Úvod do teorie čísel a RSA

Anotace

Řekneme si, čím se zabývá teorie čísel a vysvětlíme si její nejznámější aplikaci, RSA. Vybudujeme teorii kolem dělitelnosti, řekneme si základní větu aritmetiky, vysvětlíme si Eukleidův algoritmus, Bezoutovu rovnost, Eulerovu funkci a důležité vlastnosti prvočísel. Když budeme znát všechny tyto pojmy, můžeme se pustit do vysvětlení, proč vlastně RSA funguje. Na závěr si řekneme slabiny RSA a proč už se dneska přestává používat.

Poznámky

Dělitelnost

Znaménko dělitelnosti

a dělí b, pokud platí, že existuje celé číslo c takové, $a \cdot c = b$

Věta o dělení se zbytkem

Každé celé číslo jde podělit jiným číslem se zbytkem, tedy $a = b \cdot r + q$. Značíme $a \equiv q \pmod b$.

Euklidův algoritmus

```
def eucleides(x, y):
    while x != y:
        if x > y:
            x -= y
        else:
            y -= x
    return x
```

Bézoutova rovnost

Pro každou dvojici celých čísel a, b existují 2 celá čísla u, v taková, že $u \cdot a + v \cdot b = NSD(a, b)$.

```
def bezout(a, b):
    if b == 0:
        return 1, 0, a
    else:
        q, r = a // b, a % b
        x, y, g = bezout(b, r)
        return y, x - q * y, g
```

Věta o dělitelnosti součinu

Pokud $p|a \cdot b$, kde p je prvočíslo, pak buď $p|a$ nebo $p|b$.

Základní věta algebry

Každé přirozené číslo jde jednoznačně rozložit na součin mocnin prvočísel.

Příklady

1. Najděte $NSD(168, 396)$. (12)
2. Najděte $NSD(37, 10)$ a příslušné Bézoutovy koeficienty. $(1 = 3 \cdot 37 - 11 \cdot 10)$
3. Najděte $NSD(1023, 96)$ a příslušné Bézoutovy koeficienty. $(3 = (-3) \cdot 1023 + 32 \cdot 96)$
4. Najděte $NSD(F_n, F_{n+1})$ a příslušné Bézoutovy koeficienty. $(\pm 1 = F_{n-1} \cdot F_n - F_{n-2} \cdot F_{n+1})$
5. Euklidův algoritmus jde provádět i s polynomy. Spočítejte $NSD(x^3 + x^2 + x + 1, x^2 + 2x + 1)$ a Bézoutovy koeficienty. $(1 = \frac{1-x}{5}(x^3 + x^2 + x + 1) + \frac{1}{5}(x^2 + 2x + 1))$

Modulární aritmetika

Základní vlastnosti

Kongrunce je ekvivalence:

1. $a \equiv a \pmod{m}$
2. $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$
3. $a \equiv b \pmod{m}$ & $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$
   Nechť $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, pak platí:
4. $a + c \equiv b + d \pmod{m}$
5. $a - c \equiv b - d \pmod{m}$
6. $a \cdot c \equiv b \cdot d \pmod{m}$
7. $a \equiv b \pmod{m} \iff ae \equiv be \pmod{em}$
8. Jsou-li e a m nesoudělná, pak $a \equiv b \pmod{m} \iff ae \equiv be \pmod{m}$

Příklady

1. Vyřešte rovnici $x \equiv 4 \pmod{7}$. $(\{7k + 4 | k \in \mathbb{Z}\})$
2. Vyřešte rovnici $2x \equiv 7 \pmod{11}$. $(\{11k + 9 | k \in \mathbb{Z}\})$
3. Vyřešte rovnici $4x \equiv 10 \pmod{14}$. $(\{7k + 6 | k \in \mathbb{Z}\})$
4. Vyřešte rovnici $x^2 + 5x \equiv 0 \pmod{19}$. $(\{19k,\ 19k + 14 | k \in \mathbb{Z}\})$
5. Pomocí modulární aritmetiky odvoďte kritéria dělitelnosti pro čísla 9 a 11.
6. Ukažte, že století nikdy nebude začínat středou, pátkem ani nedělí.

