

TOR MEETUP #2



Osobní komunikace

- Jak ví Alice, že mluví s Bobem a ne Evou?
 - Bob je nenapodobitelný.
- Umí Alice zajistit, aby komunikace byla důvěrná?
 - Nikdo nás neslyší, Eva je vedle a stejně nám nemůže nerozumět.
- Má Alice jistotu, že slyší to, co Bob vyslovil?
 - Bobova slova nemohl nikdo změnit.

V osobní komunikaci funguje intuice, bezpečnost je levná.



Vzdálená komunikace

- Jak ví Alice, že mluví s Bobem a neEvou?
 - napodobení partnera > podvržení poznávacích znaků
- Umí Alice zajistit, aby komunikace byla důvěrná?
 - zachycení komunikace > odposlouchávání
 - porozumění komunikaci > rozluštění užité řeči
- Má Alice jistotu, že slyší to, co Bob vyslovil?
 - změna vysloveného > narušení integrity komunikačního kanálu

Tady intuice nefunguje (občanské průkazy, přístupová hesla, střežené komunikační kanály, neveřejné šifrování). Bezpečnost je drahá.



Kryptografie

- věda na rozhraní matematiky a počítačové vědy
- vytváří možnost důvěrné a zabezpečené komunikace
- klade minimální předpoklady na integritu komunikačních kanálů
- kombinuje základní kameny, pomocí kterých staví zložitější koncepty
- tyto koncepty se snaží naplnit cíle třeba jako:
 - identifikace - ověřování totožnosti
 - autenticita - prokazování původu dat
 - důvěrnost - utajení komunikace a dat
 - integrita - prokazování neporušenosti dat



Hašovací funkce

- některé kryptooperace jsou pomalé nebo neuskutečnitelné na velkých datech
- chceme pro jakákoliv vstupní data vygenerovat “otisk” pevné délky
- dále pracujeme jenom s “otiskem” → rychlejší
- naivní přístup:
 - přiřadíme každému znaku zprávy poradové číslo písmene
 - sečteme čísla a výsledek použijeme jako otisk zprávy
 - neúčinné: TADEAS = ZINA, 520000 = 250000



Hašovací funkce

SHA-2 (SHA224, SHA256, SHA384, SHA512)

sha256("") =

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

sha256("The quick brown fox jumps over the lazy dog") =

d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592

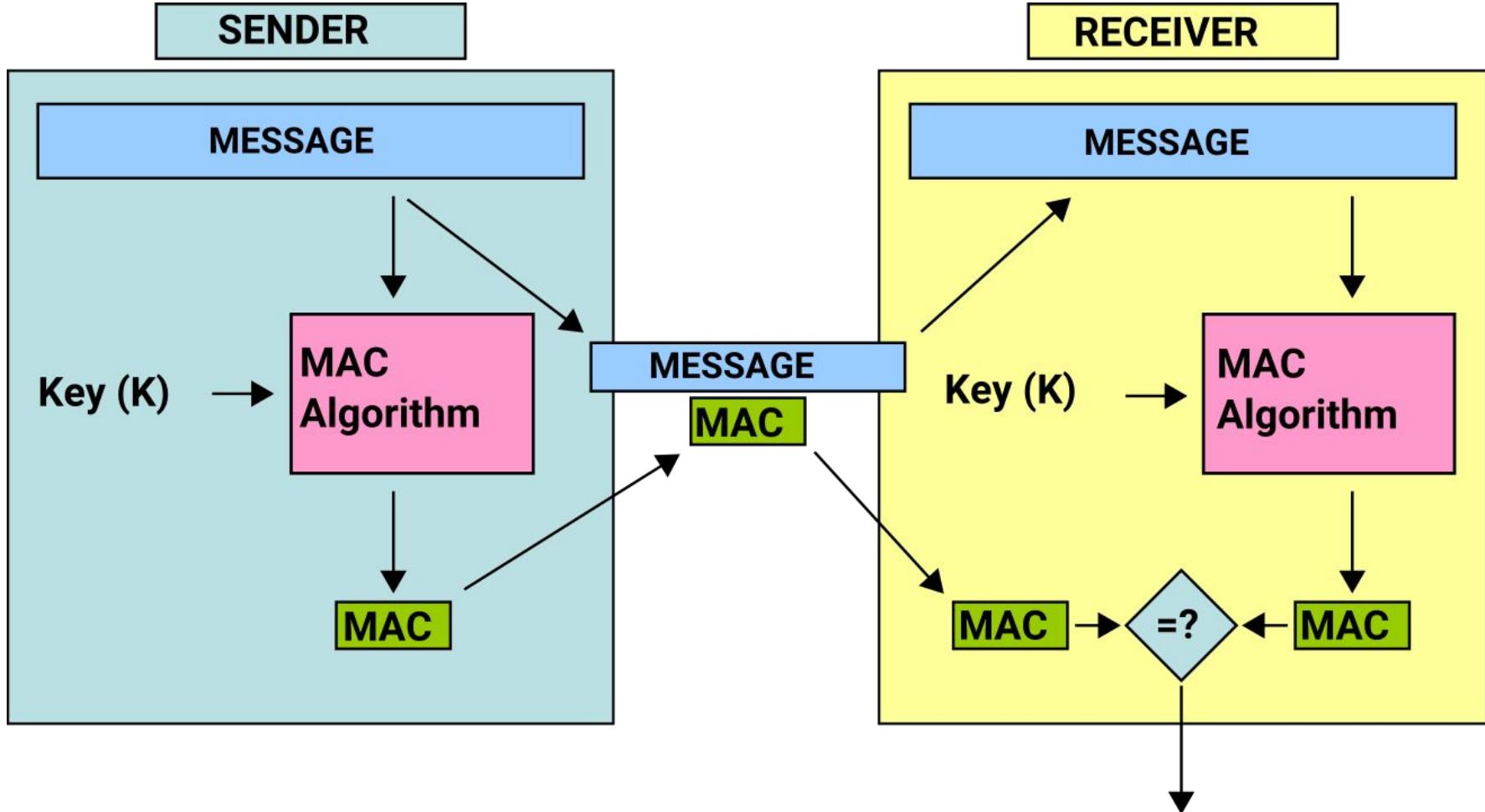
sha256("The quick brown fox jumps over the lazy dog.") =

ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c

sha256("00000.....00000") =

d29751f2649b32ff572b5e0a9f541ea660a50f94ff0beedfb0b692b924cc8025

MAC (message authentication code)





Symetrická kryptografie

Caesarova šifra

$n = 3$

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

PARALELNI POLIS → SDUDOHQL SROLV

$n = 13$

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

PARALELNI POLIS → CNENYRYAV CBYVF



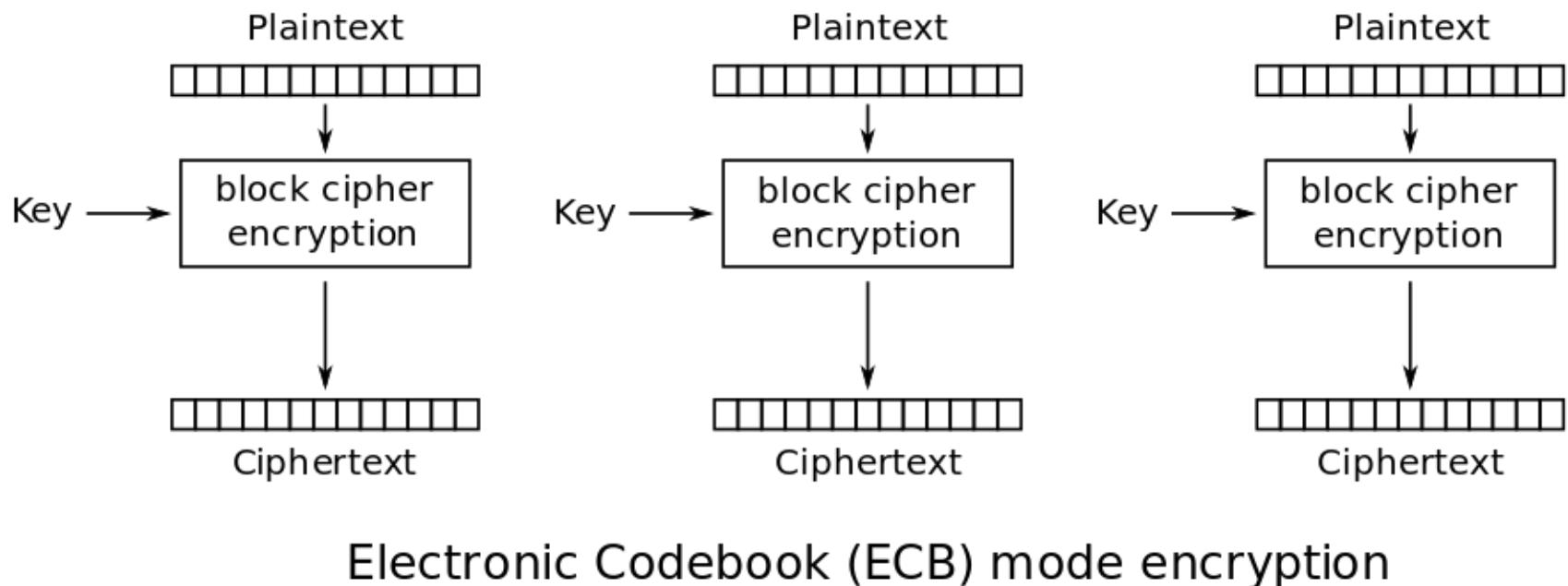
Symetrická kryptografie

AES

- podpora přímo v hardwaru (akcelerátory, později přímo procesory)
- velikost bloku 128 bitů
- velikost klíče 128 nebo 192 nebo 256 bitů
 - klíč může být slovo nebo věta, použijeme hašovací funkci
 - (ještě lepší je použít KDF - key derivation function)
- použití:
 - Šifrování disku
 - Šifrování komunikace
 - prakticky všude, kde nám jde o rychlosť

