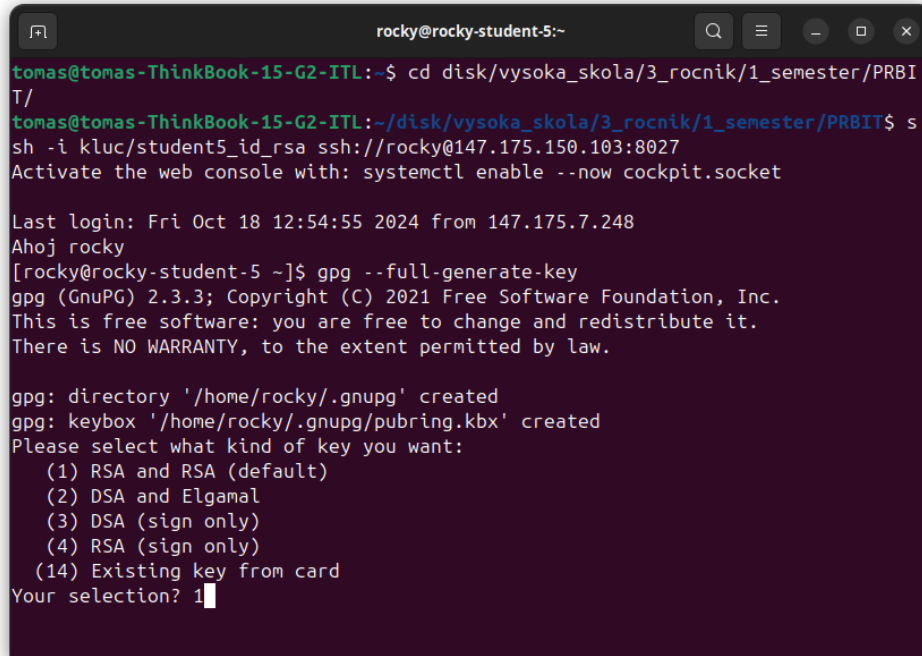


Zadanie

Úloha 1

1. Vytvorte vlastný pár kľúčov použiteľný pre šifrovanie aj pre podpisovanie dokumentov
gpg --full-generate-key – tento príkaz spustí vytváranie dvojice kľúčov

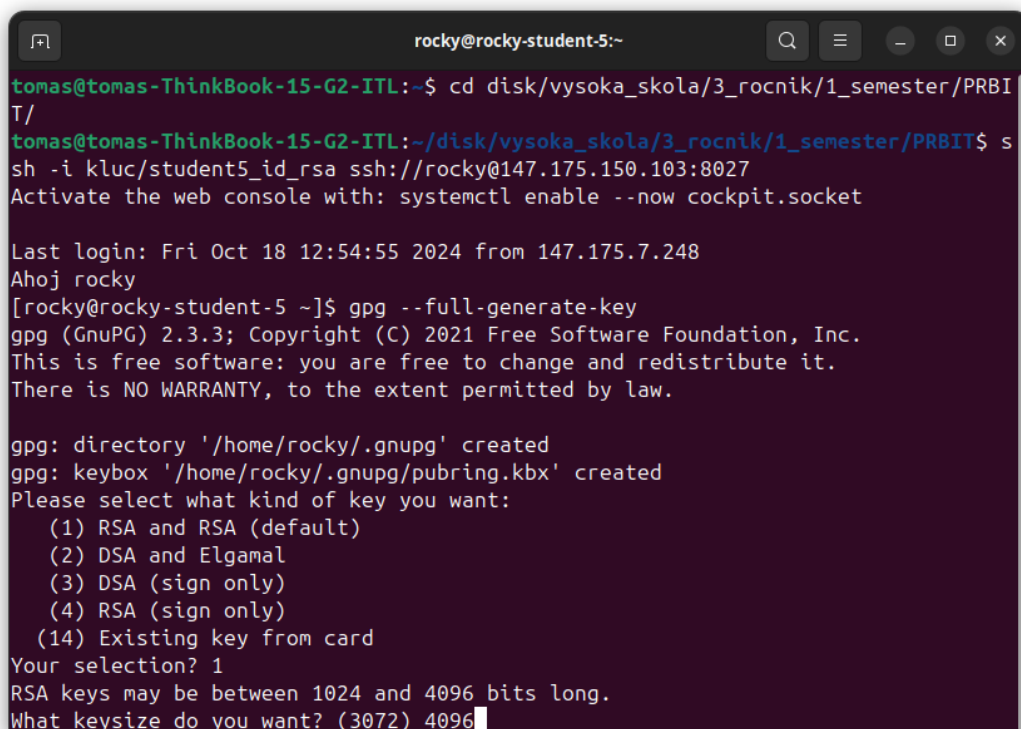


```
rocky@rocky-student-5:~  
tomas@tomas-ThinkBook-15-G2-ITL:~$ cd disk/vysoka_skola/3_rocnik/1_semester/PRBIT/  
tomas@tomas-ThinkBook-15-G2-ITL:~/disk/vysoka_skola/3_rocnik/1_semester/PRBIT$ s  
sh -i kluc/student5_id_rsa ssh://rocky@147.175.150.103:8027  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Fri Oct 18 12:54:55 2024 from 147.175.7.248  
Ahoj rocky  
[rocky@rocky-student-5 ~]$ gpg --full-generate-key  
gpg (GnuPG) 2.3.3; Copyright (C) 2021 Free Software Foundation, Inc.  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.  
  
gpg: directory '/home/rocky/.gnupg' created  
gpg: keybox '/home/rocky/.gnupg/pubring.kbx' created  
Please select what kind of key you want:  
  (1) RSA and RSA (default)  
  (2) DSA and Elgamal  
  (3) DSA (sign only)  
  (4) RSA (sign only)  
  (14) Existing key from card  
Your selection? 1
```

