Motto: "Matematika je schovaná všude, ovšem ne každý ji vidí"

Cílem přednášky je ukázat několik abstraktních matematických výsledků, které se používají při řešení praktických problémů. Některé matematické věty ovšem našly uplatnění až mnoho desítek či stovek let po svém vzniku.

Teorie čísel - šifrování zpráv

V dřívějších dobách se k šifrování používal *tajný klíč*. Nevýhodou bylo, že jej musely znát všechny komunikující strany a snadno mohlo dojít k jeho prozrazení. Ukážeme si metodu **RSA**, která slouží pro bezpečné šifrování pomocí veřejného klíče. Název metody je odvozen od iniciálů autorů: R. I. **R**ivest, A. **S**hamir, L.M. **A**dleman (1978).

Princip metody:

Alice a Bob si potřebují posílat zprávy. Nejprve textové zprávě přiřadí přirozené číslo (např. pomocí ASCII kódu). Pro vlastní šifrování si Alice a Bob vyberou každý 2 velká prvočísla (alespoň 200 cifer). Označíme je p_A, q_A pro Alici a p_B, q_B pro Boba. Každý si svá prvočísla vynásobí a získá číslo $n_A = p_A \cdot q_A$ (Alice) a $n_B = p_B \cdot q_B$ (Bob). Dále je ještě nutné zvolit tzv. **šifrovací exponenty** e_A (Alice) a e_B (Bob) a vypočítat **dešifrovací exponenty** d_A a d_B (podrobnosti viz. dále).

Každý zveřejní dvojici (n_A, e_A) a (n_B, e_B). A pokud chce jeden druhému poslat zprávu, použije pro šifrování klíč toho druhého. Řekneme, že Bob chce poslat Alici zprávu. Po převedení do ASCII kódu ji označíme X a nechť platí, že $X < n_A$ (pokud by bylo větší, rozdělila by se zpráva na více menších). šifrovanou zprávu označíme X^* a získáme jí z vlastnosti (kongruence):

$$X^* \equiv X^{e_A} \mod n_A,$$

jiným způsobem řečeno: dělíme-li X^{e_A} číslem n_A, vyjde X^* jako celočíselný zbytek ($X^* < n_A$). Alice zprávu dešifruje na číslo $(X^*)^*$ pomocí vlastnosti:

$$(X^*)^* \equiv (X^*)^{d_A} \mod n_A.$$

Otázka: Jak se určí e_A, d_A, aby platilo, že se dešifrovaná zpráva $(X^*)^*$ rovná původní zprávě X^*?

- Důležitou úlohu hraje tzv. Eulerova funkce $\varphi(n)$, která je definována jako počet přirozených čísel nepřevyšujících n, jež jsou s n nesoudělná.
- Je-li n dáno součinem 2 prvočísel ($p \neq q$), potom platí:

$$\varphi(n) = \underbrace{(p-1)}_{\varphi(p)} \cdot \underbrace{(q-1)}_{\varphi(q)} = \underbrace{p \cdot q}_{n} - (\underbrace{p}_{(1)} + \underbrace{q-1}_{(2)}),$$

(1) musím odečíst p násobků čísla q,

(2) musím odečíst q násobků čísla p, ale pq jsem už odečetl.

Příklady:

a) $125 \equiv 6 \mod 7$

$125 : 7 = 17$
55
-49
6

b) $100 \equiv 0 \mod 20$

$100 = 5 \cdot 20$

c) $1000 \equiv 12 \mod 13$

$1000 : 13 = 76$
-91
90
-78
12

- Šifrovací a dešifrovací exponent musí splňovat podmínku:

$$e \cdot d \equiv 1 \mod \varphi(n)$$

- Šifrovací exponent e musí být zvolen tak, aby byl s $\varphi(n)$ nesoudělný.

Odpověď na otázku:

Jsou-li e_A a $\varphi(n_A)$ nesoudělná a $e_A \cdot d_A \equiv 1 \mod \varphi(n_A) \quad \Rightarrow \quad (X^*)^* = X$

Důkaz je založen na **Euler-Fermatově větě** (18. století)

Pro nesoudělná x a n platí: $x^{\varphi(n)} \equiv 1 \mod n$.

Hlavní trik metody RSA

Vynásobit 2 velká prvočísla je velmi snadné, zatímco zpětně rozložit tento součin na prvočinitele není v současnosti v rozumném čase možné.

Pokud neznám rozklad na prvočinitele, nemůžu určit hodnotu Eulerovy funkce a tudíž nemohu určit dešifrovací exponent (ten je tajný a bez něj zprávu nelze dešifrovat).