Symetrická kryptografie

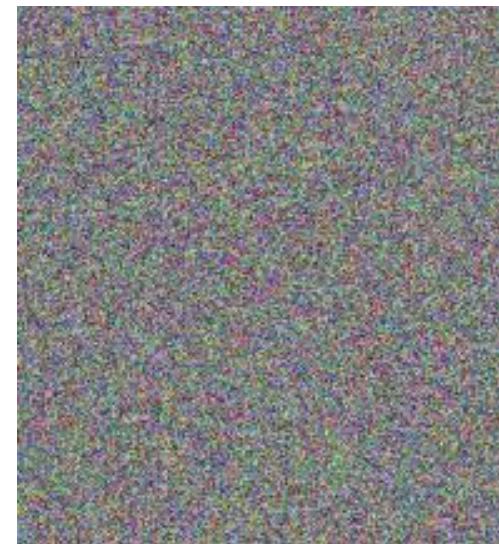
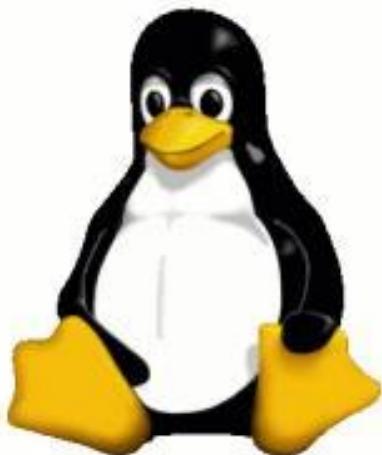
ECB





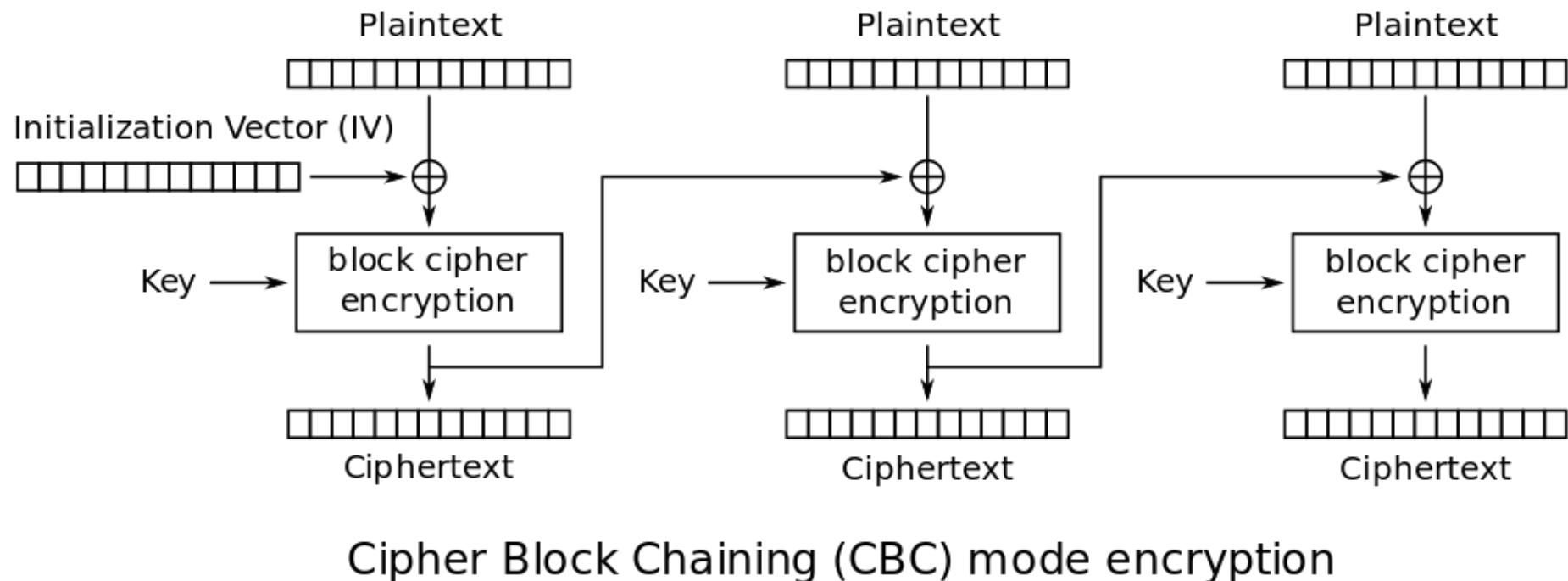
Symetrická kryptografie

Bloková šifra



Symetrická kryptografie

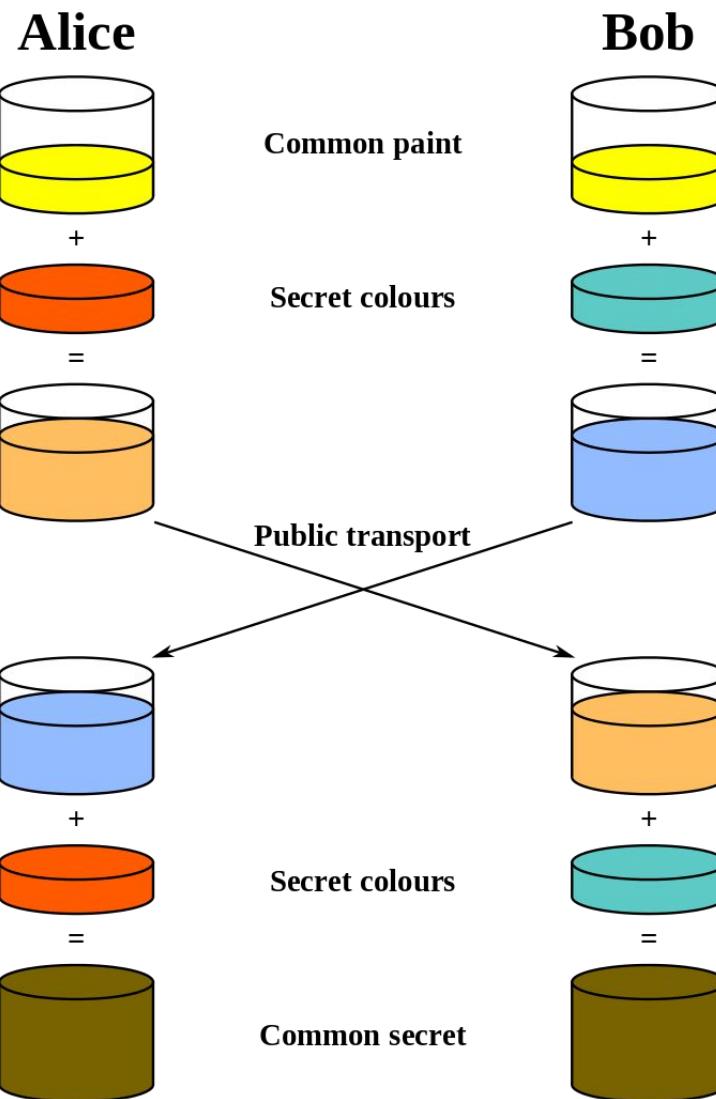
CBC





Diffie–Hellman

Výměna klíčů





Diffie–Hellman

Výměna klíčů

- problémem je man-in-the-middle útok
- Eva se pro Alici může tvářit jako Bob, pro Boba jako Alice
- Eva dešifruje zprávu a zašifruje svým klíčem
- Eva musí být přítomná při každé komunikaci Alice a Boba, jinak se prozradí
- chybějící autentizace se řeší asymetrickou kryptografií (SSH) nebo jinak (Z RTP - hash posílaných hodnot)



Jednosměrná funkce (trapdoor)

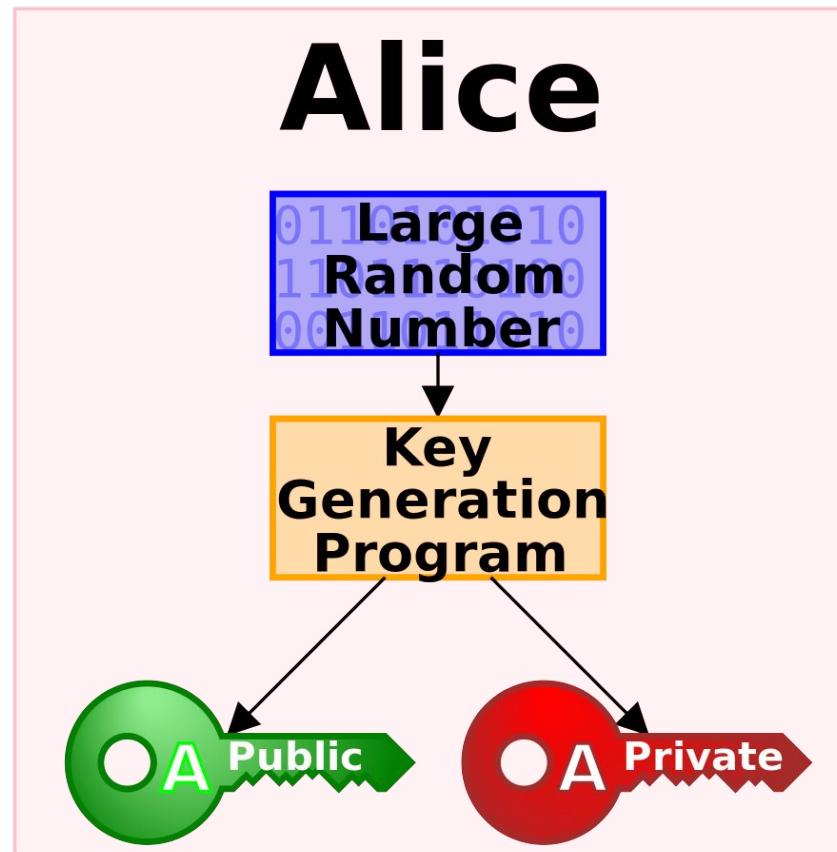
- míchání barev
- násobení (prvo)čísel (RSA)
 - $n = p \times q$
- diskrétní logaritmus (DH, DSA, ElGamal)
 - $g^x \text{ mod } p = y$
- eliptické křivky (ECDH, ECDSA, ECIES)
 - $K = k \times G$



