→ Vysvetlite binárny zápis čísla, sčítajte a vynásobte binárne čísla: 1011 a 101.

Prirodzenou sústavou počítača je dvojková - **binárna** sústava (kvôli jednotke informácie 1 bitu, ktorý môže nadobúdať dve hodnoty 0 a 1). V jednej pamäťovej bunke počítača je však 8 bitov, preto vždy doplňujeme cifry tak, aby bol ich počet deliteľný číslom 8 (8, 16, 24, 32 ...).
$(01101100)_B = 0.2^7 + 1.2^6 + 1.2^5 + 0.2^4 + 1.2^3 + 1.2^2 + 0.2^1 + 0.2^0 = 108$

$(1011)_B + (101)_B =$ **$(10000)_B$** $(1011)_B * (101)_B =$ **$(110111)_B$**

→ Stručne popíšte generácie počítačov podľa princípu ich fungovania v závislosti od vývoja použitých technických súčiastok.

Nultá generácia počítačov (30-te roky) = **elektromagnetického relé** - veľkosť haly
- vojenské účely
- Konrád Zuse zostrojil elektromechanický počítací automat **Z-1**, neskôr **Z-3** (skladal sa z 2600 relé)
- Howard Aiken (zakladateľ firmy IBM) uviedol do prevádzky MARK I, ktorý mal 5,5 t, dĺžku 15 m a pracoval v 10-kovej sústave

Prvá generácia počítačov 1944 - 1956 (40-te roky) = **elektrónka** - veľkosť haly
- vojenské účely
- ENIAC, prvý elektrónkový počítač pracoval v 10. sústave, postavený z 18000 elektróniek, chladených 2 leteckými motormi (30t monštrum)

Druhá generácia počítačov 1956 - 1964 (50-te roky) = **tranzistor** - veľkosť miestnosti
- nahradil veľkú elektrónku, pričom zmena stavu tranzistora sa udeje za 1 nanosekundu.
- počítače tejto generácie pracovali s magnetickými pamäťami
- programy sa písali v nižších programovacích jazykoch, úlohy spracovávali dávkovo
- slúžili hlavne na hromadné spracovanie dát, ako aj vedecko - technické výpočty, vojenské účely

Tretia generácia počítačov 1964 – 1980 (60-te roky) = **integrovaný obvod** - veľkosť skrine
- slúžil na hromadné spracovanie dát, vedecké výpočty, riadenie prevádzky strojov, armáda
- počítače využívali diskové magnetické pamäte, vyrovnávacie pamäte, operačnú pamäť na princípe IO, viacužívateľské OS, programovalo sa už vo vyšších programovacích jazykoch.

Štvrtá generácia počítačov 1980 - 1990 (70-te roky) = **integrovaný obvod s vysokou hustotou integrácie**
- veľkosť skrinky - vysoká hustota integrácie zmenšila rozmery počítača a mohol byť umiestnený na stôl
- mal jednoužívateľský jednoúlohový operačný systém DOS a mal označenie 8088; na 1 cm^2 bolo umiestnených až 100000 prvkov; začala tak éra 8-bitových počítačov
- mikroprocesor s označením 80286 však pracoval už so 16-bitovým slovom, 80486 s 32-bitovým slovom
- široké využitie v ekonomike, vede, armáde

Piata generácia počítačov (80-te roky) = **mikroprocesor** - na stole
- mikroprocesor s ultra vysokou hustotou integrácie (5 miliónov akt. prvkov) napr. od firmy Intel je skôr známy pod názvom "pentium". Pracuje už s 64 - bitovým slovom
- využitie vo všetkých oblastiach spracovania a prenosu informácií

Šiesta generácia počítačov (90-te roky) = **výkonnejší mikroprocesor** - veľkosť zošitu A4
- výkonnosť sa zvyšuje paralelnými systémami - viacerými mikroprocesormi, ktoré si vedia úlohy "podeliť medzi seba"
- využitie vo všetkých oblastiach ľudského života

→ Vysvetlite princíp šifrovania dokumentu pomocou elektronického podpisu, vyhľadajte na Internete inštitúciu, kde je možné vytvoriť si elektronický podpis a zobrazte cenové ponuky jednotlivých produktov.

V súčasnosti je možné písomnosti posielať elektronickou formou. Aby bolo možné odoslaným dokumentom dôverovať, je potrebné zaručiť nepopierateľnosť a nepozmeniteľnosť dokumentov. Na tento účel slúži **elektronický podpis**, ktorý je založený na asymetrickom šifrovaní - t.j. pomocou dvojice ku sebe patriacich elektronických kľúčov - verejného kľúča a súkromného kľúča. Princíp fungovania je nasledujúci:

- Na strane, ktorá vytvára dokument, sa najskôr vytvorí jednoznačný obtlačok dokumentu HASH (vlastnosti ako obtlačok prsta). To znamená, že pre dva rôzne dokumenty sa nikdy nevygeneruje rovnaký obtlačok.
- Obtlačok sa podpíše **súkromným kľúčom**, ktorý vlastní iba tvorca dokumentu.
- Takto zašifrovaný obtlačok sa pripojí k dokumentu a odošle sa prijímateľovi
- Na strane prijímateľa sa rovnakým spôsobom vytvorí HASH obtlačok dokumentu.
- Potom sa zoberie zašifrovaný obtlačok, ktorý je pripojený k dokumentu a dešifruje sa **verejným kľúčom**, ktorý prislúcha k súkromnému kľúču tvorcu dokumentu.
- Nakoniec sa porovnajú