Šifrování pro úplné začátečníky

Ing. František Kučera

OpenAlt.cz

1. 11. 2014

Osnova prezentace

1. Symetrické a asymetrické šifrování
2. E-mail a bezpečnost
3. Nástroje a praxe

Symetrické šifrování

- jeden klíč
- šifrování (originál + klíč) $\rightarrow$ šifrovaný text
- dešifrování (šifrovaný text + klíč) $\rightarrow$ originál
- Příklady: AES, Camellia, DES, Blowfish

Caesarova šifra

- jednoduchá substituční šifra
- posun abecedy
- snadno prolomitelná

Vernamova šifra

- neprolomitelná
- dokonale náhodný klíč
- stejně dlouhý jako šifrovaná data

Asymetrické šifrování

- pár klíčů: soukromý a veřejný
- šifrování (originál + veřejný klíč) $\rightarrow$ šifrovaný text
- dešifrování (šifrovaný text + soukromý klíč) $\rightarrow$ originál
- podpis
- Příklady: RSA, ElGamal

Steganografie

- skrývání informace
- použití v kombinaci s kryptografií

Trocha historie, proč šifrovat

- první e-mail: 1971
- důvěra, počátky sítí
- bezpečnost?

Protokol SMTP – ukázka

```
220 example.com ESMTP Postfix
EHLO openalt.cz
250 Hello openalt.cz
MAIL FROM: <jakykoli.odesilatel@kdokoli.cz>
250 Ok
RCPT TO: <nejaky.prijemce@example.com>
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: predmet zpravy
From: <jakykoli.odesilatel@kdokoli.cz>
To: <nejaky.prijemce@example.com>
...
```

Protokol SMTP – ukázka

```
...
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: predmet zpravy
From: <jakykoli.odesilatel@kdokoli.cz>
To: <nejaky.prijemce@example.com>

Ahoj, tohle je rucne poslany e-mail. Franta
.
250 Ok: queued as 2A4B2C6F3D
QUIT
221 Bye
```