Asymetrická kryptografie

Klíče

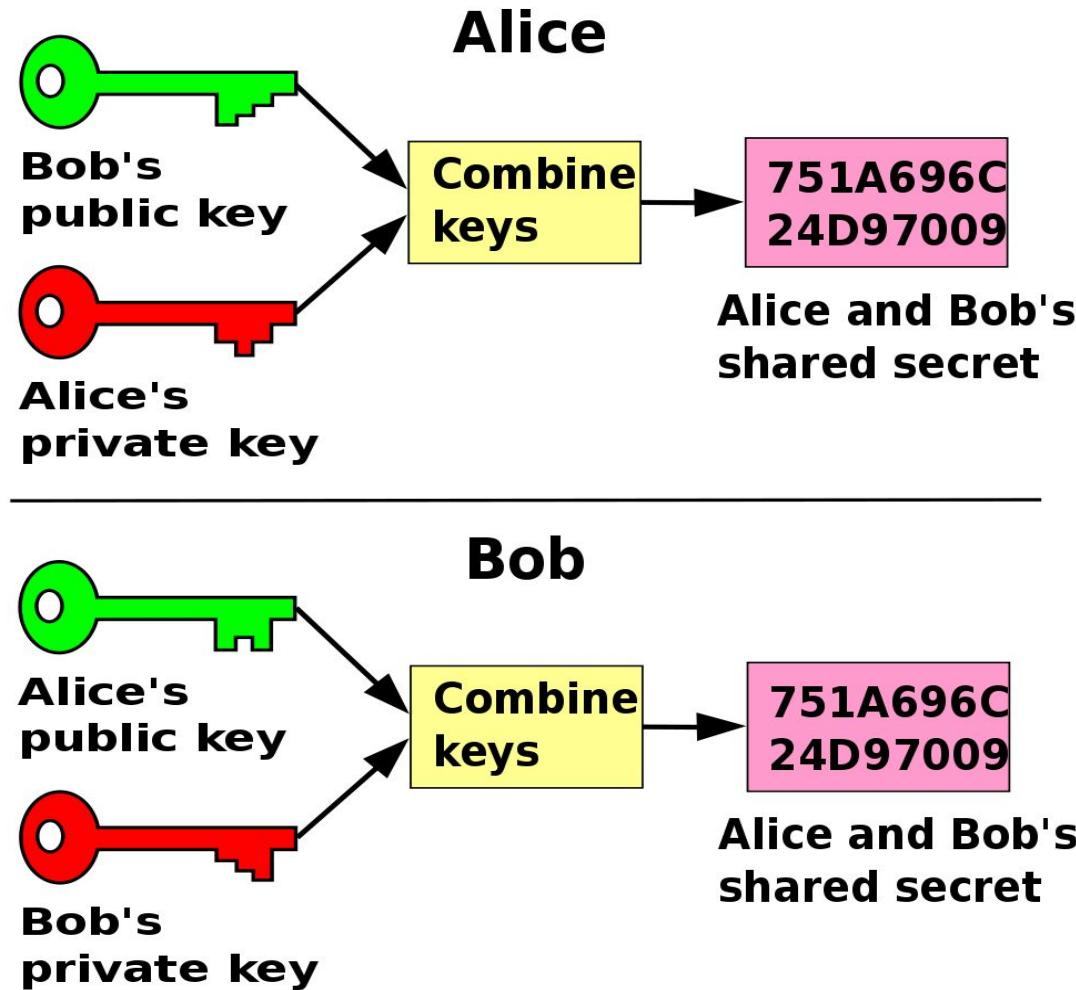
- používáme dvojici klíčů: veřejný a privátní klíč





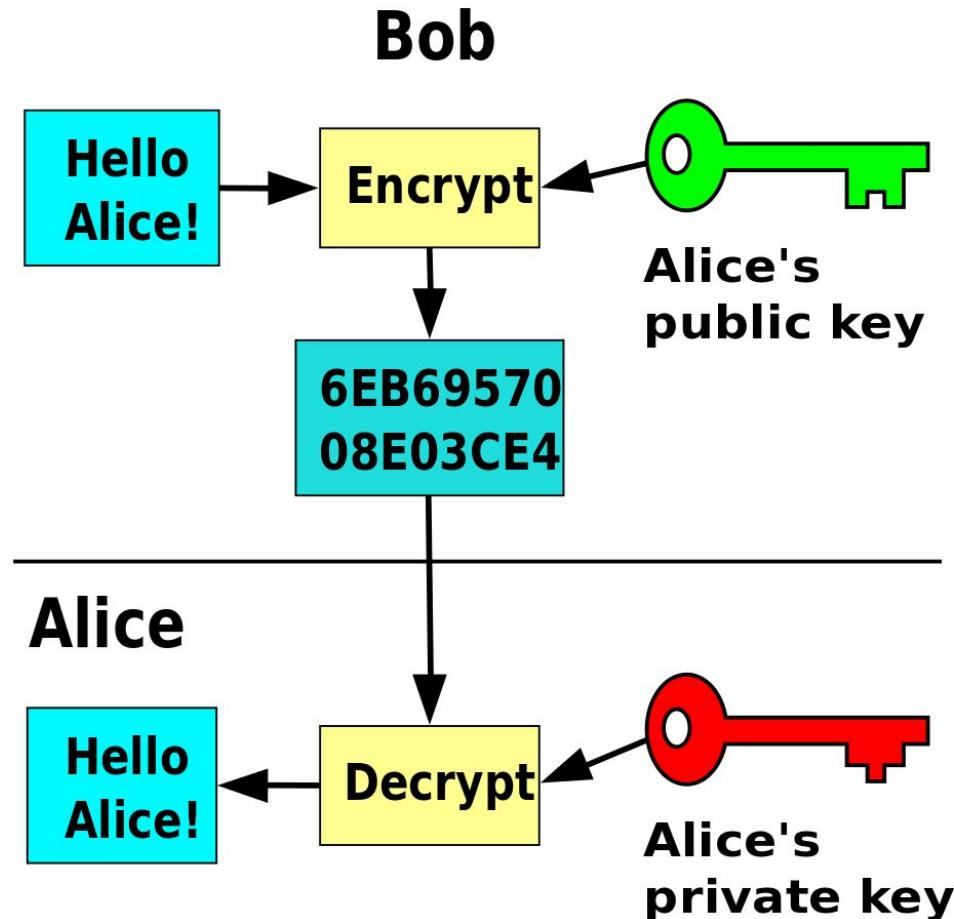
Asymetrická kryptografie

Sdílené tajemství



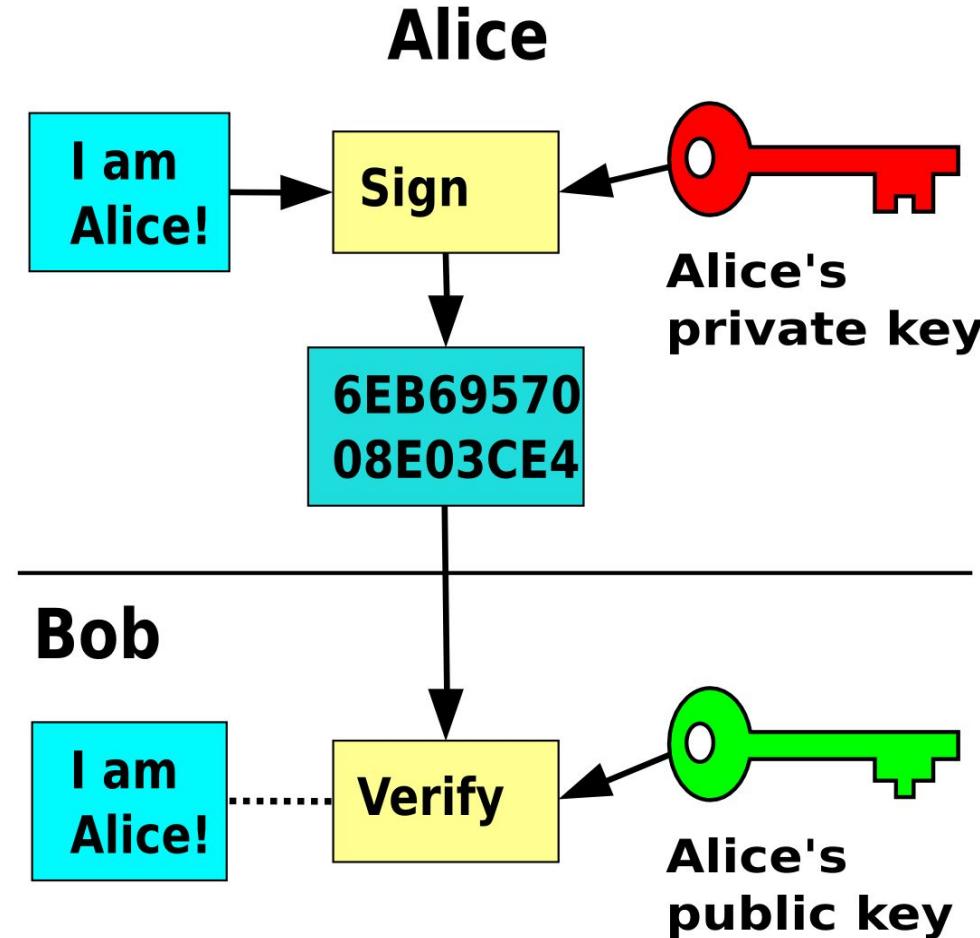
Asymetrická kryptografie

Šifrování veřejným klíčem



Asymetrická kryptografie

Digitální podpis





RSA

- $(m^e)^d \equiv m \pmod{n}$
- $(m^d)^e \equiv m \pmod{n}$
- i při znalosti hodnot m, n, e je těžké najít d



