# 2- Základní programové konstrukce

# Algoritmus

* Teoretický přesný postup, kterým lze vyřešit určitý problém
* Vlastnosti:
  + Elementárnost: skládá se z konečného počtu jednoduchých a snadno srozumitelných kroků
  + Konečnost: Musí mít konečný počet kroků pro každý vstup
  + Obecnost: Algoritmus řeší problém bez ohledu na vstup
  + Determinovanost: Za stejných podmínek pro stejné vstupy stejný výstup (až na prvek náhodnosti); předurčitost
  + Výstup: Má alespoň jeden výstup v požadovaném vztahu ke vstupům

# Algoritmická složitost

* Slouží k porovnávání kvality algoritmů, které řeší stejný problém
* Složitost se určuje funkcí závislou na velikost vstupních dat To ovlivňuje, jak rychle se algoritmus dokončí, případně jak náročný bude běh algoritmu na procesorový čas či kapacitu paměti
* Značí se O()
* Bubble-sort – O(n2)

# Rekurze

* Stav, kdy je objekt součástí sebe samého
* Funkce je znovu volána dříve, než se dokončilo její předchozí volání
* Funkce volá sama sebe
* Přímá rekurze: Funkce volá sama sebe
* Nepřímá: Více podprogramů se volá navzájem
* Lineární: Podprogram volá sám sebe vždy jednou
* Stromová: Podprogram se volá sama sebe vícekrát s různými parametry

# Náhodnost

* Šifrován, simulace, generace úrovní ve hrách

## Pravá náhodná čísla

* Hardwarový generátor náhodných čísel
* TPM (Trusted Platform Module)
  + Čip, který popisuje zabezpečený kryptoprocesor (šifrovací procesor), na který lze ukládat šifrovací klíče
  + Obsahuje RNG (Random Number Generator), který využívá ke generaci tepelný šum, proudění vzduchu atd.
  + Tyto hodnoty se poté zahashují

## Čísla pseudonáhodná

* Generování softwarově, později se sekvence opakují
* Jako základ (seed) se používají např. hodiny v PC, které měří čas v ms