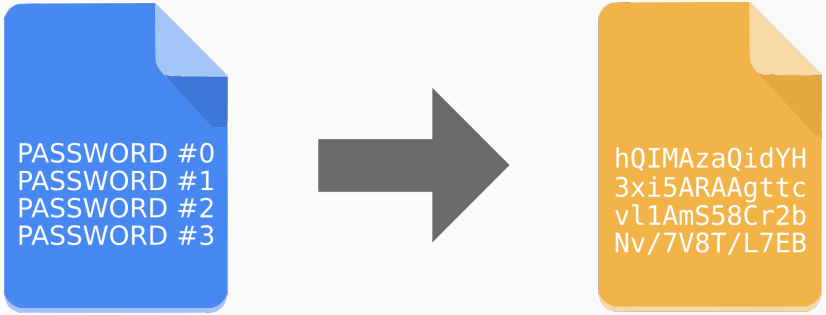
Základy GnuPG

Emil Miler

https://fingerprinter.pdostal.cz

???


PASSWORD #0
PASSWORD #1
PASSWORD #2
PASSWORD #3
hQIMAzaQidYH
3xi5ARAAgttc
vl1AmS58Cr2b
Nv/7V8T/L7EB


hQIMAZaQidYH
3xi5ARAAgttc
vl1Ams58Cr2b
Nv/7V8T/L/EB

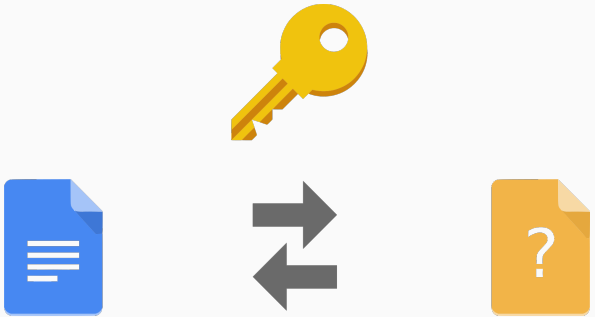

hQIMAzaQidYH
3xi5ARAAgttc
vl1AmS58Cr2b
Nv/7V8T/L7EB

Obsah přednášky

- Kryptografie
- PGP, OpenPGP & GnuPG
- Generování klíčů
- Základy šifrování & dešifrování
- Elektronické podpisy
- Příprava na key signing párty
  - Průběh párty
  - Proces podepisování

Kryptografie

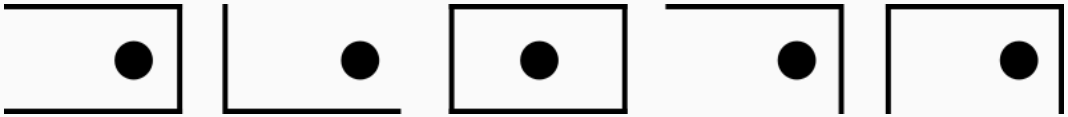
Symetrická kryptografie



Symetrická kryptografie - Velký polský kříž

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

Symetrická kryptografie - Velký polský kříž

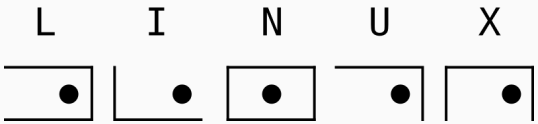


Symetrická kryptografie - Velký polský kříž

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	

Symetrická kryptografie - Velký polský kříž

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	



Asymetrická kryptografie

Key Pair

Public Key

Private Key

PGP, OpenPGP & GnuPG

Pretty Good Privacy

OpenPGP + GnuPG

Generování klíčů

```
$ gpg --full-gen-key
```

```
$ gpg --full-gen-key
```

Algoritmus: RSA

Délka klíče: 4096 bit

Expirace: ??

Jméno:

Email:

Komentář:

```
 $ gpg -k
pub    rsa4096 2016-09-15 [SC] [expires:  2018-10-06]
        52C29D89915D03EC3F55F03523BB315BAB68B241
uid        [ultimate] Emil Miler <emil.miler@pedf.cuni.cz>
uid        [ultimate] Emil Miler <em@cocaine.ninja>
sub    rsa4096 2016-09-15 [E] [expires:  2018-10-06]
```

Základy šifrování & dešifrování

```
$ gpg -ear recipient
```

```
$ gpg -ear recipient
```

-e : encrypt

-a : armour

-r : recipient

```
$ cat message.txt | gpg -ear recipient > secret.asc
```

```
$ gpg -d secret.asc
```