Eliptické křivky

- $y^2 = x^3 + ax + b$

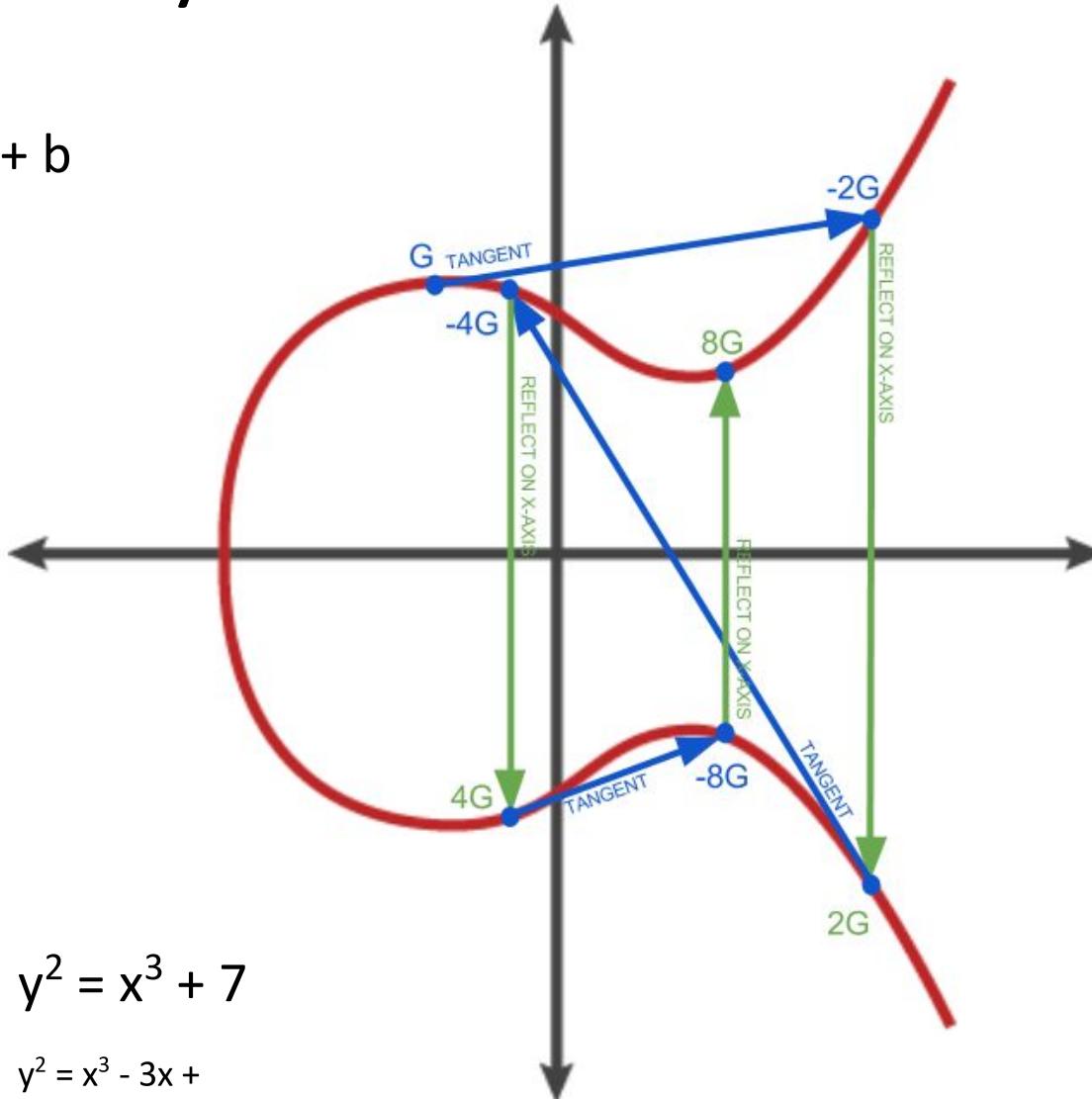
- $k = 8$

- $K = 8G$

- secp256k1 $y^2 = x^3 + 7$

- NIST P-256 $y^2 = x^3 - 3x +$

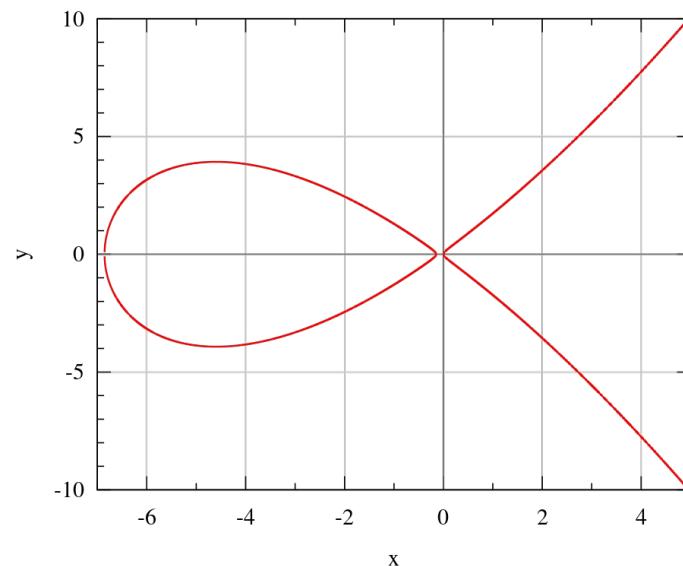
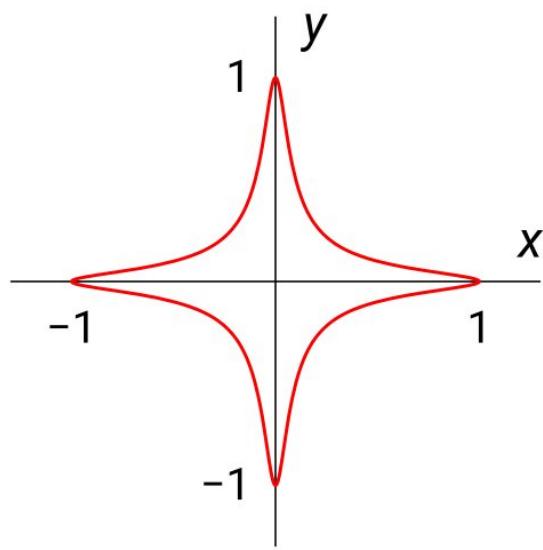
41058363725152142129326129780047268409114441015993725554835256314039467401291





Eliptické křivky

- Edwards
- $x^2 + y^2 = 1 + dx^2y^2$
- Ed25519
 - $-x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2$
- Montgomery
- $by^2 = x^3 + ax^2 + x$
- Curve25519
 - $y^2 = x^3 + 486662x^2 + x$





Prostředky elektronické komunikace

- e-mail
- instant messengery
- audio
- video



Elektronická komunikace

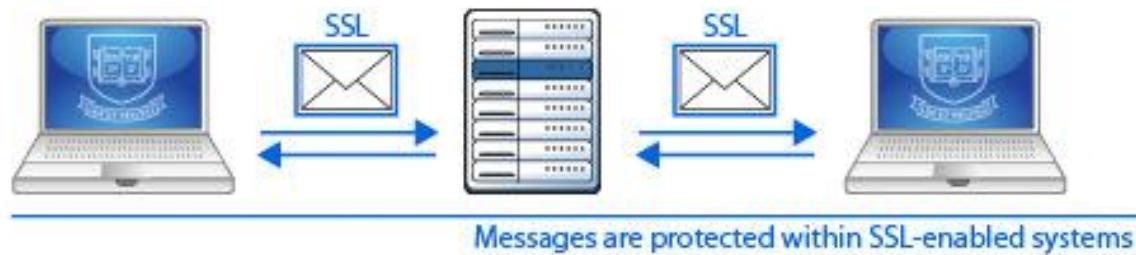
e-mail - šifrování

- E-mail
 - Většina lidí nešifruje, protože “nemá důvod”
 - Každý má důvod (zneužití v budoucnu)
 - Šifrované spojení při připojení k mail serveru (IMAPS, POP3S, SMTPS) není šifrování mailu
 - Chráníme autentizační údaje, tot' vše (MITM risk)
 - Bráníme třetí straně číst náš mail?



Elektronická komunikace

e-mail - šifrování





Elektronická komunikace

e-mail - šifrování

- ~~Ochrana přenášených dat~~



Elektronická komunikace

e-mail - šifrování

- ~~Ochrana přenášených dat~~
- Máme jistotu, že odesílatel je ten za koho se vydává?



Elektronická komunikace

e-mail - šifrování

- ~~Ochrana přenášených dat~~
- ~~Máme jistotu, že odesílatel je ten za koho se vydává?~~



Elektronická komunikace

e-mail - šifrování

- ~~Ochrana přenášených dat~~
- ~~Máme jistotu, že odesílatel je ten za koho se vydává?~~
- Nebyla data během doručování pozměněna?



