

# GnuPG pro normální lidi

Katarína 'Bubli' Macháková

# Osnova přednášky

- Co je to GnuPG a k čemu slouží ?
- Proč podepisovat a šifrovat poštu ?
- Jak funguje elektronický podpis a šifrování ?
- Jak si vytvořit vlastní dvojici klíčů ?
- Co s cizím veřejným klíčem ? Jak ověřit jeho důvěryhodnost ?
- Jak zprovoznit podporu pro GnuPG v KMailu ?

# Co je GnuPG a k čemu slouží ?

- Free software uvolněn pod GNU GPL
- Náhrada komerčního PGP, nepoužívá patentované algoritmy
- Soubor nástrojů pro elektronické podepisování a šifrování dokumentů (nejčastěji elektronické pošty)
- A také pro správu privátních a veřejných klíčů
- Podpora pro GnuPG v řadě mailových klientů jako zásuvný modul (plug-in)

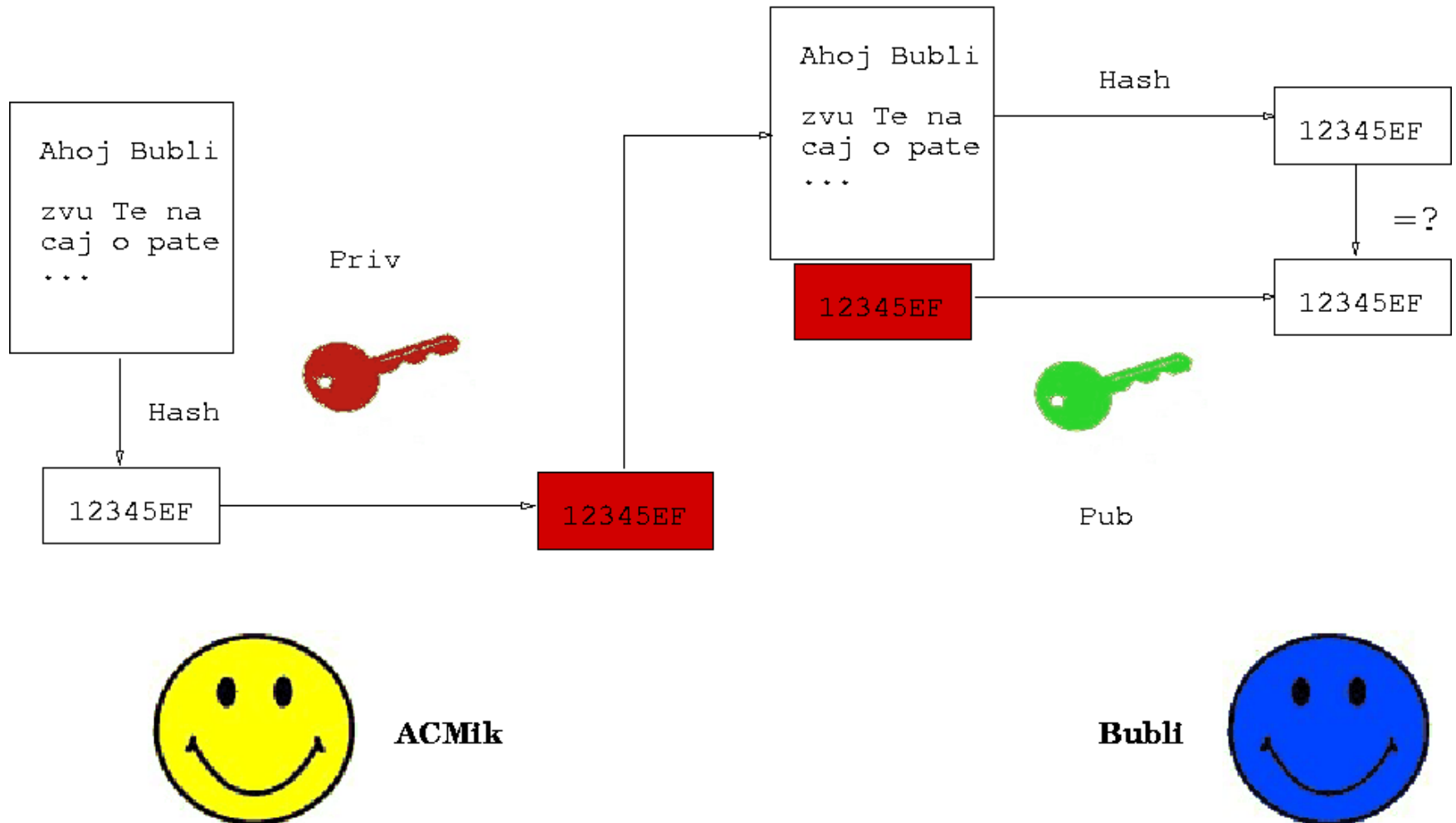
# Podepisování a šifrování pošty

- Proč podepisovat ?
  - ověření autentičnosti (autorství e-mailu nelze zpochybnit)
  - ověření integrity (e-mail nebyl cestou od odesílatele k adresátovi změněn)
- Proč šifrovat ?
  - utajení obsahu zprávy pro kohokoliv, kromě adresáta

# Jak funguje elektronický podpis ?

- Uživatel A vypočítá pomocí **hashovací funkce** z textu zprávy **kontrolní součet**
- Zašifruje ho svým **privátním klíčem** a odešle e-mailem jako podpis
- Uživatel B rozšifruje podpis **veřejným klíčem** uživatele A (ověření autentičnosti) -> získá kontrolní součet odeslané zprávy
- Vypočítá kontrolní součet přijaté zprávy a obě hodnoty porovná (ověření integrity)

# Jak funguje elektronický podpis ?



## Jak funguje šifrování ?

- Uživatel B zašifruje zprávu **jednorázovým klíčem** (session key) s použitím **symetrické šifry**
- Tento klíč zašifruje **veřejným klíčem** uživatele A a odešle spolu se zprávou
- Uživatel A svým **privátním klíčem** rozšifruje session key...
- ... a ten použije k rozšifrování celé zprávy