Roundcube - `Enigma`

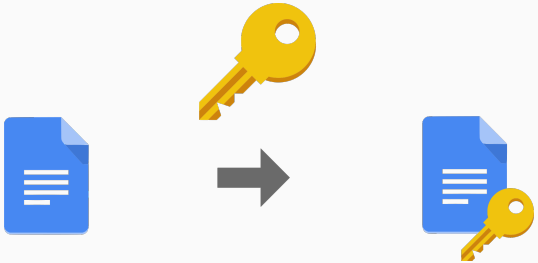
Thunderbird - `Enigmail`

Claws Mail - `GPG Plugin`

KMail

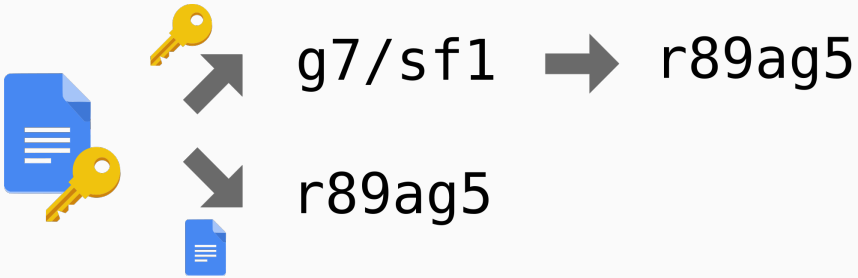
Elektronické podpisy

Elektronické podpisy



Elektronické podpisy - Průběh podpisu

Elektronické podpisy - Průběh ověření podpisu



```
$ gpg --sign message.txt
```

```
$ gpg --verify message.txt.gpg
```

Příprava na key signing párty

Lístečky

```
0x23BB315BAB68B241 2016-09-15 [SC]
fingerprint: 52C2 9D89 915D 03EC 3F55
             F035 23BB 315B AB68 B241
Emil Miler <emil.miler@pedf.cuni.cz>
Emil Miler <em@cocaine.ninja>
```

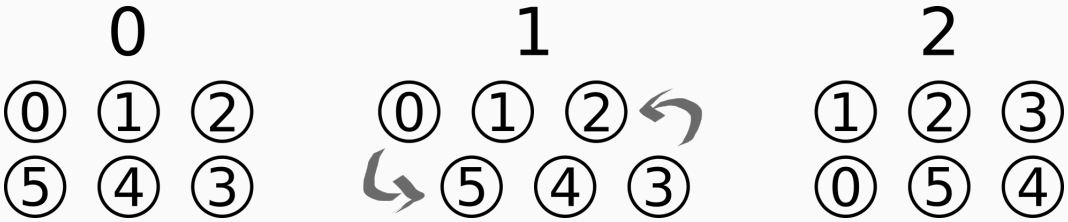

```
0x23BB315BAB68B241 2016-09-15 [SC]
fingerprint: 52C2 9D89 915D 03EC 3F55
             F035 23BB 315B AB68 B241
Emil Miler <emil.miler@pedf.cuni.cz>
Emil Miler <em@cocaine.ninja>
```

```
0x23BB315BAB68B241 2016-09-15 [SC]
fingerprint: 52C2 9D89 915D 03EC 3F55
             F035 23BB 315B AB68 B241
Emil Miler <emil.miler@pedf.cuni.cz>
Emil Miler <em@cocaine.ninja>
```

```
0x23BB315BAB68B241 2016-09-15 [SC]
fingerprint: 52C2 9D89 915D 03EC 3F55
             F035 23BB 315B AB68 B241
Emil Miler <emil.miler@pedf.cuni.cz>
Emil Miler <em@cocaine.ninja>
```


https://fingerprinter.pdostal.cz

Formace



Výměna lístků

Během párty zkontrolovat:

- průkaz identity s fotografií
- že lístek obsahuje adresu a otisk

```
0x23BB315BAB68B241 2016-09-15 [SC]
fingerprint: 52C2 9D89 915D 03EC 3F55
             F035 23BB 315B AB68 B241
Emil Miler <emil.miler@pedf.cuni.cz>
Emil Miler <em@cocaine.ninja>
```

https://fingerprinter.pdostal.cz

Průběh podepisování

- Stáhnout klíč z keyserveru
  - `$ gpg --keyserver pool.sks-keyservers.net --recv-keys <keyid>`
- Zkontrolovat otisk podle papírku
  - `$ gpg --fingerprint <keyid>`
- Podepsat správné identity
  - `$ gpg --sign-key --ask-cert-level <keyid>`
- Odeslat klíč majiteli
  - `$ gpg -a --export <keyid> | gpg -ear <keyid> > <keyfile>.asc`

https://www.linuxdays.cz/2017/key-signing-party

https://fingerprinter.pdostal.cz