Elektronická komunikace

e-mail - šifrování

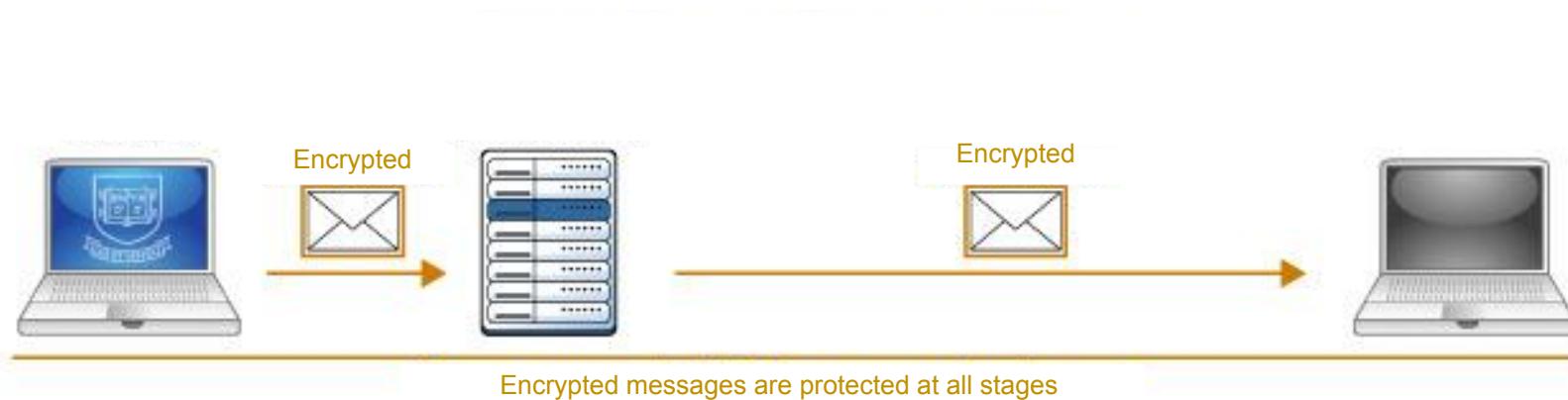
- ~~Ochrana přenášených dat~~
- ~~Máme jistotu, že odesílatel je ten za koho se vydává?~~
- ~~Nebyla data během doručování pozměněna?~~



Elektronická komunikace

e-mail - šifrování

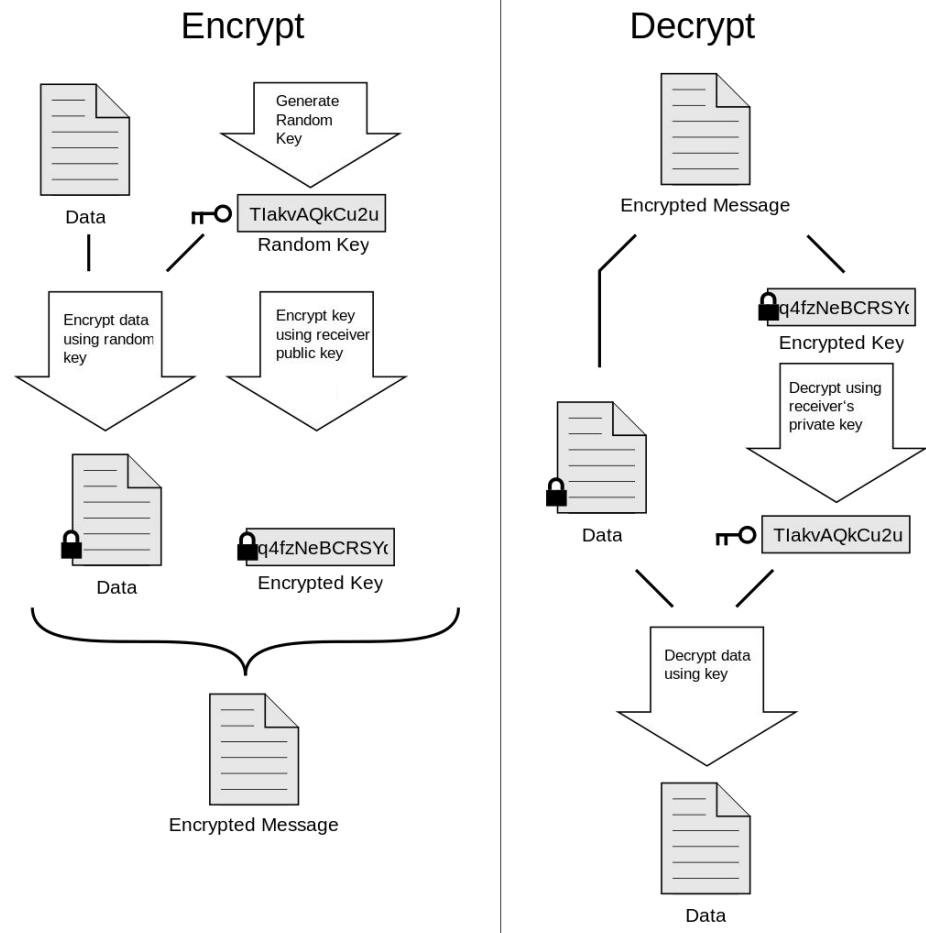
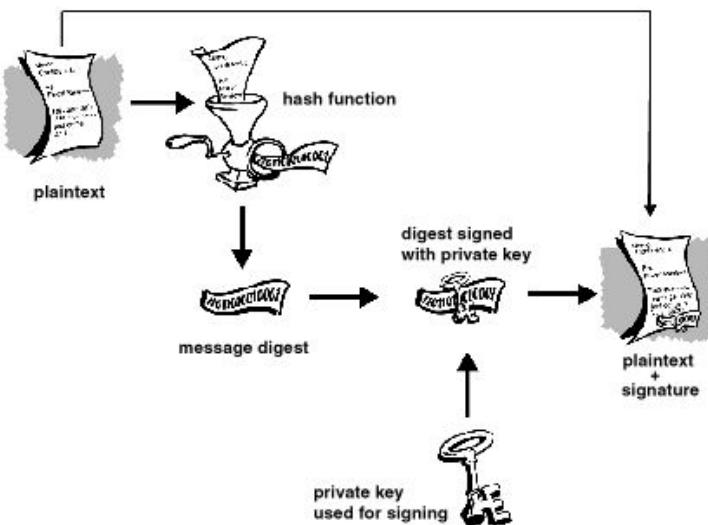
šifrování a podepisování mailů
S/MIME, OpenPGP



Elektronická komunikace

e-mail - šifrování

- Kombinace symetrické a asymetrické kryptografie (výkon)
- Vygeneruji klíče pro asymetrickou kryptografii (privátní, veřejný)
- Klíč se skládá z master key a subkey
- Master key složí k podepisování zprávy (u pgp subkeys), subkey šifruje/dešifruje session key (DSA/EIGamal)





Elektronická komunikace

e-mail - šifrování

- S/MIME (Secure/Multi-purpose Internet Mail Extensions)
 - Standard pro šifrování a podepisování věřejným klíčem
 - Založeno na CMS (Cryptographic Message Syntax) - standard pro kryptografickou ochranu zpráv, který vychází ze standardu PKCS #7
 - Implementováno téměř ve všech MUA => snadné použití
 - Privátní klíč, cert. Request -> CA -> X.509 v3 certifikát (veřejný klíč, os. údaje (jméno, mail, ...); podepsáno CA)
 - Certifikační Autorita
 - lokální - problém s ověřováním mimo organizaci
 - globální
 - Vydání a obnova certifikátu za poplatek (vyjimky, např. StartSSL/StartCOM, Comodo,...)
 - Musím mít v klientovi její certifikát, kterým ověřím validitu podpisu na uživatelského certifikátu



Elektronická komunikace

e-mail - šifrování

- Veřejný klíč (certifikát) součástí podpisu -> nepotřebuji kontaktovat odesílatele, abych ho získal
- S/MIME 3.2 - RSA + SHA256 pro podpis, RSA pro session key, AES



Elektronická komunikace

e-mail - šifrování

Zašifrovaná (+ podepsaná) zpráva:

```
MIME-Version: 1.0
Content-Type: application/pkcs7-mime; name="smime.p7m"; smime-type=enveloped-data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"
Content-Description: S/MIME Encrypted Message
```

```
MIAGCSqGSIB3DQEHA6CAMIACQAxggGBMIIIBfQIBADBlMFkxEjAQBg0JkiaJk/IsZAEZFgJj
ejEZMBcGCgmSJomT8ixkARKWCWNlc25ldC1jYTESMBAGA1UECgwJQ0VTTkVUIENBMRQwEgYD
VQQDDAtDRVNRVQgQ0EgMwIIGf0MQJPhpowDQYJKoZIhvcNAQEBBQAEggEAGHd79kE8Se3h
9Kbm/pWHXJ4vDhdL5l2/whzU2phAaBhTsuCWR10hgg8hRca3N9TxwYvM9fGjTV0vRpckbL4
```

Pouze podepsaná zpráva:

```
MIME-Version: 1.0
Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg=sha-256; boundary="-----ms080601060806030003010903"
```

This is a cryptographically signed message in MIME format.

```
-----ms080601060806030003010903
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: quoted-printable
```

Ahoj

```
-----ms080601060806030003010903
Content-Type: application/pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature
```

```
MIAGCSqGSIB3DQEHAqCAMIACQExDzANBglghkgBZQMEAqEFADCABgkqhkiG9w0BBwEAAKCC
CMWggRGMIIDLqADAgECAgC90pWgpoxMA0GCSqGSIB3DQEBBQUAMFwxEjAQBg0JkiaJk/Is
ZAEZFgJjejEZMBcGCgmSJomT8ixkARKWCWNlc25ldC1jYTESMBAGA1UEChMJQ0VTTkVUIENB
MRcwFQYDVQQDEw5DRVNORVQgQ0EgUm9vdDAeFw0wOTEyMTUxNTQ2NDdaFw0xOTEyMTgxNTQ2
NDdaMFkxEjAQBg0JkiaJk/IsZAEZFgJjejEZMBcGCgmSJomT8ixkARKWCWNlc25ldC1jYTES
```

