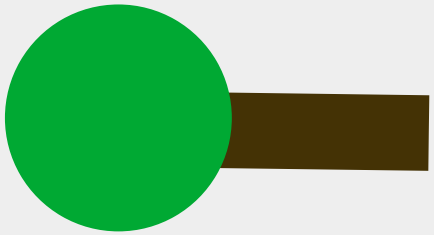
Farebná paleta - bitov/px

- Monochromatická - 2 farby (1 bit)
- Odtiene šedej - 256 farieb (8 bitov)
- High Colour, 65 536 farieb (16 bitov)
- True Colour, 16,7 mil. farieb (24 bitov)

Veľkosť nekomprimovaného obrázka (B):

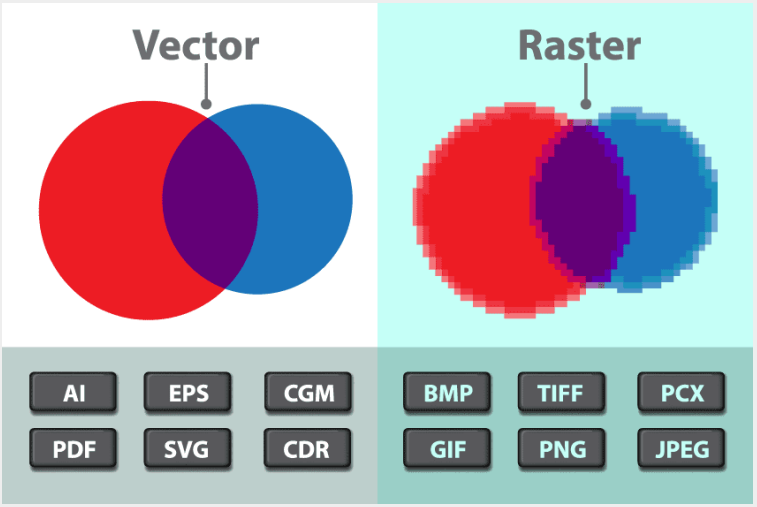
napr.: 600 px x 400 px x 16 b = 3,66 Mb (0,46 MB)