Zvolil som možnosť 1 pre RSA a RSA kľúč.

- zvoľte maximálnu možnú veľkosť kľúča

Pre zvolenie maximálnej možnej veľkosti kľúča som zadal najvyššiu hodnotu, ako bolo možné zadať, a teda 4096 bitov.

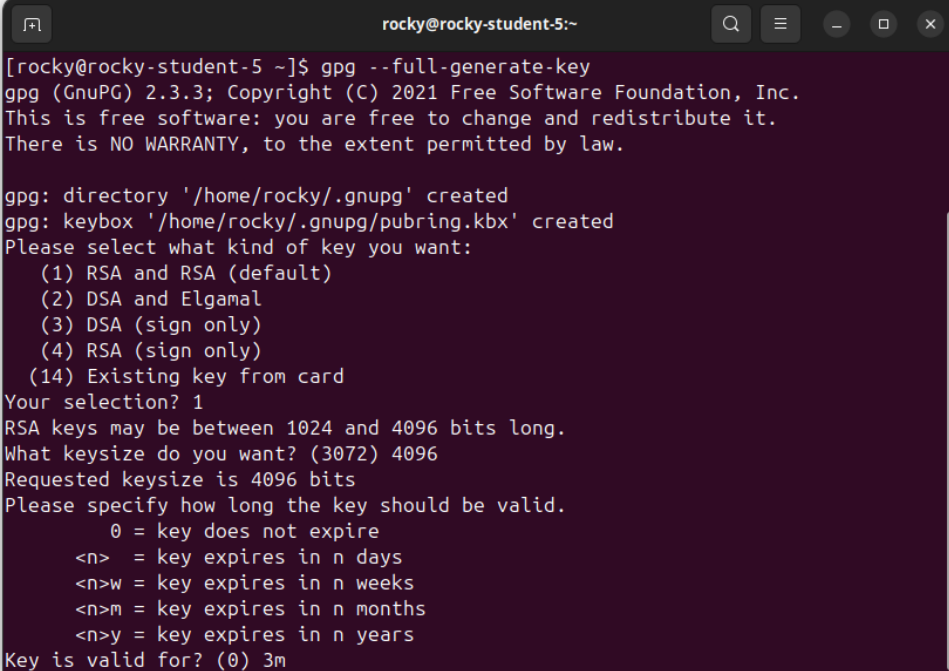


```
rocky@rocky-student-5:~  
tomas@tomas-ThinkBook-15-G2-ITL:~$ cd disk/vysoka_skola/3_rocnik/1_semester/PRBIT/  
tomas@tomas-ThinkBook-15-G2-ITL:~/disk/vysoka_skola/3_rocnik/1_semester/PRBIT$ s  
sh -i kluc/student5_id_rsa ssh://rocky@147.175.150.103:8027  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Fri Oct 18 12:54:55 2024 from 147.175.7.248  
Ahoj rocky  
[rocky@rocky-student-5 ~]$ gpg --full-generate-key  
gpg (GnuPG) 2.3.3; Copyright (C) 2021 Free Software Foundation, Inc.  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.  
  
gpg: directory '/home/rocky/.gnupg' created  
gpg: keybox '/home/rocky/.gnupg/pubring.kbx' created  
Please select what kind of key you want:  
  (1) RSA and RSA (default)  
  (2) DSA and Elgamal  
  (3) DSA (sign only)  
  (4) RSA (sign only)  
  (14) Existing key from card  
Your selection? 1  
RSA keys may be between 1024 and 4096 bits long.  
What keysize do you want? (3072) 4096
```