Elektronická komunikace

e-mail - šifrování

- PGP - Pretty Good Privacy
- Vytvořil Phil Zimmermann v roce 1991
- Umístěno na veřejný FTP server
- Žaloba od RSA Data Security Inc. za použití RSA, vyšetřování za porušení Arms Export Control Act
- 1996 - vlastní firma PGP Inc., nová verze PGP a další na PGP postavené produkty
- PGP Inc. prodáno různým firmám, nakonec v roce 2010 skončilo v Symantecu
- PGP 2.x - IDEA (patent), PGP 5.0 - CAST5
- Paralelní vývoj dalších implementací => v roce 1997 vzniká IETF standard OpenPGP, založený na PGP 5.0, definovaný momentálně v RFC 4880 - OpenPGP message format (6637 - ECC in OpenPGP)





Elektronická komunikace

e-mail - šifrování - OpenPGP

- Web of trust
 - Získání (keyserver, web, osobně) a ověření veřejného klíče (telefonické ověření fingerprintu, keysigning party, WoT)
 - Keysigning party - ověřování fingerprintů, podepisování klíčů
 - ověřím fingerprint -> podepíši public key -> je pro mne validní
 - Trust levels
 - unknown (initial status nových klíčů na mého public keyringu), none, marginal, full
 - Nevalidní klíč, podepsaný jedním fully trusted nebo třemi marginally trusted => validní (default settings)
- Podpora v mnoha MU chybí
- Platnost a sílu šifrování určuje každý zvlášť při vytváření klíčů (nebezpečí konfliktu verzí)
- Podpora mnoha crypto algoritmů, nově včetně ECC
- Mohu generovat subkeys dle libosti (expiration date nezávisí na master key, podepsáno master key)



Elektronická komunikace

e-mail - šifrování

- SKS keyservery (Synchronizing Key Server)
 - Sloučeny do poolu: pool.sks-keyservers.net
 - Synchronizace, RFC compliance, aktualizace

eu.pool.sks-keyservers.net

ipv4.pool.sks-keyservers.net

ipv6.pool.sks-keyservers.net

p80.pool.sks-keyservers.net

jirk5u4osbsr34t5.onion

- 4250000 klíčů (1000/den)



Elektronická komunikace

e-mail - šifrování - OpenPGP

- Jak podepisovat maily
 - Clear Signing (inline)
 - MIME Content Type: Text/Plain (Text/HTML :])
 - Funguje všude, může být matoucí pro ostatní bez PGP, text navíc (BEGIN PGP SIGNED MESSAGE , ...)
 - application/pgp
 - Mutt <= 1.4 a možná další
 - Content-disposition: inline při podepisování inline zpráv => bez podpory PGP nečitelné
 - pgp/mime
 - MIME Content Type: Multipart/Signed
 - Tělo mailu je Text/Plain -> čitelné všude bez matoucího textu navíc



Elektronická komunikace

e-mail - šifrování



- Gnu Privacy Guard/GnuPG/GPG/
 - Balík nástrojů pro šifrování dat (mohu šifrovat a podepisovat nejen maily, ale jakákoli data (soubory, adresáře))
 - FOSS implementace OpenPGP standardu
 - + něco navíc :) (takže pozor na kompatibilitu)
 - <https://www.gnupg.org/>
 - GnuPG stable (2.0) - stabilní verze, OpenPGP, S/MIME (gpgsm)
 - GnuPG modern (2.1) - nová verze s pokročilými funkcemi, jako je podpora ECC, časem nahradí 2.0 jako stable
 - GnuPG classic (1.4) - obsolete, portable verze, jedna staticky zkompilovaná binárka; chybí jí mnoho vlastností moderních verzí



Elektronická komunikace

e-mail - šifrování

- postaveno na knihovně libgcrypt (aktuální stable verze 1.6.5)

```
gpg (GnuPG) 2.1.10
libgcrypt 1.6.4
Copyright (C) 2015 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: ~/.gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2
```

- Default RSA+SHA256 pro podpis a digest, RSA pro zašifrování session key a CAST5 pro zašifrování těla zprávy
- 2.1 - AES, SHA512



Elektronická komunikace

e-mail - šifrování

- Implementace v různých OS
 - Linux - GnuPG běžně přítomno v distribucích
 - Mutt - native support
 - Thunderbird - Enigmail
 - Kontact (Kmail) - native
 - Evolution - native
 - Windows - GPG4WIN - stable verze GnuPG (2.0)
 - Thunderbird - Enigmail
 - OS X - GnuPG (homebrew), GPGTools (2.0)
 - Apple mail - GPGTools
 - Thunderbird - Enigmail
 - Mutt - native support
- GPGRelay - GPG proxy



Elektronická komunikace

e-mail - šifrování

- Implementace na mobilních OS
 - Android
 - PGP/Inline
 - K9 mail, Kaiten Mail
 - Crypto provider - APG, OpenKeychain
 - PGP/MIME + S/MIME
 - Maildroid + Flipdog Solutions Crypto Plugin
 - iOS
 - iPGMail
 - oPenGP