Vektorové obrázky

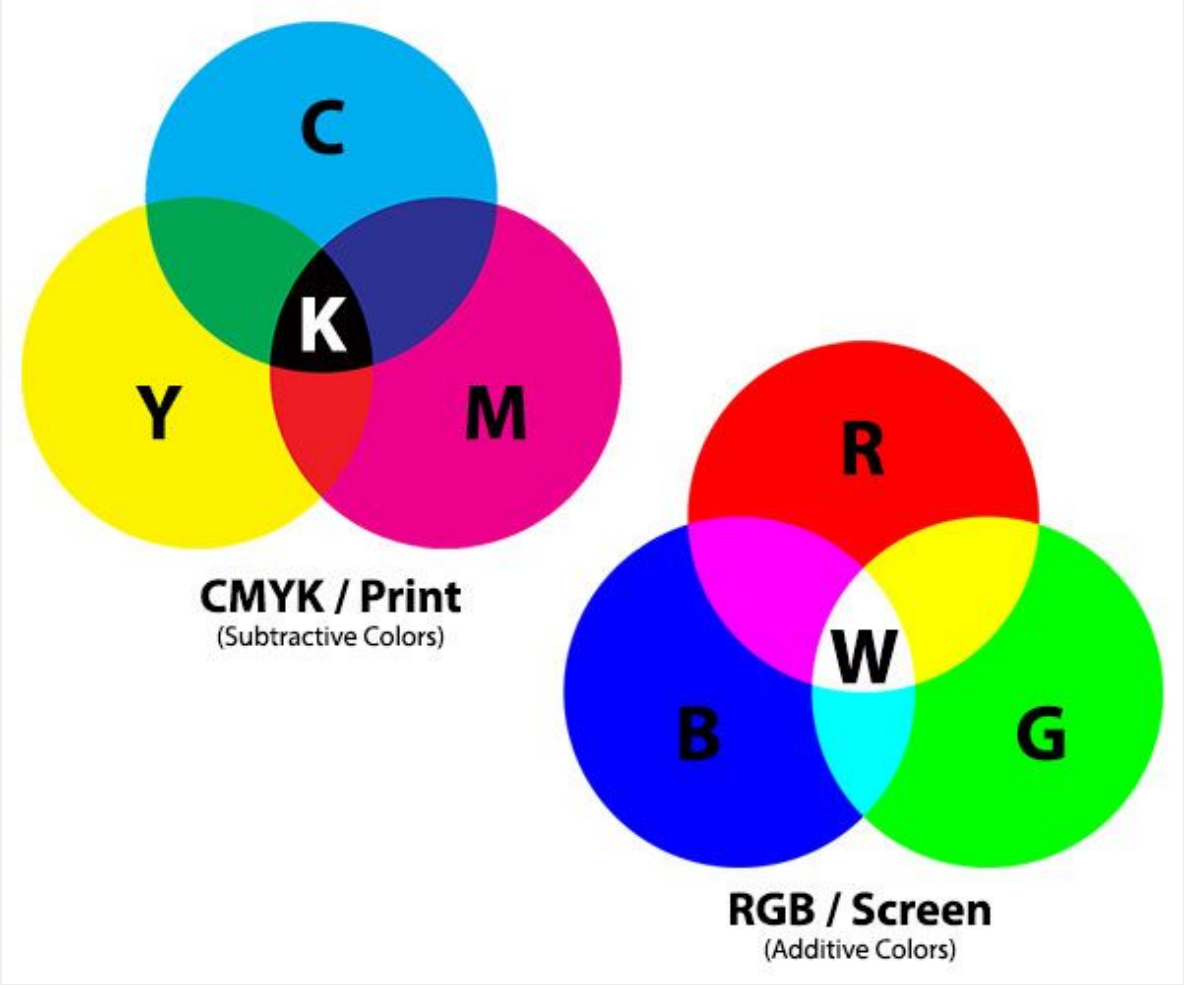


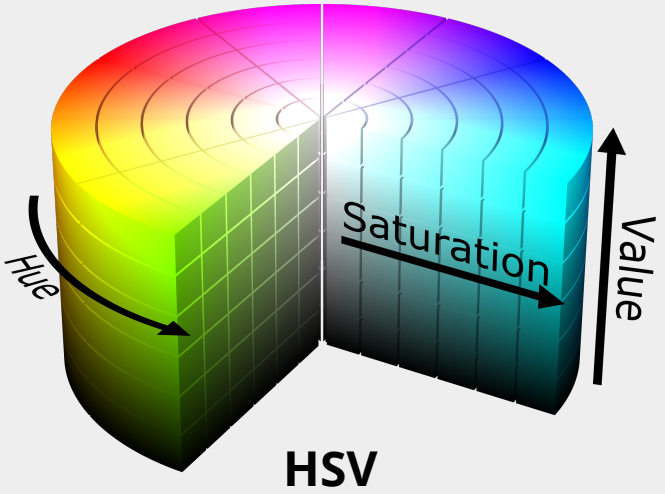
```
<svg>
    <rect width="200" height="100" fill="#443205" />
    <circle cx="75" cy="75" r="75" fill="#00A933" />
</svg>
```

Obrazové formáty



Farebné modely





HSV

Kompresia dát

Bezstratová

- Dokážeme obnoviť pôvodnú informáciu bezo zmeny
- RLE, Lempl-Ziv (LZ77, LZMA, DEFLATE, LZSS)