Tomáš Brček, ID:120761
Cvičenie: Pondelok 17:00

- pár by mal stratiť platnosť po 3 mesiacoch od vytvorenia

Keďže by tento pár mal stratiť platnosť po 3 mesiacoch od vytvorenia, pri ďalšej otázke som zadal
3m



```
rocky@rocky-student-5:~  
[rocky@rocky-student-5 ~]$ gpg --full-generate-key  
gpg (GnuPG) 2.3.3; Copyright (C) 2021 Free Software Foundation, Inc.  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.  
  
gpg: directory '/home/rocky/.gnupg' created  
gpg: keybox '/home/rocky/.gnupg/pubring.kbx' created  
Please select what kind of key you want:  
  (1) RSA and RSA (default)  
  (2) DSA and Elgamal  
  (3) DSA (sign only)  
  (4) RSA (sign only)  
  (14) Existing key from card  
Your selection? 1  
RSA keys may be between 1024 and 4096 bits long.  
What keysize do you want? (3072) 4096  
Requested keysize is 4096 bits  
Please specify how long the key should be valid.  
  0 = key does not expire  
  <n> = key expires in n days  
  <n>w = key expires in n weeks  
  <n>m = key expires in n months  
  <n>y = key expires in n years  
Key is valid for? (0) 3m
```

Po zadaní všetkých údajov, vrátane mena, emailovej adresy a frázy, bol vygenerovaný pár kľúčov.

- Exportujte svoj verejný kľúč a vymenťte si exportovaný kľúč s kolegom

`gpg --armor --export xbrcek@stuba.sk > my_public_key.asc` – exportovanie môjho verejného kľúča do `my_public_key.asc`

`--armor` – exportovanie do formátu ASCII armor

Takto exportovaný kľúč som následne poslal kolegovi a on mne poslal svoj. Kolegov kľúč som uložil do súboru `kolegov_verejny_kluc.asc` a importoval som ho príkazom:

Tomáš Brček, ID:120761
Cvičenie: Pondelok 17:00

gpg --import kolegov_verejny_kluc.asc – importovanie kolegovho verejného kľúča

```
rocky@rocky-student-5:~$ cat kolegov_verejny_kluc.asc
JTPy80pyH0EHtBioY0xTfCXdQ2Qxqsm5IFhvQJPaGFSQt10gj+2iCGBrNzQxtbnp
czu0afHBHIU2bFmSjJ0WjRpRaPLO6aWAaM8t7CvhZeWYqZZwruLNQzugL6WZ1iEz
k0VFsQUAEQEAAYkCPAQYAQgAJhYhBBfdRqv7VyXttVJtrRTGn6V0lqAdBQJnFi5Q
AhsMBQkAdqcAAAOJEBTGn6V0lqAdGE8P/3o0nViCU1Tfc1ywGwAcJ3Lj+vAY43FY
eYw0ENvWz/1Dp9eqisz8jNpntk6jk/+xsNFhC0VdLKdKe6ehuiXVIfo81h18dE9G
HsHIOMphfWCFTJ4k19VVIkKab3iWqjlGb3XPgWHEQGAwVfAzW0Hqps1szpavlZ90
WTduu1T1of0SZzD0F98iR+sQFMjtPIDpgweVe68KpEnIc3bA/JDqFbSGSTRMhcmP
U6qTTF/ItSWJXXwLaRpw6gw3P5iP1R+6RrCPkc0ZXj0zKfPLCeSE+dLudTcVpQ4
6XjWrWpcDieN6mbQz91YpQ362JpxxwkeyNIboHQurQiFQRJy8xsi+/DZkzvMFgtQ
o0naDr1y5RNIj2RbF3BbMIqfkXQR7GKK9SivCgwjPE8N0H1x53K/grqVkp1q3pS
5IZlQ0Lcen81dTgjd95S0qMNH0o8ZSa8wZ8jmZpWVE37mS1ckzdHFSjAm323Ymo
UISZjsndnhx9r/4qEz6wD7YpxNEnQakbXzmYvZnb+f1QK68h8L3mPjHFurO/ChdB
SojmhUgRQFwyPI3FRG3DHmiGJcDHCUNajzMJCdPMXBqeuZXPMS4RLE5lfQ8PGMSs
qWZERX5Sz3qG/xBmI5+DvTYMSS+xSJ3pV34Jw9YVjMcel9kMC57j0NVVuedxCj7y
HvFyosqfYHhX
=mqlX
-----END PGP PUBLIC KEY BLOCK-----
[rocky@rocky-student-5 ~]$ vim kolegov_verejny_kluc.asc
[rocky@rocky-student-5 ~]$ gpg --import kolegov_verejny_kluc.asc
gpg: key BC2C0E1258AD991E: public key "Tomáš (Key creation) <xkubrican@stuba.sk>"
imported
gpg: Total number processed: 1
gpg: imported: 1
[rocky@rocky-student-5 ~]$
```

- Overte odtlačok importovaného kľúča vo vašej kľúčenke s odtlačkom kolegu a podpíšte daný kľúč

gpg --fingerprint xkubrican@stuba.sk - overenie odtlačku kolegovho verejného kľúča

```
rocky@rocky-student-5:~$ gpg --fingerprint xkubrican@stuba.sk
pub  rsa3072 2024-10-22 [SC] [expires: 2025-01-20]
      01C8 3E21 0A2C 21A1 69CC B8B3 BC2C 0E12 58AD 991E
uid   [ unknown] Tomáš (Key creation) <xkubrican@stuba.sk>
sub   rsa3072 2024-10-22 [E] [expires: 2025-01-20]

[rocky@rocky-student-5 ~]$
```

Tomáš Brček, ID:120761

Cvičenie: Pondelok 17:00

gpg --sign-key xkubrican@stuba.sk - podpísanie kolegovho kľúča

```
rocky@rocky-student-5:~$ gpg --sign-key xkubrican@stuba.sk

pub rsa3072/BC2C0E1258AD991E
   created: 2024-10-22  expires: 2025-01-20  usage: SC
   trust: unknown      validity: unknown
sub rsa3072/EB4EF8B3BF1AAD27
   created: 2024-10-22  expires: 2025-01-20  usage: E
[ unknown] (1). Tomáš (Key creation) <xkubrican@stuba.sk>

pub rsa3072/BC2C0E1258AD991E
   created: 2024-10-22  expires: 2025-01-20  usage: SC
   trust: unknown      validity: unknown
Primary key fingerprint: 01C8 3E21 0A2C 21A1 69CC  B8B3 BC2C 0E12 58AD 991E

    Tomáš (Key creation) <xkubrican@stuba.sk>

This key is due to expire on 2025-01-20.
Are you sure that you want to sign this key with your
key "Tomas Brcek <xbrcek@stuba.sk>" (14C69FA54E96A01D)?

Really sign? (y/N) y
Please enter the passphrase to unlock the OpenPGP secret key:
"Tomas Brcek <xbrcek@stuba.sk>"
4096-bit RSA key, ID 14C69FA54E96A01D,
created 2024-10-21.

Passphrase:

[rocky@rocky-student-5 ~]$
```