Náznak důkazu:

Š: $X^* \equiv X^{e_A} \mod n_A \quad \Rightarrow \quad (X^*)^{d_A} \equiv (X^{e_A})^{d_A} = X^{e_A \cdot d_A} \mod n_A \qquad (A)$

D: $(X^*)^* \equiv (X^*)^{d_A} \mod n_A \qquad (B)$

Dále platilo:

$$e_A \cdot d_A \equiv 1 \mod (p_A - 1) \text{ a}$$
$$e_A \cdot d_A \equiv 1 \mod (q_A - 1).$$

Malá Fermatova věta: $\forall p$ prvočíslo a $\forall a \in Z$ nesoudělné: $a^{p-1} \equiv 1 \mod p$.

$\Rightarrow \qquad X^{e_A \cdot d_A} \equiv X \mod p_A$

$\Rightarrow \qquad X^{e_A \cdot d_A} \equiv X \mod q_A$

Čínská věta o zbytcích $\Rightarrow \quad X^{e_A \cdot d_A} \equiv X \mod \underbrace{p_A \cdot q_A}_{n_A} \qquad (C)$

$(A) + (C) \Rightarrow \qquad (X^*)^{d_A} \equiv X \mod n_A \qquad (D)$

$(B) + (D) \Rightarrow \qquad (X^*)^* = X$

□

Ukázkový příklad:

Uvažujeme velmi malá prvočísla - v praxi se používají o mnoho řádů větší.

$p_A = 61$ a $q_A = 53$ jsou dvě zvolená prvočísla

$n_A = p_A \cdot q_A = 3\ 233 \quad \ldots$ **modul** (veřejný)

$e_A = 17 \ldots$ zvolený **šifrovací exponent** tak, aby byl nesoudělný s

$$\varphi(n_A) = (p_A - 1)(q_A - 1) = 60 \cdot 52 = 3120$$

$d_A = 2\ 753 \ldots$ vypočtený soukromý **dešifrovací exponent** tak, aby platilo:

$d_A \cdot e_A \equiv 1 \mod \varphi(n_A)$

čili $d_A \cdot 17 \equiv 1 \mod 3120 \quad (d_A < n_A$ takové, že toto splňuje je jediné)

Veřejný klíč = modul + šifrovací exponent: $n_A = 3233$ a $e_A = 17$

```
   Generovani verejneho a tajneho klice pro sifrovani
-----------------------------------------------------------

 Prvni zadane prvocislo     p = 61 .
 Druhe zadane prvocislo     q = 53 .
 Zadany sifrovaci exponent  e = 17 .

 Verejny modul    n = p * q  = 3233
 Eulerova funkce  phi = (p-1) * (q-1) = 3120

 Spravne zadani pro sifrovani:
 -----------------------------

  1. prvocislo je   p = 61
  2. prvocislo je   q = 53
  Eulerova funkce phi = 3120
  verejny klic je   n = 3233, e = 17
  tajny klic   je   d = 2753
```

Chceme zašifrovat třeba zprávu $X = 123$.

$$X^* = 123^{17} \mod 3233 = 855$$

Dešifrujeme

$$(X^*)^* = 855^{2753} \mod 3233 = 123 = X.$$

```
                  Sifrovaci metoda RSA
-----------------------------------------------------------

 Prvni zadane prvocislo     p = 61 .
 Druhe zadane prvocislo     q = 53 .
 Zadany sifrovaci exponent  e = 17 .

 Verejny modul    n = p * q  = 3233
 Eulerova funkce  phi = (p-1) * (q-1) = 3120


  Verejny klic je   n = 3233, e = 17
  Tajny klic   je   d = 2753

  Zadej zpravu  ( 0<x<3233 )       x=123
  Sifrovana zprava je     855
  Desifrovana zprava je   123
```

Digitální podpis:

Pokud chce mít Alice jistotu, že zprávu X^* skutečně poslal Bob, pak Bob musí za X^* připojit číslo Y^*, které získá takto:

Elektronický podpis

$$Y^* \equiv X^{d_B} \mod n_B.$$

Alice po obdržení spočítá

$$\underbrace{(Y^*)^*}_{=X^*} = (Y^*)^{e_B} \mod n_B$$

Pokud při použití veřejného klíče (e_B, n_B) na dešifrování Y^* dostanu stejnou zprávu jako při dešifrování X^* pomocí mého tajného klíče (d_A, n_A), pak vím, že zprávu odeslal majitel klíče (e_B, n_B).