Eulerova věta a inverze

Eulerova funkce

Eulerova funkce $\varphi(n)$ označuje počet čísel $\{1, 2, \ldots, n\}$ nesoudělných s n, tj. $NSD(k, n) = 1$.

Hodnota Eulerovy funkce pro prvočíslo

Pro p prvočíslo je $\varphi(p) = p - 1$.

Hodnota Eulerovy funkce pro součin 2 různých prvočísel

Pro p, q různá prvočísla je $\varphi(p, q) = (p-1)(q-1)$.

Malá Fermatova věta

Pro p prvočíslo a a nesoudělné s p platí $a^p \equiv a \pmod{p}$.

Eulerova věta

Pro a, m nesoudělná platí $a^{\varphi(m)} \equiv 1 \pmod{m}$

Existence inverze

Pro a, m nesoudělná vždy existuje číslo b takové, že $a \cdot b \equiv 1 \pmod{m}$. Takové číslo značíme a^{-1}. Toto číslo můžete nalézt pomocí algoritmu na Bézoutovu rovnost.

Příklady

1. Zjistěte $\varphi(91)$. (72)
2. Spočítejte $3^{425} \pmod{19}$. (10)
3. Spočítejte $7^{7^7} \pmod{11}$. (2)
4. Vyřešte rovnici $37x \equiv 1 \pmod{61}$. $(\{61k + 33 | k \in \mathbb{Z}\})$
5. Dokažte malou Fermatovu větu.

RSA

Asymetrické šifrování

Alice a Bob si chtějí poslat zprávu. Jenže se předem nedomluvili, jaký klíč budou používat. A tak se rozhodli, že si ten klíč pošlou pomocí asymetrické šifry. Bob si vytvoří privátní a veřejný klíč. Privátní si u sebe schová, veřejný pošle Alici. Ta vezme zprávu, třeba klíč pro symetrické šifrování, a zašifruje ji pomocí veřejného klíče. Takto zašifrovanou zprávu pošle Bobovi. Ten ji jako jediný držitel privátního klíče dovede rozluštit.

Generování klíče

1. Vybereme si náhodná velká prvočísla p, q. Spočítáme jejich součin $pq = N$. Taktéž spočítáme $\varphi(N) = (p-1)(q-1)$.
2. Zvolíme náhodné číslo e nesoudělné s $\varphi(N)$. Pomocí Euklidova algoritmu spočítáme d takové, že $ed \equiv 1 \pmod{\varphi(N)}$.
   (N, e) je veřejný klíč, d je klíč soukromý.

Zašifrování zprávy

Mějme zprávu x. Spočítáme $y \equiv x^e \pmod{N}$. y je zašifrovaná zpráva.

Dešifrování zprávy

Mějme zašifrovanou zprávu y. Tu dešifujeme Následovně: $y^d \equiv (x^e)^d \equiv x^{ed} \equiv x \pmod{N}$.

Výhody RSA

1. Jednoduchý algoritmus
2. Neexistuje rychlý způsob faktorizace čísla nebo počítání hodnoty eulerovy funkce, pokud je N součin 2 velkých prvočísel.

Nevýhody RSA

1. Pomalé
2. Ne vždy, co vygenerujeme, je prvočíslo.
3. Příliš malé e usnadňuje rychlejší prolomení šifry (nejčastěji $e = 2^{16} + 1 = 65537$)

Digitální podpis

1. Integrita zprávy
2. Autentizace odesílatele zprávy
3. Nepopiratelnost původu zprávy

Podpisové schéma RSA

Veřejný klíč je opět (N, e), soukromý d.
Podpis zprávy x je $y \equiv x^d \pmod N$.
Verifikace probíhá porovnáním x s hodnotou $y^e \pmod N$. Pokud je y opravdu podpis x, pak by verifikační funkce měla vrátit True.
Obvykle se místo celé zprávy používá pouze její hash.
Existuje i takzvaný slepý podpis RSA. Využití: elektronické volby, kryptoměny.