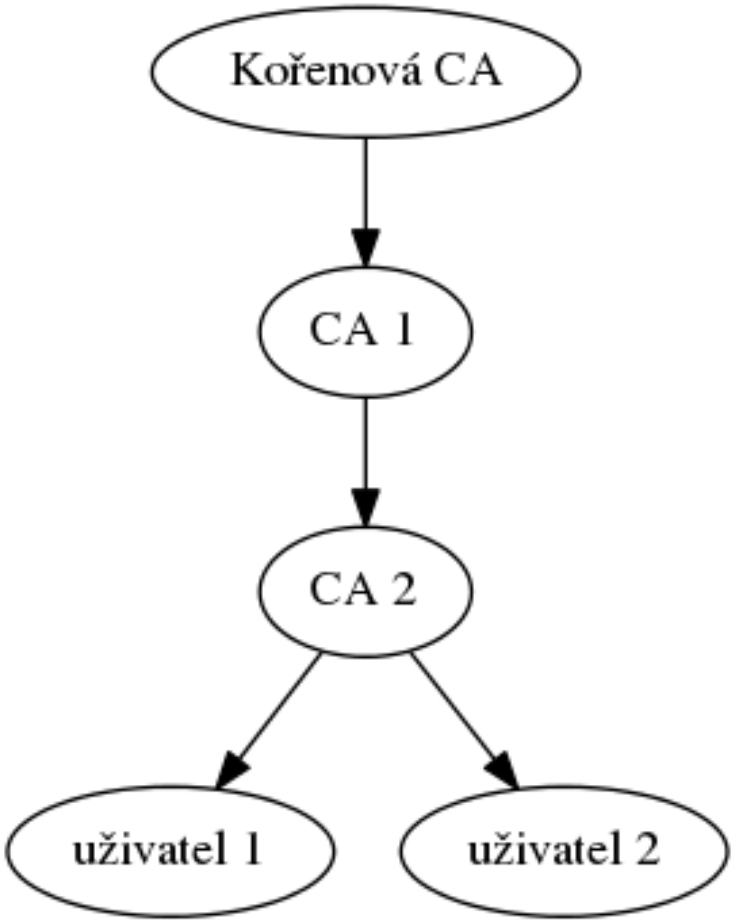
Protokol SMTP – vlastnosti

- v základu žádné šifrování
- ani ověřování identity
- spam – SPF, DKIM, ADSP

technologie pro šifrování a podepisování

- X.509 – hierarchie CA
- OpenPGP/GnuPG – pavučina důvěry – Web of trust

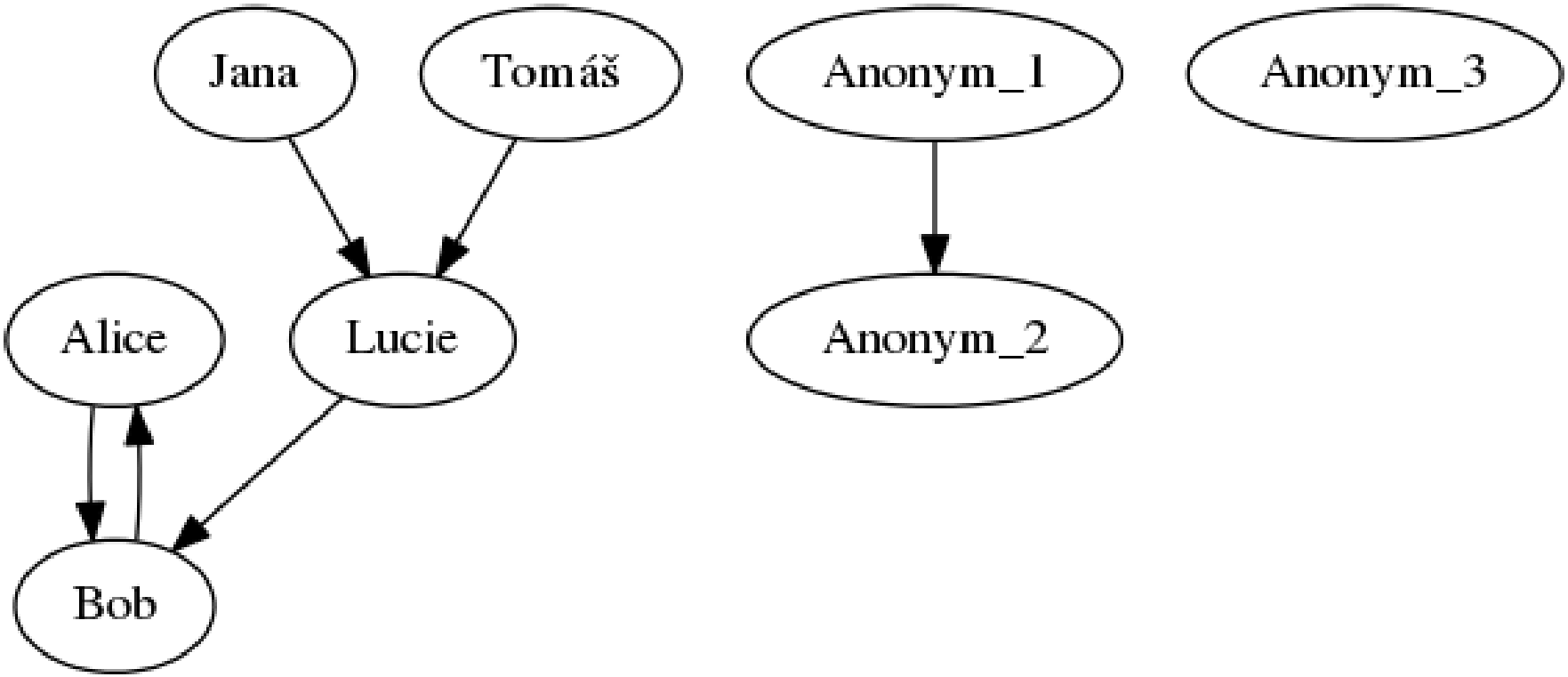
Hierarchie CA



CA – postup

- distribuce certifikátů CA
- vytoření páru klíčů resp. získání certifikátu
- distribuce veřejného klíče
- používání (šifrování, podepisování)

Pavučina důvěry



Pavučina důvěry – postup

- vytoření páru klíčů
- distribuce veřejného klíče
- získání důvěry
- používání (šifrování, podepisování)

Nástroje

- CLI: gpg, gpgsm, openssl, gnutls
- GUI: Kleopatra (KDE), Seahorse (Gnome)
- E-Mail: KMail, Thunderbird+Enigmail
- Dolphin: integrace s Kleopatrou

OpenPGP / GnuPG

```
gpg --gen-key
gpg --fingerprint
gpg --import franta.pkr.asc
gpg --list-keys / --list-secret-keys
gpg --encrypt --armor
gpg --encrypt soubor.txt
gpg soubor.txt.gpg
gpg --send-keys / --recv-keys
```

Prostor pro diskusi

Kontakt a licence

- Autor: Ing. František Kučera
  `https://frantovo.cz/`
  `http://www.abclinuxu.cz/clanky/bezpecnost/bezplatne-ca-nebojte-se-sifrovat-s-s-mime`
- Licence: Creative Commons BY-ND 3.0
  `https://creativecommons.org/licenses/by-nd/3.0/`
  Toto dílo lze použít pro komerční i nekomerční účely, uveďte autora, nezasahujte do díla.