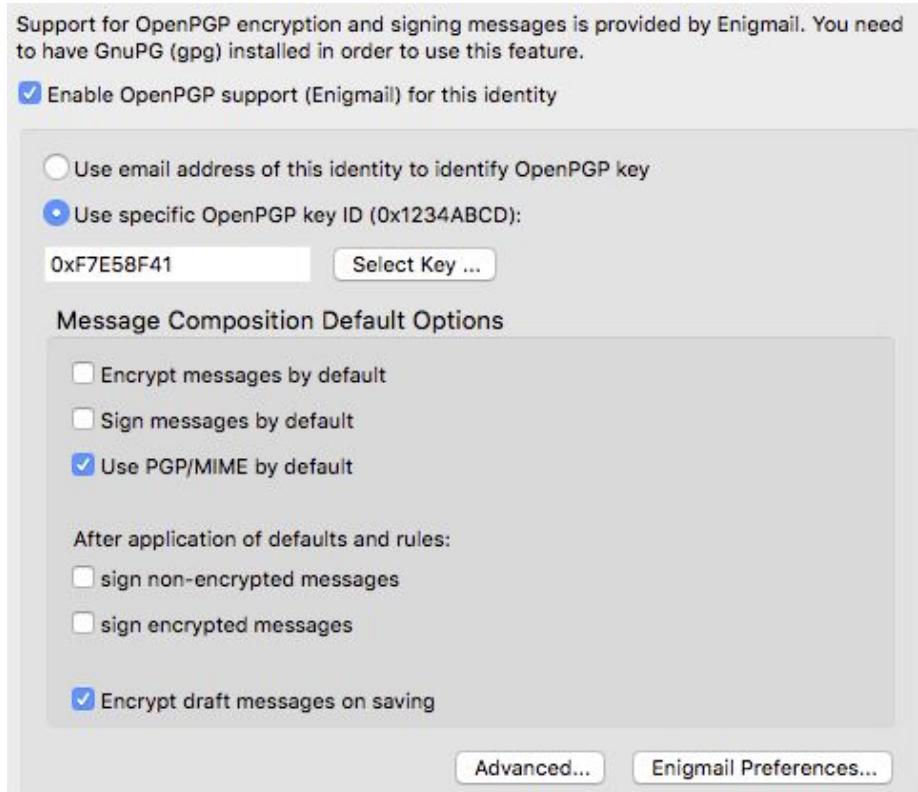
Elektronická komunikace



e-mail - šifrování

- Enigmail

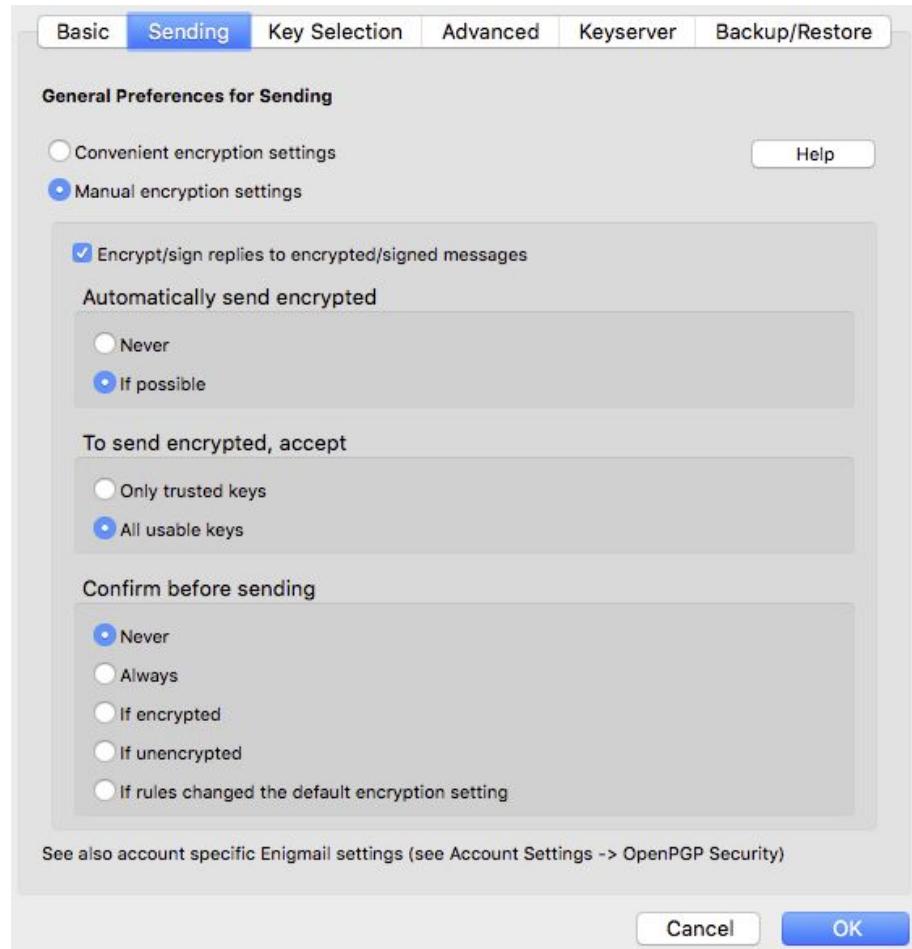
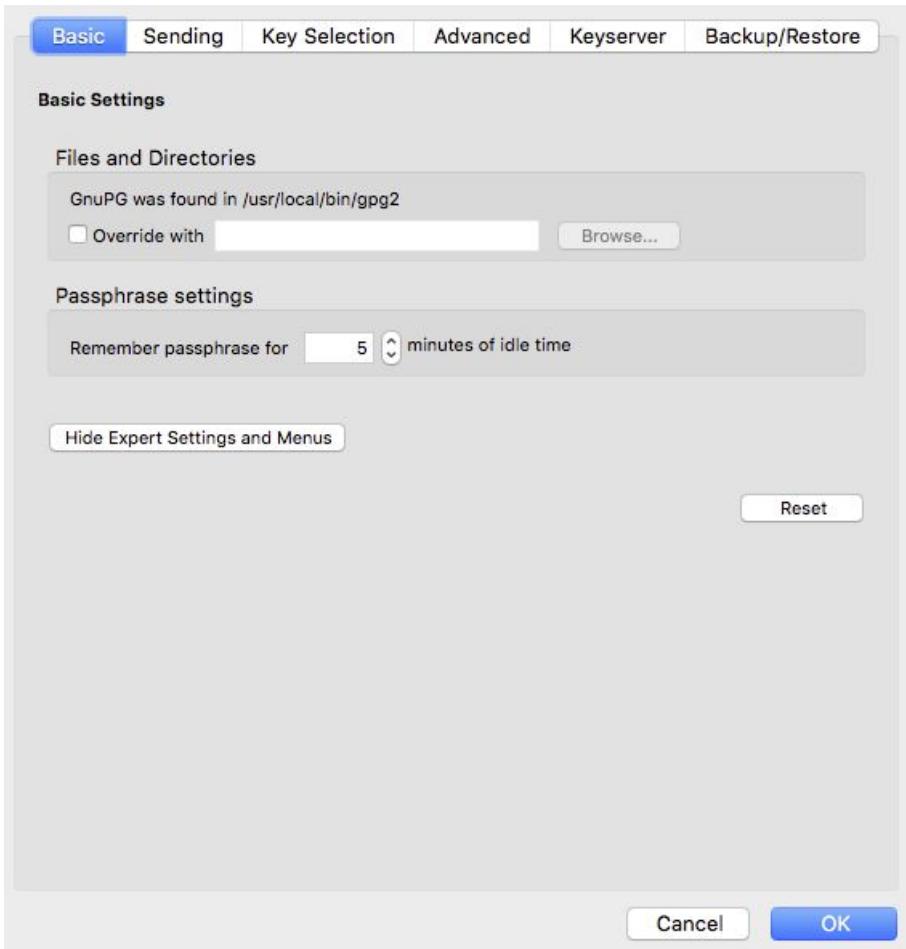
- Podpora GPG v Mozilla Thunderbird ve formě pluginu
- Funguje všude kde běží Thunderbird



Elektronická komunikace

e-mail - šifrování

- Enigmail





Elektronická komunikace

e-mail - šifrování

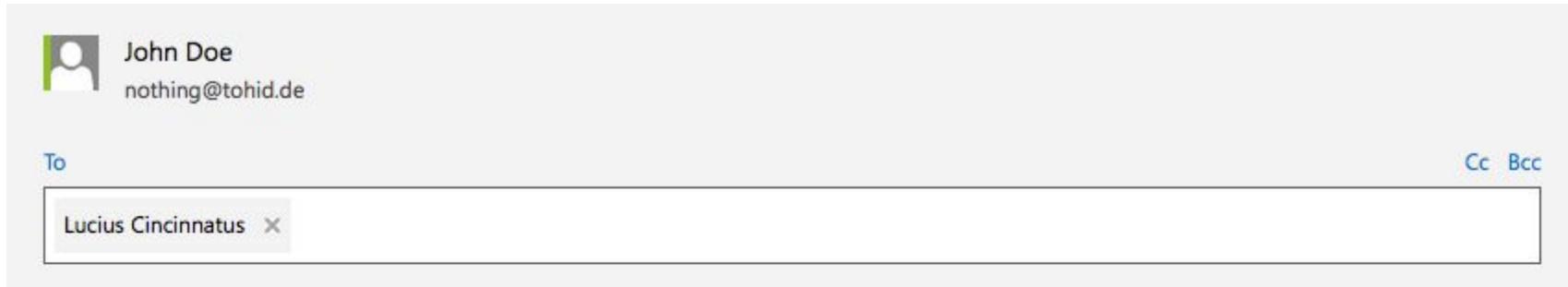
- Mailvelope

- <https://www.mailvelope.com/>
- Podpora GnuPG ve webmailech
- Firefox addon, Chrome plugin
- Aplikace, běžící v browseru
- Kompletná správa klíčů, vygenerování nových



