Složitost a moderní kryptografie

Radek Pelánek

Modulární systém dalšího vzdělávání pedagogických pracovníků JmK
v přírodních vědách a informatice CZ.1.07/1.3.10/02.0024

Složitost a moderní kryptografie

- Kerckhoffův princip:
  - bezpečnost šifry – nikoliv utajení principu pouze hesla
- kryptografie tedy potřebuje:
  - rychlé zašifrování a dešifrování při znalosti hesla
  - náročné dešifrování bez znalosti hesla
- teorie složitosti: jak rychle lze (umíme) řešit problémy

Teorie složitosti

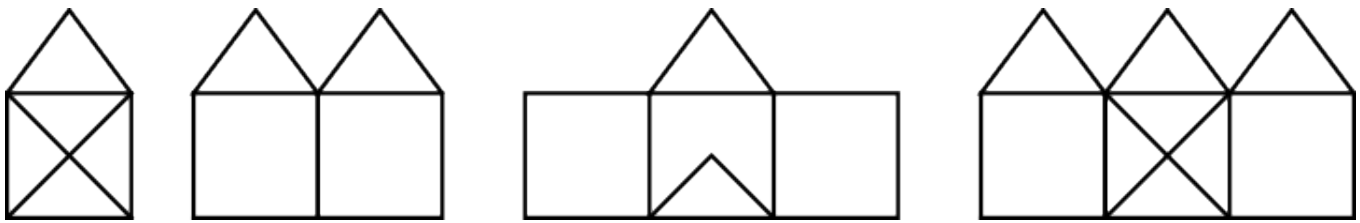
- délka výpočtu algoritmu nad konkrétním vstupem
- složitost algoritmu $\sim$ délka výpočtu v nejhorším případě
- složitost problému $\sim$ složitost nejlepšího algoritmu

příklad: řadicí algoritmy

Složitostní třídy

- L – logaritmický prostor
- **P** (PTIME) – polynominální čas
- **NP** – nedeterministický polynomiální čas
  - uhádni řešení a pak polynomiálně ověř, že je správně
- PSPACE – polynominální prostor
- EXPTIME
- ...

Příklad



- *Eulerovská cesta*: navštívit každou hranu právě jednou
  - **P** – lze řešit efektivně
- *Hamiltonovská cesta*: navštívit každý vrchol právě jednou
  - **NP** – lze ověřit efektivně, ale neumíme hledat efektivně

NP-úplné problémy

- „nejtěžší“ problémy z třídy NP
- redukce problémů, pokud umíme vyřešit NP-úplný problém, umíme libovolný NP problém
- příklady:
  - Hamiltonovská cesta
  - barvení grafu
  - splnitelnost booleanovských formulí
  - zobecněné Sudoku
  - podmnožinový součet

Problém P vs NP

P =? NP

- většina věří, že P $\neq$ NP
- jeden z „Millennium Prize Problems“, odměna 1 milión dolarů
- kryptografie založena na P $\neq$ NP

Násobení a faktorizace

$$197 \cdot 261 = 51417$$

- jednosměrná funkce
- násobení – jednoduché
- faktorizace na prvočísla
  - náročné (neumíme v P)
  - není však NP-úplné
- (generování/rozpoznání prvočísla – „jednoduché“)

Házení mincí pomocí faktorizace

- Alice: vygeneruje prvočísla a vynásobí je.
- Bob hádá: jde o součin lichého či sudého počtu prvočísel?
- Alice: řekne prvočísla.
- Bob: může snadno ověřit.

Kryptografie

- symetrická šifra
  - šifrování i dešifrování stejný klíč
- asymetrická šifra
  - veřejný klíč – zašifrování
  - soukromý klíč – dešifrování

Asymetrická kryptografie: poslání zprávy

- Alice: vytvoří soukromý a veřejný klíč.
- Alice: zveřejní veřejný klíč (problematika certifikace).

- Bob: zpráva + veřejný klíč Alice $\rightarrow$ šifrovaný text.
- Eva: šifrovaný text $\rightarrow$???
- Alice: šifrovaný text + soukromý klíč $\rightarrow$ zpráva.

Asymetrická kryptografie: podpis

- Alice: vytvoří soukromý a veřejný klíč.
- Alice: zveřejní veřejný klíč (problematika certifikace).

- Alice: zpráva + soukromý klíč $\rightarrow$ podepsaná zpráva
- Bob: podepsaná zpráva + veřejný klíč Alice $\rightarrow$ zpráva
- Bob si může být jistý, že zprávu poslala Alice.

(praktická pozn.: podepisuje se hash zprávy)

Šifra RSA

- RSA = Rivest, Shamir, Adleman
- asymetrická šifra založená na problému faktorizace
- soukromý klíč $\sim$ dvě velká prvočísla p, q
- veřejný klíč $\sim$ součin $p \cdot q$

Šifra RSA

- Zvolte dvě tajná prvočísla p, q.
- Spočítejte $n = p \cdot q$ a $r = (p-1) \cdot (q-1)$.
- Zvolte číslo k nesoudělné s r a najděte g tak, aby $g \cdot k \mod r = 1$
- Dvojice (k, n) je veřejný klíč, g je soukromý klíč.
- Zprávu $M \leq n-1$ nyní zašifrujeme jako $e(M) = M^k \mod n = H$.
- Zašifrovanou zprávu H dešifrujeme jako $d(H) = H^g \mod n = M$.
- Korektnost založena na Fermatově větě: $a^{p-1} \mod p = 1$.

RSA, faktorizace, vývoj

- bezpečnost RSA založena na obtížnosti faktorizace
- aktuální stav:
  - 100 ciferná čísla běžně faktorizovatelná, hranice kolem 200 cifer (700 bitů)
  - klíče: zatím bezpečné 1024 bitů, doporučuje se 2048 bitů
- současné techniky: kombinace komplikované matematiky („General Number Field Sieve“) a speciálního hardware, paralelizace, ...

Praktické použití

- asymetrické šifrování – výpočetně náročné
- symetrické šifrování rychlejší
- praktický postup (hybridní kryptografie):
  - asymetrická šifra – domluva klíče S
  - symetrická šifra s klíčem S – vlastní komunikace

Shrnutí

Bezpečnost kryptografie stojí na mnoha předpokladech:

- princip: problém, na kterém je šifra založena je opravdu těžký a nelze ho obejít
  (utajujeme klíč nikoliv algoritmus)
- klíč: použitý klíč je dostatečně velký a vhodně zvolený
- použití: používáme systém správně