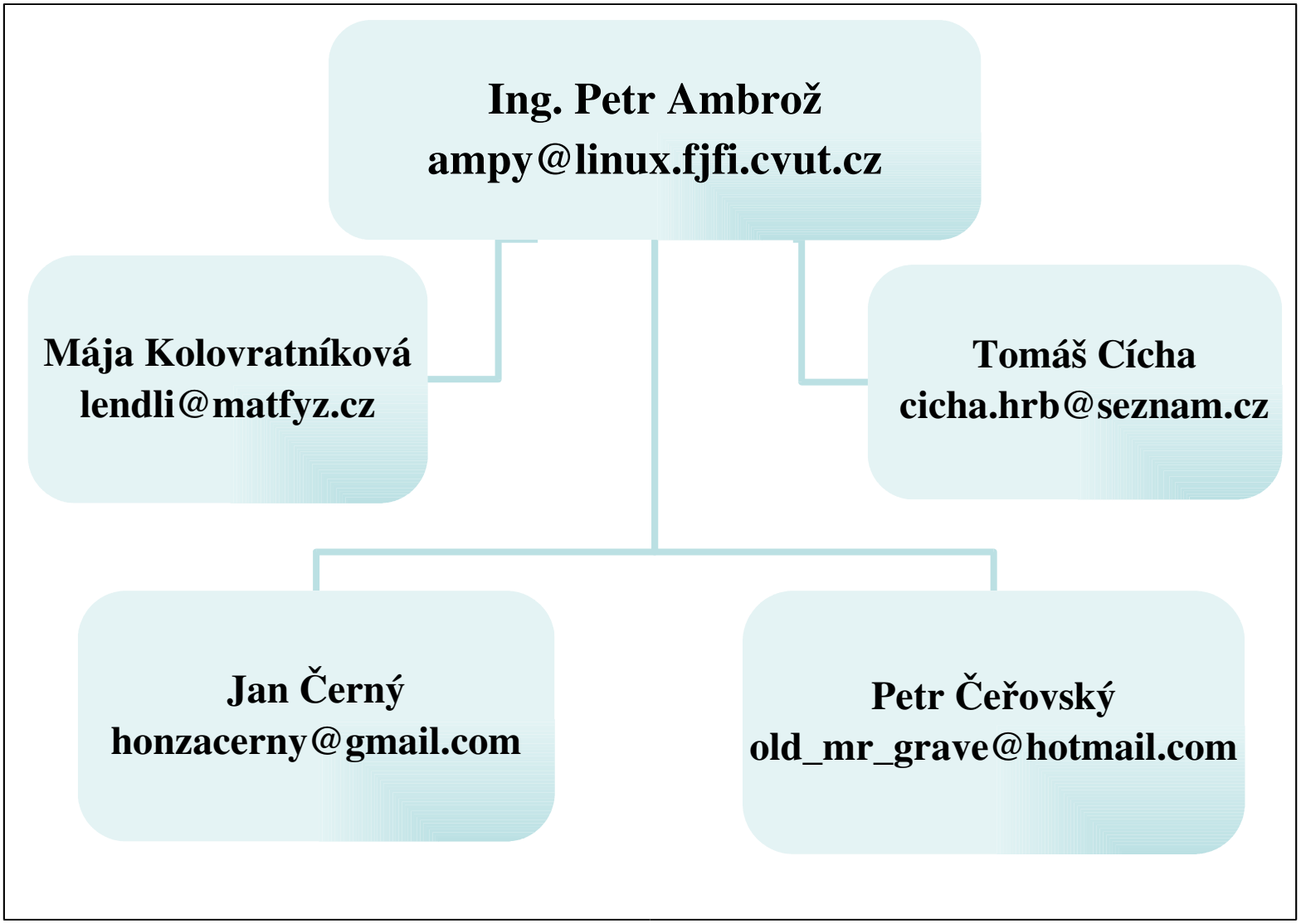
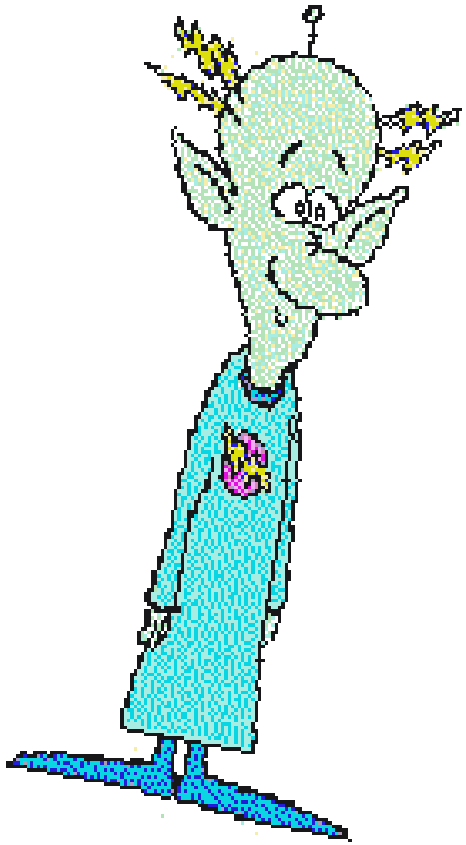
Teorie čísel a šifrování