Úloha 2

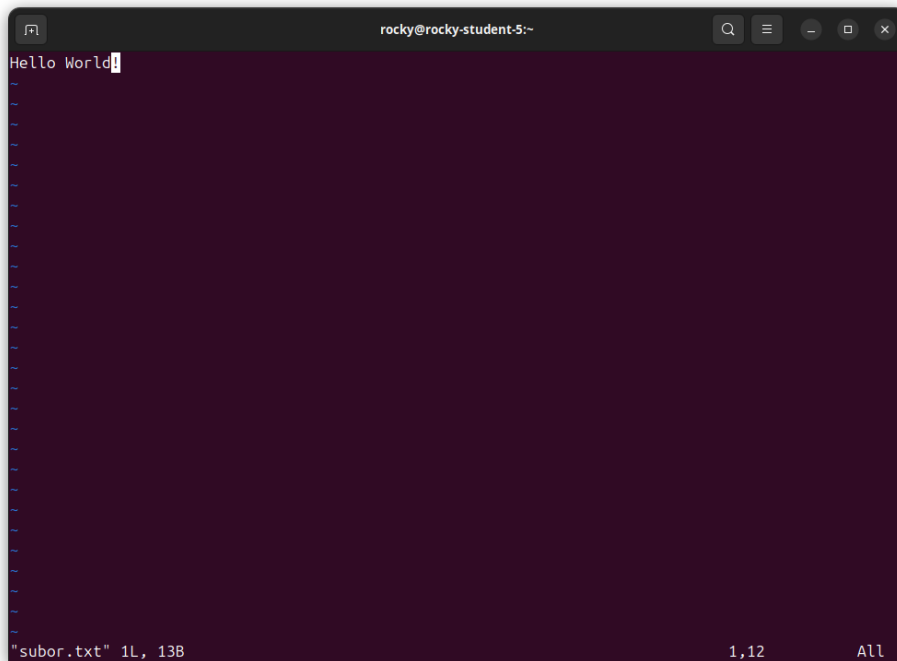
2. Zašifrujte a podpíšte bežný súbor asymetrickou šifrou.

- Zašifrujte súbor tak, aby si jeho obsah dokázal prečítať kolega i Vy.
- Správa a podpis by mali byť v jednom súbore.

Tomáš Brček, ID:120761

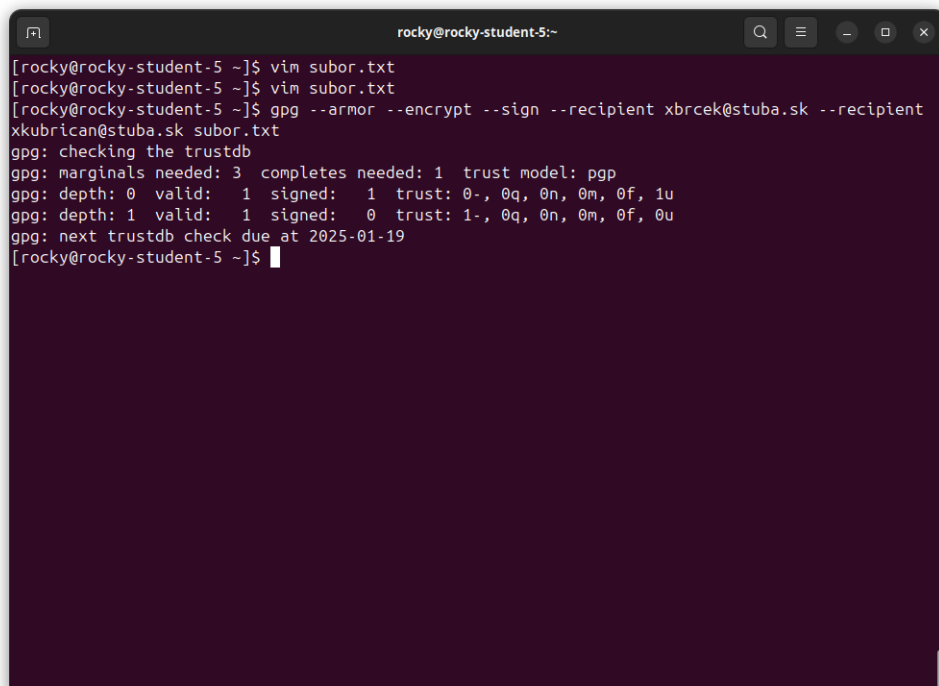
Cvičenie: Pondelok 17:00

Vytvorenie súboru subor.txt a vloženie textu:



```
rocky@rocky-student-5:~  
Hello World  
"subor.txt" 1L, 13B 1,12 All
```