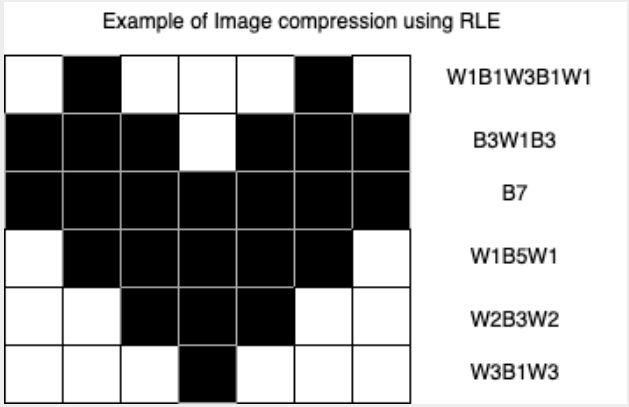
Stratová

- Nedokážeme obnoviť pôvodné dáta
- MP3, JPEG, MPEG

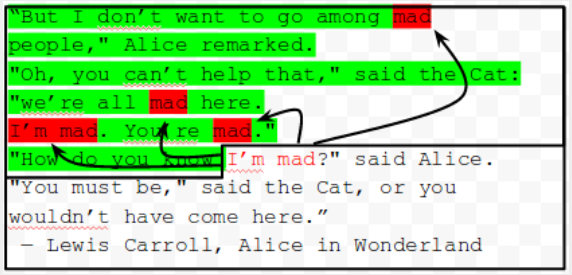
RLE – Run-length Encoding

AAAAAARRRKKKKKKKKMM

A6R3K8M2



LZ77 – Lempel-Ziv



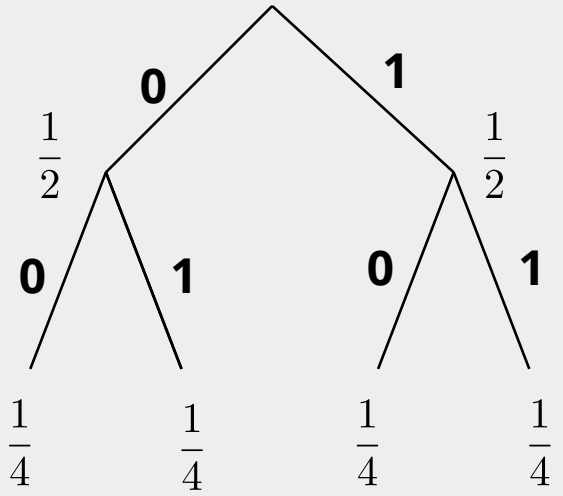
JPEG JFIF

1. Transformácia pôvodných dát
   - DCT, FFT
2. Potlačenie niektorých dát
   - kompresný pomer
3. Kódovanie
   - Huffmanove kódy

Huffmanove stromy

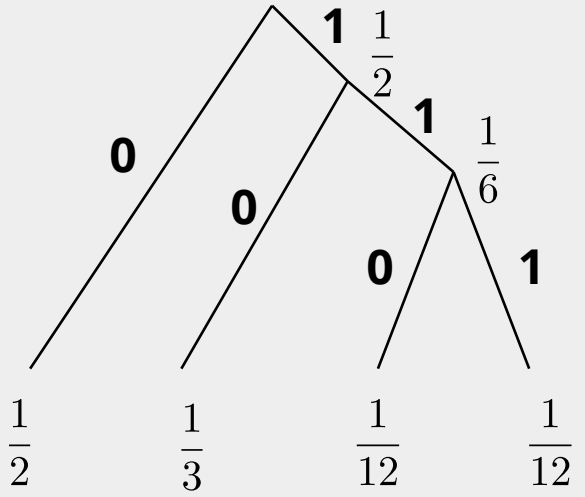
Slnečno	Zamračené	Dážď	Hmla
$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
00	01	10	11

$H = 2$ b



Slnečno	Zamračené	Dážď	Hmla
$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{12}$	$\frac{1}{12}$
0	10	110	111

$H = 1.63$ b



Samodetekujúce a samoopravné kódy

Kontrolný súčet

- Overenie, či je vlastná informácia úplná a nedošlo pri chybe pri prenose

Paritný bit

$$p = x_1 \oplus x_2 \oplus \ldots \oplus x_n$$

- Dopĺňa počet jednotiek v správe na párny počet
- Deteguje 1-bitovú chybu

10010101

01100000

Rodné číslo - Zákon č. 301/1995 §2

821025/9101

rok, mesiac (u žien + 50), deň, koncovka

- Do 1953 - 9-miestne s 3-miestnou koncovkou
- Po 1954 - 10-miestne so 4-miestnou koncovkou
- Celé 10-miestne rodné číslo musí byť bezo zvyšku deliteľné číslom 11.