Ukázkový příklad (viz předchozí):

veřejný klíč příjemce $n_A = 3233$, $e_A = 17$

tajný klíč příjemce $d_A = 2753$

veřejný klíč odesílatele $n_B = 6319$, $e_B = 29$

tajný klíč odesílatele $d_B = 2549$

zpráva $X = 123$

šifrovaná zpráva $X^* = 855$

zprávu $X = 123$ zašifruji znovu, tentokrát s použitím svého tajného klíče:

$$123^{2549} \mod 6319 = 4662$$

Zašifrovaný podpis připojím za šifrovanou zprávu.

Dále příjemci pošlu můj veřejný klíč, aby ho použil pro identifikaci podpisu

$$4662^{29} \mod 6319 = 123.$$

Příjemce po dešifrování obdržel stejnou zprávu 2x.

Podpis mohl poslat pouze držitel tajného klíče k zaslanému veřejnému klíči.

Poznámka: Prakticky se jako digitální podpis neposílá celá zašifrovaná zpráva, ale pouze její tzv. *otisk*. Otisk je zhuštění původní zprávy (takové, že při změně původní zprávy se mění i její otisk) https://cs.wikipedia.org/wiki/Hašovací_funkce).

Příjemce tedy kontroluje shodnost dešifrovaného otisku a otisku vytvořeného z původní nešifrované zprávy.

Poznámka: Pokud by se posílal podpis pro celou zprávu i s veřejným klíče odesílatele, mohl by si každý zprávu dešifrovat a tím by se celá zpráva prozradila.

```
                    Digitalni podpis
-------------------------------------------------------

 Zadana data pro prijemce:
---------------------------
    p_prijemce = 61
    q_prijemce = 53
    e_prijemce = 17

 Zadana data pro odesilatele:
------------------------------
    p_odesilatele = 71
    q_odesilatele = 89
    e_odesilatele = 29


 Spravne zadani pro sifrovani pro prijemce:

  verejny klic prijemce je     n = 3233, e = 17
  tajny klic prijemce je       d = 2753


 Spravne zadani pro sifrovani pro odesilatele:

  verejny klic odesilatele je  n = 6319, e = 29
  tajny klic odesilatele je    d = 2549

  Zadej zpravu  ( 0<x<min(3233,6319) )       x=123
  Sifrovana zprava je     855
  Sifrovany podpis je     4662

  Desifrovana zprava je   123
  Pro desifrovani podpisu pouzij verejny klic odesilatele.
  Desifrovany podpis je   123
```

Teorie matic - řešení SLAR

Celá řada aplikací vede ve své podstatě na problém řešit soustavu lineárních algebraických rovnic (SLAR)

$$\mathbf{A}\mathbf{x} = \mathbf{b},$$

$\mathbf{A}$ ... regulární matice typu N x N (det $\mathbf{A} \neq 0$, $\forall$ vl. č. $\neq 0$, hod$(\mathbf{A}) = N$)

$\mathbf{b}$ ... sloupcový vektor o N složkách

$\mathbf{x}$ ... hledané řešení (sloupcový vektor o N složkách)

1. způsob řešení: **Cramerovo pravidlo**

i-tou složku vektoru řešení vypočteme ze vztahu

$$x_i = \frac{\det \mathbf{A}_i}{\det \mathbf{A}}.$$

$\mathbf{A}_i$ ... vznikne z původní matice tak, že $i-$tý sloupec nahradíme pravou stranou $\mathbf{b}$.

Počet operací:

- musíme vypočítat $N + 1$ determinantů
- při výpočtu determinantu je třeba $N!$ sčítání a v každém sčítanci je N - 1 násobení

Celkem operací:

$$(N + 1) \cdot [(N - 1)N! + N!] = N(N + 1)!$$

2. způsob řešení: **Gaussova eliminační metoda**

- nejprve převedeme na $\triangle$ tvar
- zpětným chodem dosazujeme a počítáme složky řešení

Počet operací:

- v přímém chodu postupně bereme každý řádek o N složkách a jeho násobek přičítáme ke zbývajícím ... N^2
- to opakujeme, abychom vynulovali všechny sloupce pod hlavní diagonálou ... N^3

Celkem operací přesněji

$$\frac{2}{3}N^3$$

3. způsob řešení: **Metoda sdružených gradientů** (1952 M. R. Hesteners, E. Stiefel)

- metoda pro symetrické, pozitivně definitní matice

$$\mathbf{A} = \mathbf{A}^T, \qquad \mathbf{x}^T\mathbf{A}\mathbf{x} > 0 \ \text{ pro } \ \mathbf{x} \neq 0$$