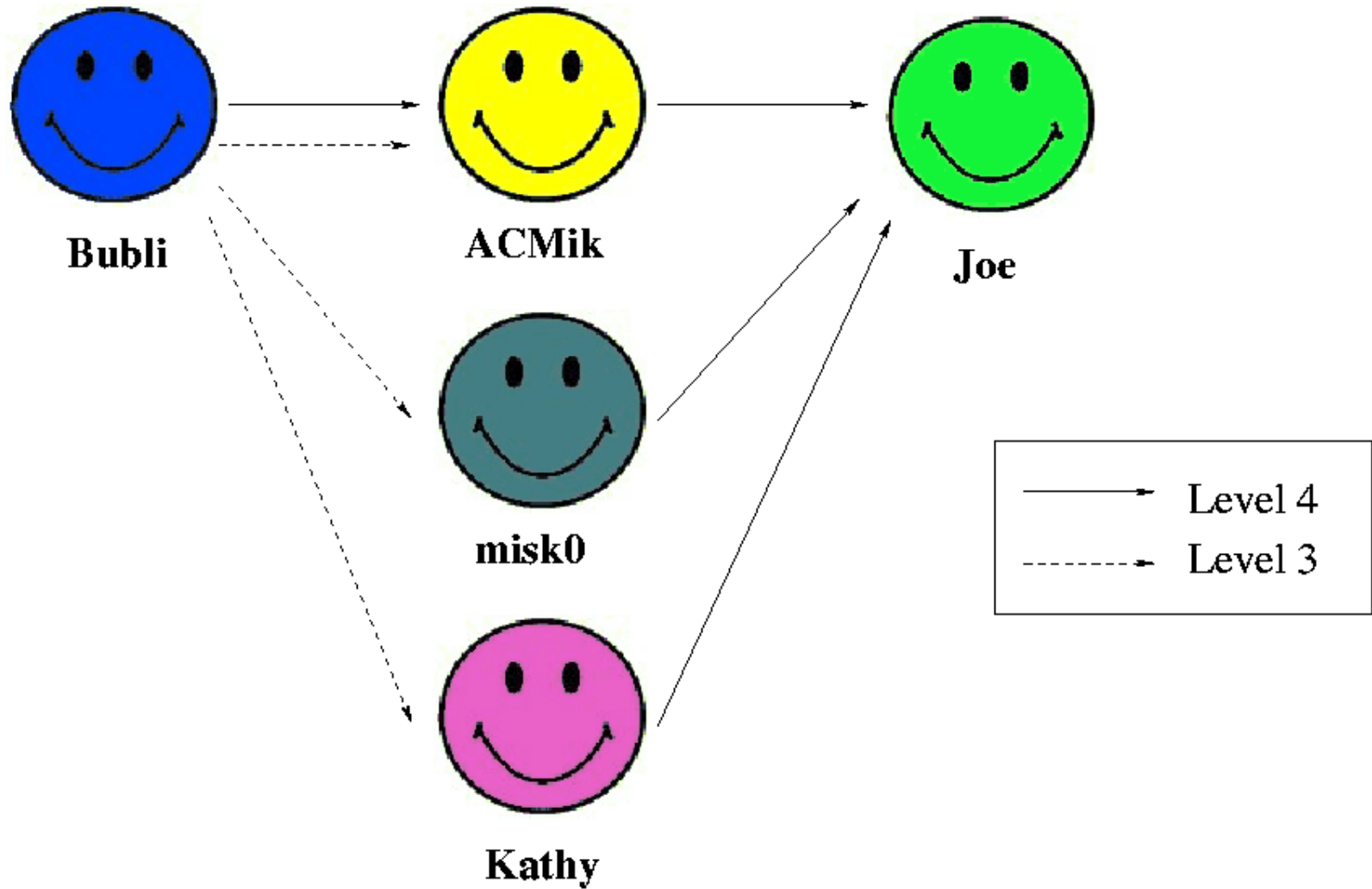
# Začínáme: generujeme dvojici klíčů

- Výběr algoritmu pro podepisování a šifrování (DSA a ElGamal) a délky klíče
- Přidání osobních údajů (jméno + e-mailová adresa)
- Zvolení BEZPEČNĚHO hesla na ochranu privátního klíče
- Nastavení platnosti klíče
- Všechny údaje lze později měnit

# Co s cizím veřejným klíčem ?

- Import do databáze klíčů
- DŮKLADNÉ ověření vlastnictví klíče (pomocí fingerprintu)
- **Problém:** Nemožnost ověřit fingerprint jinou cestou osobně
- **Řešení:** Sít' důvěry

# Sít' důvěry



# KMail a GnuPG

- KMail je grafický mail klient pro desktopové prostředí KDE
- Od verze 1.7 je podpora pro GnuPG pevnou součástí aplikace
- Některá další rozšíření (**gpg-agent** – aplikace, která si určitou dobu “pamatuje” heslo k privátnímu klíči, **pinentry** – GUI aplikace pro vložení hesla) je nutno doinstalovat

## Co potřebujeme ?

- libgpgme
- pinentry
- libksba
- GnuPG  $\geq$  1.9.10 nebo GnuPG  $\geq$  1.2.0 + newpg
- hlavičkové soubory (jen pokud překládáme GnuPG ze zdrojových textů)
- konfigurace viz. praktická ukázka

## Další možnosti ?

- Grafické rozhraní ke GnuPG
  - Seahorse
  - KGpg
- Mail klienty s podporou GnuPG
  - Mozilla Thunderbird + Enigmail
  - Ximian Evolution
  - Mutt
  - a další...

# Užitečné čtivo

- <http://www.gnupg.org/>
- <http://kmail.kde.org/kmail-pgpmime-howto.html>
- Steven Levy: *Crypto*, Penguin books, New York, 2001

# Otázky ?

„...ptejte se mně na co chcete, já vám na co chci  
odpovím.“

© kpt. Ing Jiří Dastych