Elektronická komunikace

e-mail - šifrování



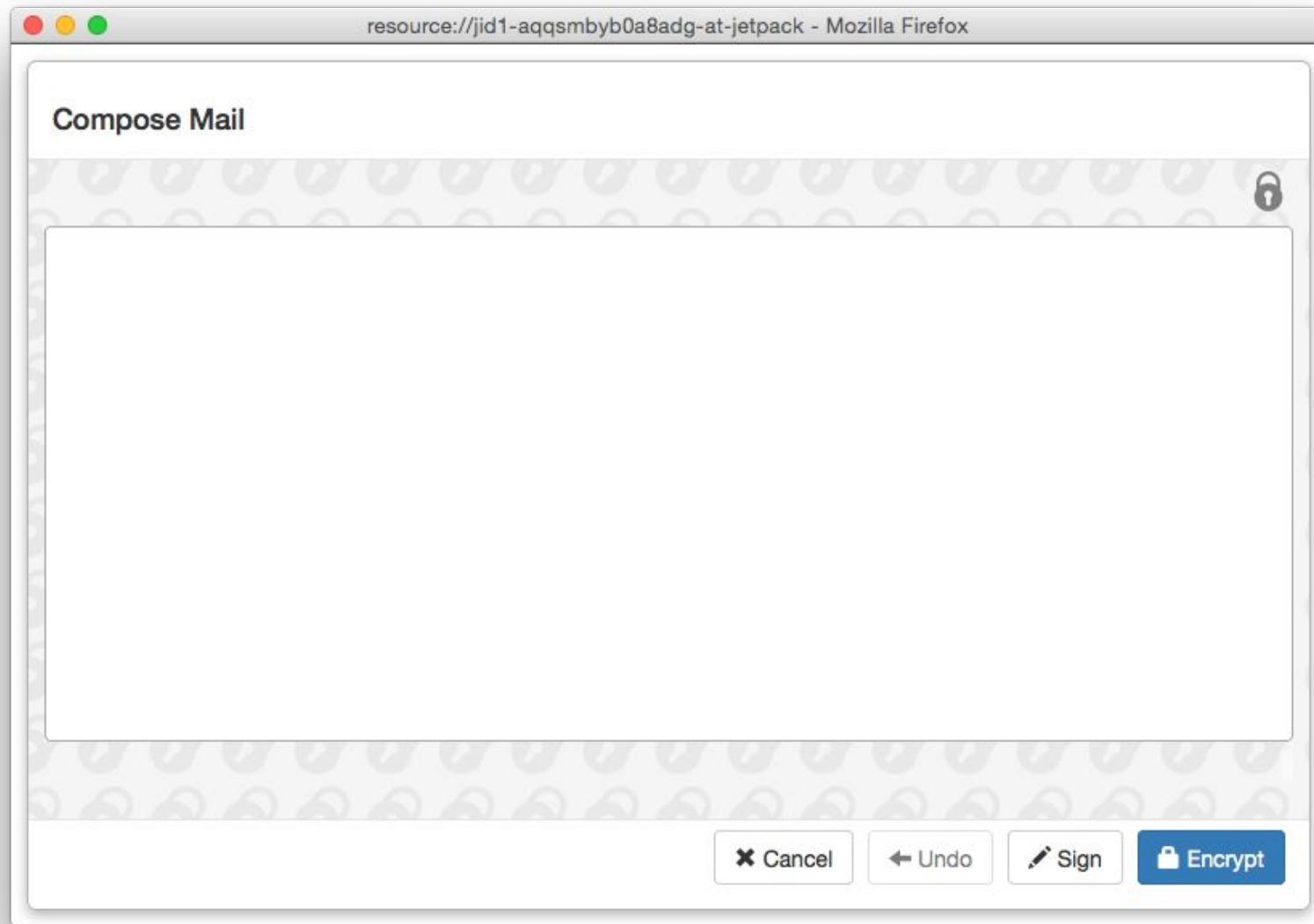
Draft saved at 1:32 PM





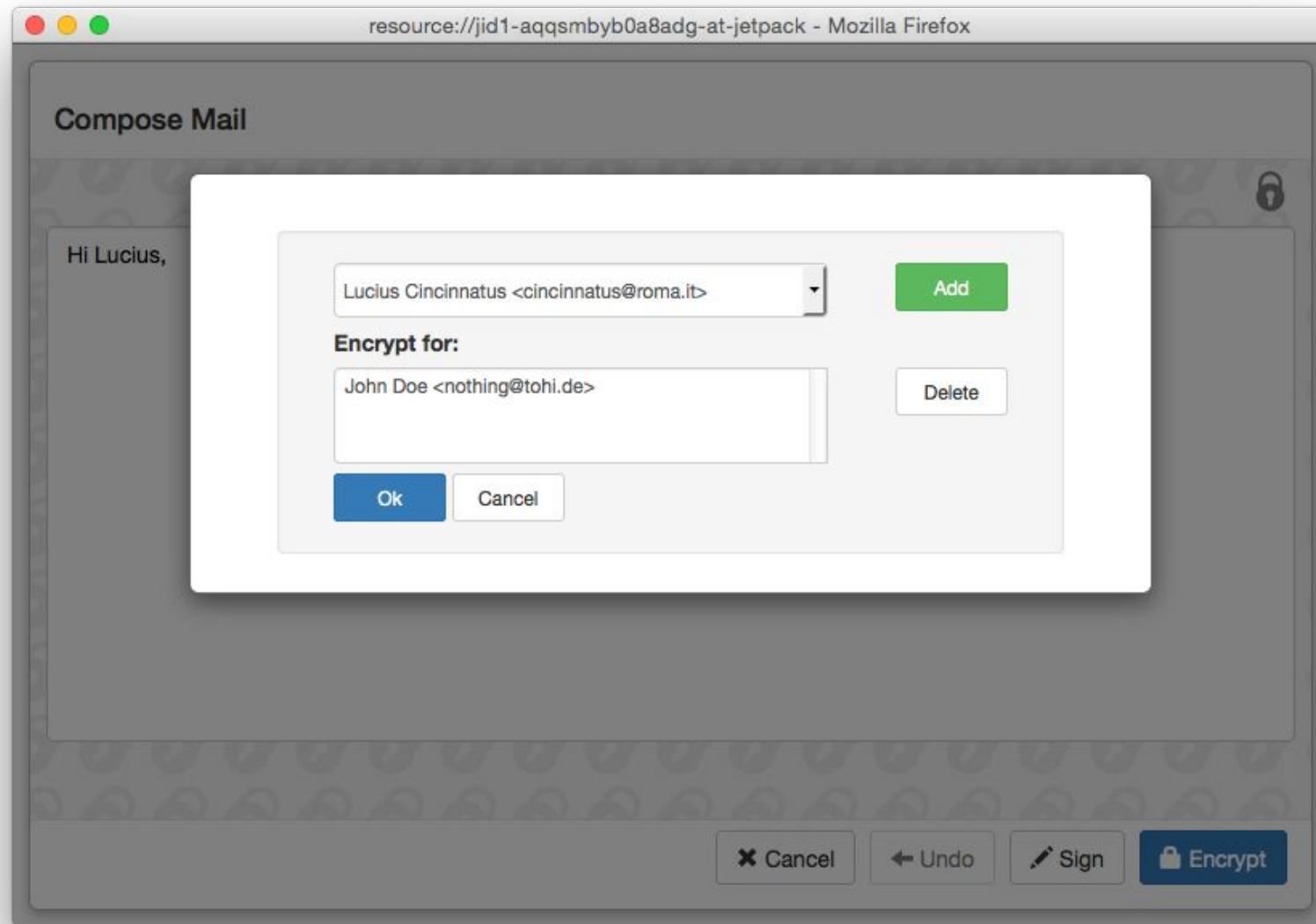
Elektronická komunikace

e-mail - šifrování



Elektronická komunikace

e-mail - šifrování



Elektronická komunikace

e-mail - šifrování

 John Doe
nothing@tohid.de

Draft saved at 1:47 PM

B / U Aa A⁺ A

-----BEGIN PGP MESSAGE-----

Version: Mailvelope v1.1.0

Comment: <https://www.mailvelope.com>



wcFMA5j8x6LC/hY+AO/+LEW+cyShFHR6oLqceov5YhfwtTpzNVEEMbi8+zjwi
18j1YYmqFsS23cIdueBZ42izkwFio+uLsyYf26C71hk1CoWqWGJDTpXjkTW1
JhQ5t20Reo/iCRv8xREx61a0OH7zQyOaiEKcbA1guqbKcZ6zNMMjPt2rUikj
TdU8ZafPyQ0UTEaL/QX908YzQ9Srsw+5Vv+omZ5tyG8WcAUSzXfT1G/VRfbm
wq8c3S0/QfBMZqVU4V2dN2sKk/C6qKS4dEHuEiHzaZGOOYadKTCC2ZFFGpu
bCf8eKfqCi0lamG2kct2H6LnrByqgUdejwTCIrKnG3kBEOyEC9pvsL70afiM
280rnf5o6XC2mfen7rTnAcAcEvDHR8Oqpu/DU4q6al3B8v1HTJUyJ9gGvuat
gBoE933QcBo14YMF7Co3b4HpurUmvrM0TQzVjhJjpGR6aa0ne9vjeovEwzMm
SQ1KjcSFJs1eo3QTzAkPle/vH625GxdUzW/t4ZBwh7ao70Pm+bdc7Uz1Chc
Ay3mTkhSZumLf0jXchscOPQOubyLJW0mRHDCS3TYmowUwdeKIeMAixI99wFZR

Elektronická komunikace

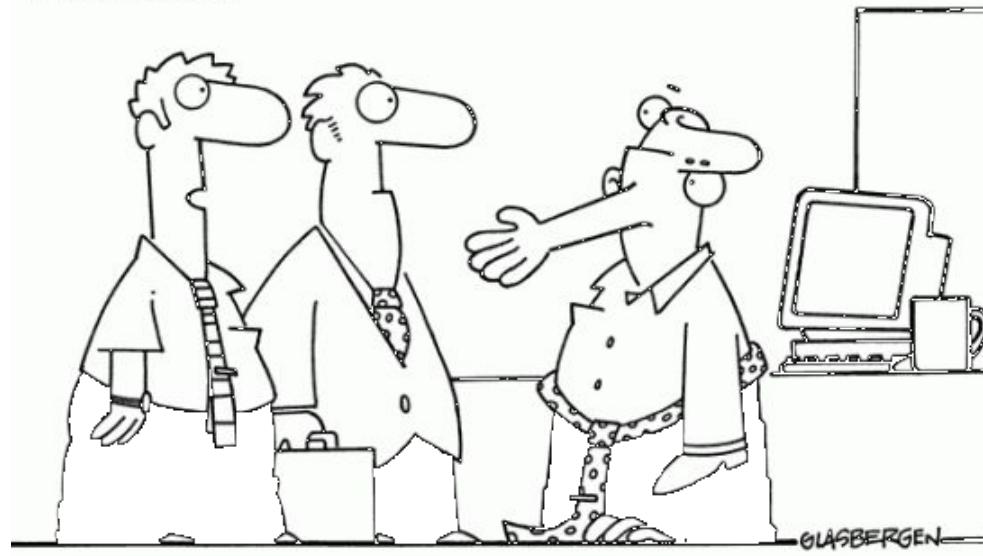


e-mail - šifrování

Nic není dokonalé:

- Zašifrovaný mail nelze cestou zkontoirovat na přítomnost malware
- Metadata a subject se nešifrují
- Neexistující forward secrecy (lze řešit pomocí OpenPGP subkeys, ale je to neohrabane)

Copyright 2002 by Randy Glasbergen.
www.glasbergen.com



"That's our CIO. He's encrypted for security purposes."



OTR - off the record messaging

- Kryptografický protokol pro šifrování IM konverzací
- Ian Goldberg a Nikita Borisov, released 2004
 - Poskytuje knihovnu pro integraci OTR do IM klientů (Gaim, Pidgin, Adium, ...)
- Kromě autentizace a šifrování nabízí navíc
 - Forward secrecy - per-message AES klíče, dohodnuté pomocí Diffie-Hellman key exchange (odvozené z master secret, spolu s klíčem pro MAC, zajišťujícím integritu zprávy)
 - Deniable authentication - zprávy nejsou podepsány žádným dlouhodobým klíčem, po ukončení konverzace může kdokoliv vytvořit stejnou zprávu
- Od v3 (libotr 4.0.0) - více konverzací se stejným člověkem, který je zalogovaný na více místech/zařízeních najednou
- Nepodporuje group chat



Signal protocol

- Moxie Marlinspike & Trevor Perrin, 2013
- Signal (née TextSecure, RedPhone)
 - Open source, #1!
- WhatsApp (od 5.6.16')
- Inspirace OTR
- Group chat!
- Zvuk!
- Asynchronní komunikace
 - handshake pomocí pre-keys uložených na serveru
 - async PFS pomocí double ratchet
 - Zlepšuje deniability (TripleDH místo DH+DES)





Axolotl (double) ratchet

- OTR (3-step ratchet)
 - Klíče rotovány pomocí Diffie-Hellman ve zprávách
 - + Self-healing (future secrecy)
 - - Klient drží klíč dokud strana neodpoví
- Silent Circle (2-step ratchet)
 - Klíče se zahazují po každé zprávě, rotují se $K_n = \text{KDF}(K_{n-1})$
 - + Skvělá PFS
 - - Chybí future secrecy, problémy při porušení pořadí
- **Double ratchet, “Axolotl”**
 - 2-step, kombinuje HD a KDF ratchet
 - Výhody obou
 - Async, PFS, self-healing





Další použití Axolotl ratchet

- Pond, Mute
 - Mail-like systémy, vysokolatenční
 - Key distribution (hash-chain), metadata
- OMEMO, Wire, ...



Doporučení klienti

- Signal (když nám nejde o anonymitu)
 - <https://whispersystems.org/>
- ChatSecure + Orbot (když nám jde o anonymitu)
 - <https://guardianproject.info/apps>
- Secure Messaging Scorecard
 - <https://www.eff.org/secure-messaging-scorecard>
- Surveillance Self-Defense
 - <https://ssd.eff.org/>

Tor Meetup



1N3Mafk6nTxds5wnKUkQV7iHnsUjSN9UXz

<https://github.com/ParalelniPolis/tor-meetup>

stick@gk2.sk PGP/B9A02A3D