`gpg --armor --encrypt --sign --recipient xbrcek@stuba.sk --recipient xkubrican@stuba.sk subor.txt`
`vim sprava_kolega.asc` – podpísanie súboru asymetrickou šifrou tak, aby som si ho dokázal prečítať ja, aj kolega



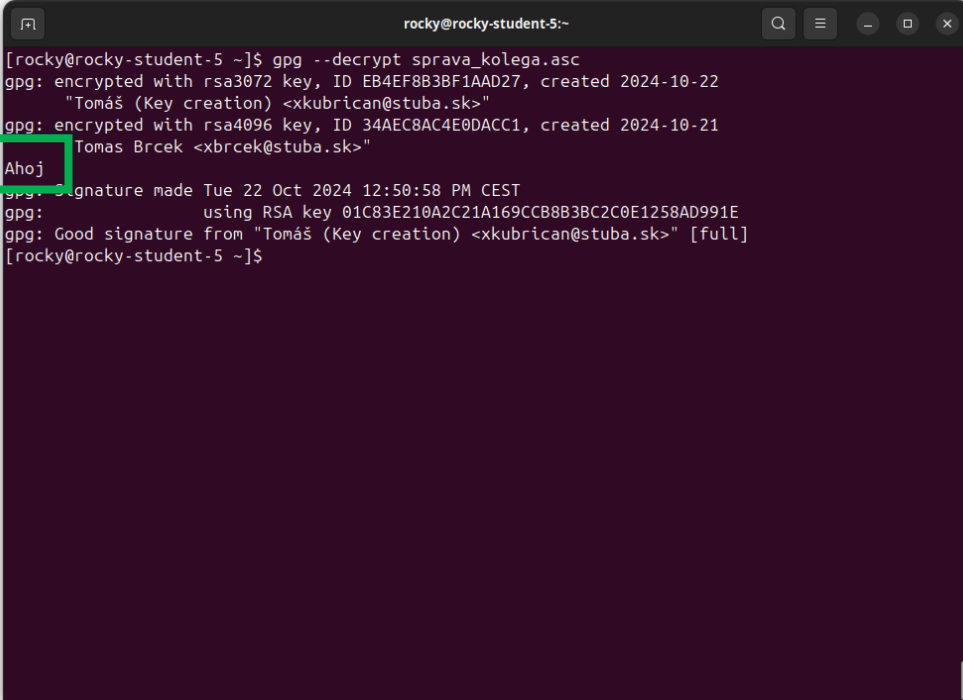
```
rocky@rocky-student-5:~  
[rocky@rocky-student-5 ~]$ vim subor.txt  
[rocky@rocky-student-5 ~]$ vim subor.txt  
[rocky@rocky-student-5 ~]$ gpg --armor --encrypt --sign --recipient xbrcek@stuba.sk --recipient xkubrican@stuba.sk subor.txt  
gpg: checking the trustdb  
gpg: marginals needed: 3 completes needed: 1 trust model: pgp  
gpg: depth: 0 valid: 1 signed: 1 trust: 0-, 0q, 0n, 0m, 0f, 1u  
gpg: depth: 1 valid: 1 signed: 0 trust: 1-, 0q, 0n, 0m, 0f, 0u  
gpg: next trustdb check due at 2025-01-19  
[rocky@rocky-student-5 ~]$
```

- Vymeňte si zašifrovaný súbor s kolegom, ktorého kľúč bol použitý na zašifrovanie súboru.
Vymenili sme si zašifrované súbory a ja som súbor od kolegu uložil do súboru `sprava_kolega.asc`.
- Dešifrujte obdržaný súbor a overte jeho obsah a podpis.