- konverguje k řešení (nalezne řešení) po N krocích

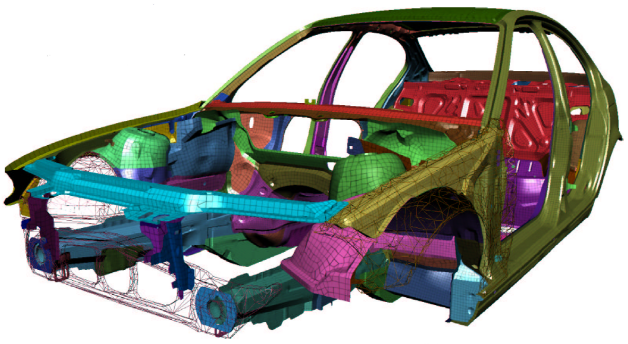
- počet iterací je řádově $2N^3$ (pro plné matice)

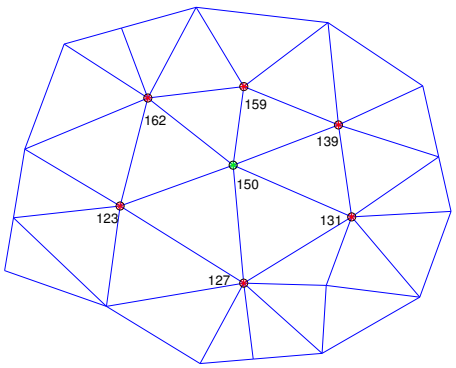
- metoda je odvozena pro řešení ekvivalentního problému:

Věta: Nechť $\mathbf{A}$ je symetrická a pozitivně definitní matice. Pak $\widehat{\mathbf{x}}$ je řešením soustavy $\mathbf{A}\mathbf{x} = \mathbf{b} \ \Leftrightarrow$ minimalizuje funkcionál $J(x) = \frac{1}{2}\mathbf{x}^T\mathbf{A}\mathbf{x} - \mathbf{b}^T\mathbf{x}$ na prostoru $\mathbb{R}^{\mathbb{N}}$.

- při jednotlivých iteracích metody sdružených gradientů se funkcionál J minimalizuje na podprostorech, jejichž dimenze postupně vzrůstá

V úlohách, kde matice $\mathbf{A}$ je plná vychází nejlépe použití Gaussovy eliminační metody. Situace se výrazně změní, pokud bude matice $\mathbf{A}$ řídká. To nastane velmi často, např. při použití metody konečných prvků dostáváme matice např. pro $N = 1000\,000$ neznámých, které jsou ovšem velmi řídké a mají řádově N prvků. Očíslujeme-li vrcholy pak bude mít matice nenulové prvky pouze v pozicích $[i, j]$ takových, že i a j jsou sousední vrcholy (spojeny hranou).





Pokud je matice $\mathbf{A}$ řídká, stačí pro její uložení použít řádově N buněk. V průběhu metody sdružených gradientů se matice $\mathbf{A}$ nemění, zatímco pokud bychom k řešení použili GEM, ztratili bychom vlastnost řídkosti, matice se postupně začne zaplňovat a pro její uložení budeme potřebovat opět řádově N^2 buněk.

V důsledku velké rychlosti konvergence metody sdružených lze ukončit proces dříve než po N krocích. Pro trojrozměrné úlohy vyžaduje GEM řádově $N^{\frac{7}{3}}$ operací, zatímco metoda sdružených gradientů řádově $N^{\frac{4}{3}}$ operací a tzv. metoda sdružených gradientů s předpodmíněním jen $N^{\frac{7}{6}}$ operací.

V tabulce uvedeme příslušné časy pro řešení $\mathbf{Ax} = \mathbf{b}$ různými metodami pro $N = 10^3$ a $N = 10^6$ a rychlosti 10^6 operací za sekundu.

Metoda	Plná matice		Řídká matice	
	$N = 10^3$	$N = 10^6$	$N = 10^3$	$N = 10^6$
Cramerovo pravidlo	$4 \cdot 10^{2567}$s	$(\star)$		
GEM	667 s	21125 let	10 s	3,17 roku
Sdružené gradienty			0,01 s	100 s
Předpodmíněné sdružené gradienty			0,0032 s	10 s

Pozn.: Rok má 60 x 60 x 24 x 365,25 = 3,15576 x 10^7 sekund.

$(\star)$ $1000000! \approx 8{,}2639 \cdot 10^{5565708}$ $\qquad \dfrac{N(N+1)!}{10^6} = (N+1)! \ldots$ pro $N = 10^6$

$$\frac{1000001 \cdot 1000000!}{3,15576 \cdot 10^7} = \frac{8,2639 \cdot 10^{5565708}}{31,5576} = 2,619 \cdot 10^{5565707} \text{ let.}$$