ISBN (EAN-13)

- Medzinárodné štandardné číslo knihy
- Súčet na nepárnych pozíciach + 3 x Súčet na párnych pozíciach
- Kontrolná cifra - Odpočítame výsledok od zaokrúhlenia na číslo deliteľné desiatimi

Luhnov algorimus

- Platobné karty
- Zdvojnásobenie každej druhej cifry zprava a ciferný súčet výsledku
- Sčítanie cifier a deliteľné 10

Samoopravné kódy:

- Hammingove kódy
- QR Kód – Reed-Solomonov kód

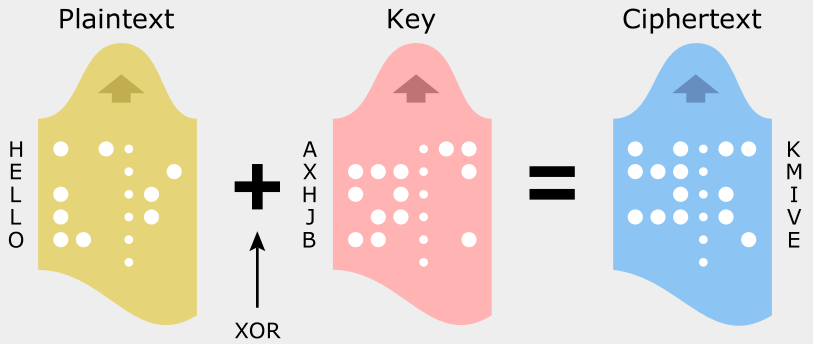
Šifry

- **Šifrovanie** je zapisovanie textu v podobe,
aby mu nepovolaný čitateľ nemal šancu porozumieť.
- **Šifra** = tajné písmo

Vernamova šifra

- Jednorázová tabuľková šifra
- Posun každého znaku o náhodný počet miest
- V princípe nerozlúštiteľná

1) Kľúč je tak dlhý ako správa
2) Kľúč je dokonale náhodný
3) Kľúč nemožno použiť opakovane