O čem si povíme

- Co je to kryptologie
- Symetrická kryptografie
- Asymetrická kryptografie
- Šifrovací algoritmy
- Naše programy
- Shrnutí
- Poděkování



Kryptologie

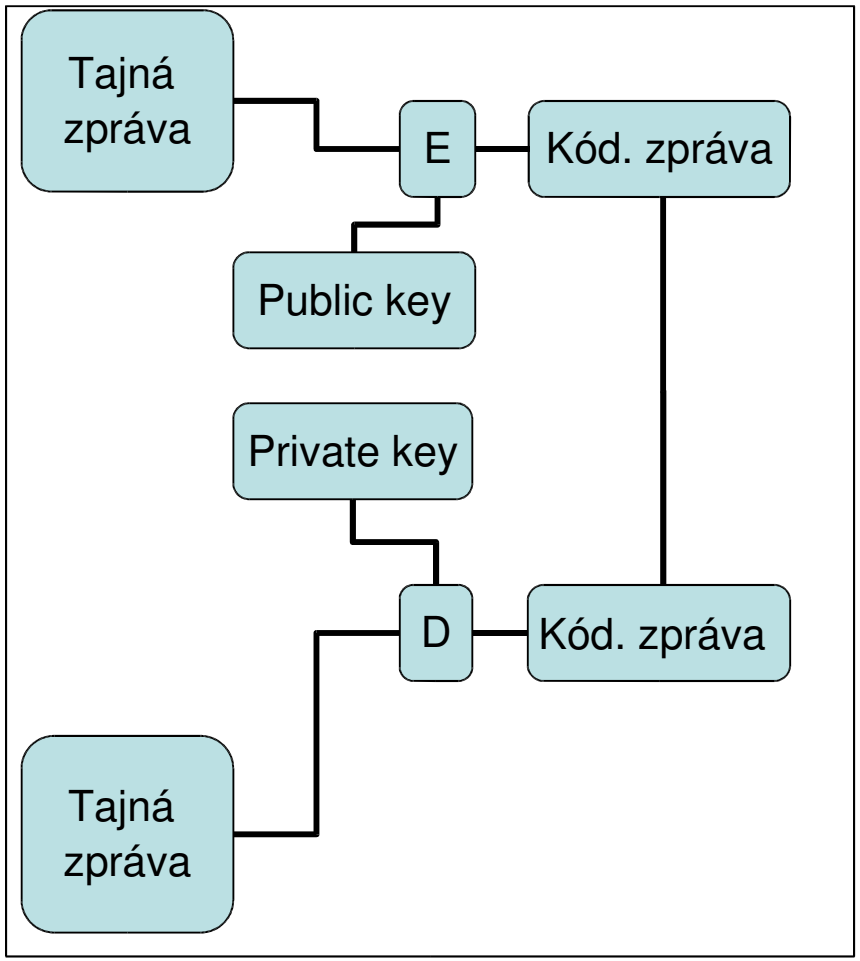
- **Kryptologie** je věda zabývající se šiframi
- **Kryptografie** je část kryptologie, která se zabývá převedením srozumitelné zprávy do nesrozumitelné a zpět
- **Kryptoanalýza** je část kryptologie zabývající se odhalením klíče pro dekódování zašifrované zprávy.

Symetrická kryptografie

Šifrování, které využívá k šifrování i dešifrování jednoho klíče, zadaného uživatelem.

Čím delší klíč je, tím hůře je šifra pro hackera rozluštitelná

Asymetrická kryptografie



- Šifrování které využívá public a private key
- Public key pouze pro zašifrování
- Private key pouze pro dešifrování

M&J's encryption program

- Šifrování s jedním klíčem
- Posun znaků o proměnou hodnotu
- Obtížnost rozluštění roste s délkou klíče

Maticové šifrování

Tam

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} x' \\ y' \end{pmatrix}$$

Zpět

$$D^{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix}=\begin{pmatrix} x \\ y \end{pmatrix}$$

$$D=ad-bc$$

x, y – původní znaky

x’, y’ – zašifrované znaky

Použijeme inverzní matici

Shrnutí

- Využití šifrování
- Současný stav
- Výhled do budoucna

Poděkování

- Děkujeme FJFI ČVUT v Praze
- Panu Ing. Vojtěchu Svobodovi, Csc.
- Panu Ing. Petru Ambrožovi
- Sponzorům
- Všem organizátorům, zvláště pak přednášejícím profesorům
- Rootovi na PC v uč.115 za usnadnění naší práce :o)

Náš tým