Otvorený text **Kľúč** **Zašifrovaný text**

Druhy šifier

- Substitučné
- Transpozičné
- Symetrické
- Asymetrické

Substitučné šifry

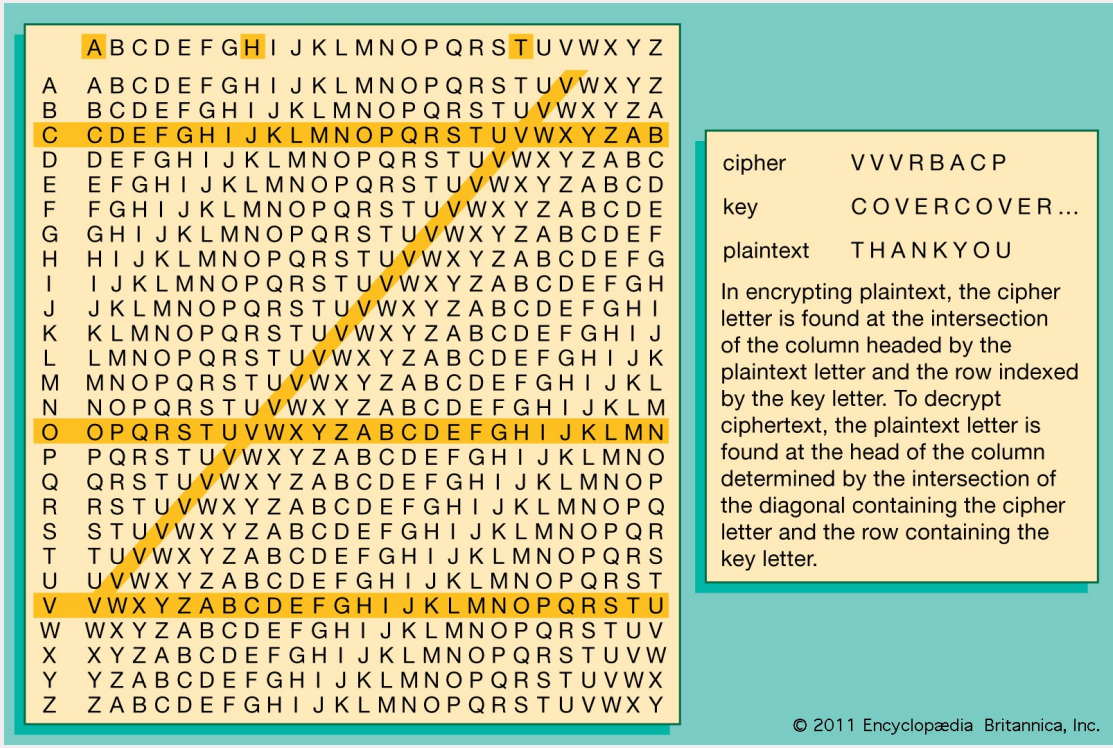
Zámena znaku abecedy otvoreného textu za znak zašifrovanej abecedy

Cézarova šifra

- Posun abecedy o fixný počet písmen (kľúč)
- Prelomiteľná frekvenčnou analýzou

Vigenèrova šifra

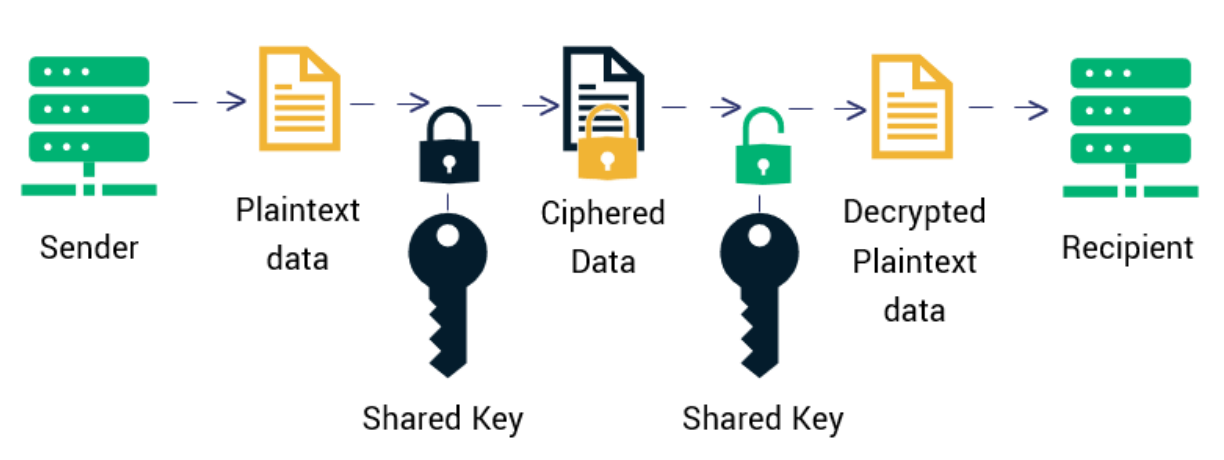
- Slabinou sú krátke kľúče



https://sectigostore.com/blog/types-of-encryption-what-to-know-about-symmetric-vs-asymmetric-encryption/

Symetrické a Asymetrické šifry

Symetrické šifrovanie



Algoritmy

Symetrické šifry:
- DES
- Triple DES
- AES

Výmena kľúčov:
- Diffieho-Hellmanova

Asymetrické šifry:
- RSA

Asymetrické šifrovanie a digitálne podpisy