Tomáš Brček, ID:120761

Cvičenie: Pondelok 17:00

gpg --decrypt kolegov_subor.txt.gpg – dešifrovanie súboru od kolegu

A terminal window titled 'rocky@rocky-student-5:~' with a dark purple background. The terminal shows the command 'gpg --decrypt sprava_kolega.asc' being executed. The output indicates the file was encrypted with an RSA key and contains a message from 'Tomáš (Key creation) <xkubrican@stuba.sk>'. The word 'Ahoj' is highlighted with a green box. The terminal also shows the signature was made on 'Tue 22 Oct 2024 12:50:58 PM CEST' and is a 'Good signature from "Tomáš (Key creation) <xkubrican@stuba.sk>" [full]'.

```
rocky@rocky-student-5:~$ gpg --decrypt sprava_kolega.asc
gpg: encrypted with rsa3072 key, ID EB4EF8B3BF1AAD27, created 2024-10-22
      "Tomáš (Key creation) <xkubrican@stuba.sk>"
gpg: encrypted with rsa4096 key, ID 34AEC8AC4E0DACC1, created 2024-10-21
      Tomas Brcek <xbrcek@stuba.sk>
Ahoj
gpg: Signature made Tue 22 Oct 2024 12:50:58 PM CEST
gpg:       using RSA key 01C83E210A2C21A169CCB8B3BC2C0E1258AD991E
gpg: Good signature from "Tomáš (Key creation) <xkubrican@stuba.sk>" [full]
[rocky@rocky-student-5 ~]$
```

Úloha 3

- Aktivujte na vašom stroji webovú konzolu 'cockpit'.

sudo systemctl start cockpit – spustenie cockpit ako služby na rocky linux

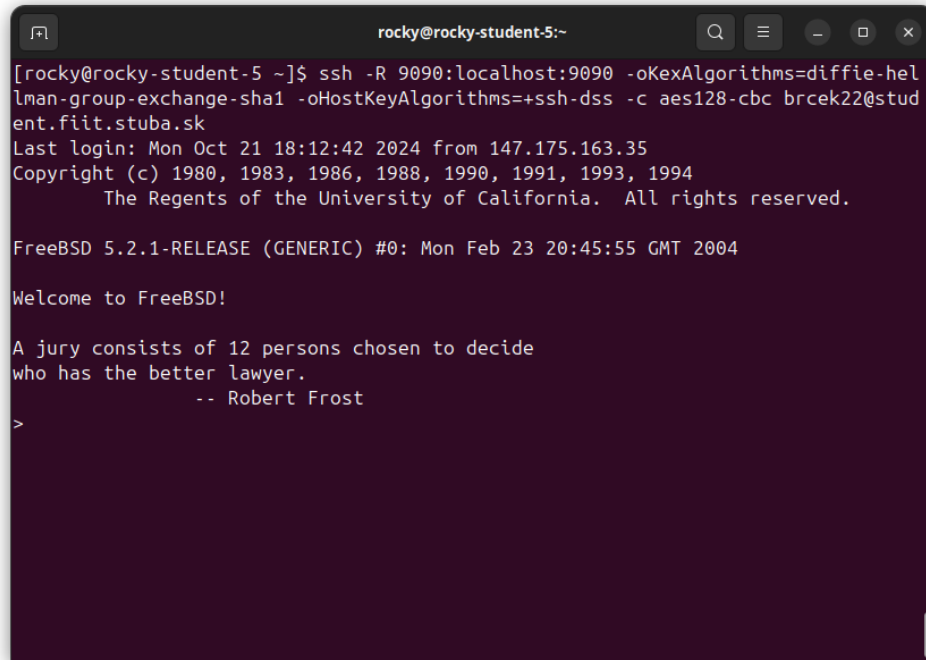
Tomáš Brček, ID:120761

Cvičenie: Pondelok 17:00

- Vytvorte tunel ktorý umožní cez verejne dostupný server na ktorý máte prístup (napr. 'student.fiit.stuba.sk'), urobiť spojenie z vonkajšej siete (napr. z domu) na webovú konzolu na vašom virtuálnom stroji (ktorý je za NAT a nemá verejnú IP adresu).

```
ssh -R 9090:localhost:9090 -oKexAlgorithms=diffie-hellman-group-exchange-sha1 -oHostKeyAlgorithms=+ssh-dss -c aes128-cbc brcek22@student.fiit.stuba.sk
```

- tento príkaz som spustil na rocky linuxe
- tento príkaz vytvoril tunel medzi rocky linuxom a serverom student.fiit.stuba.sk



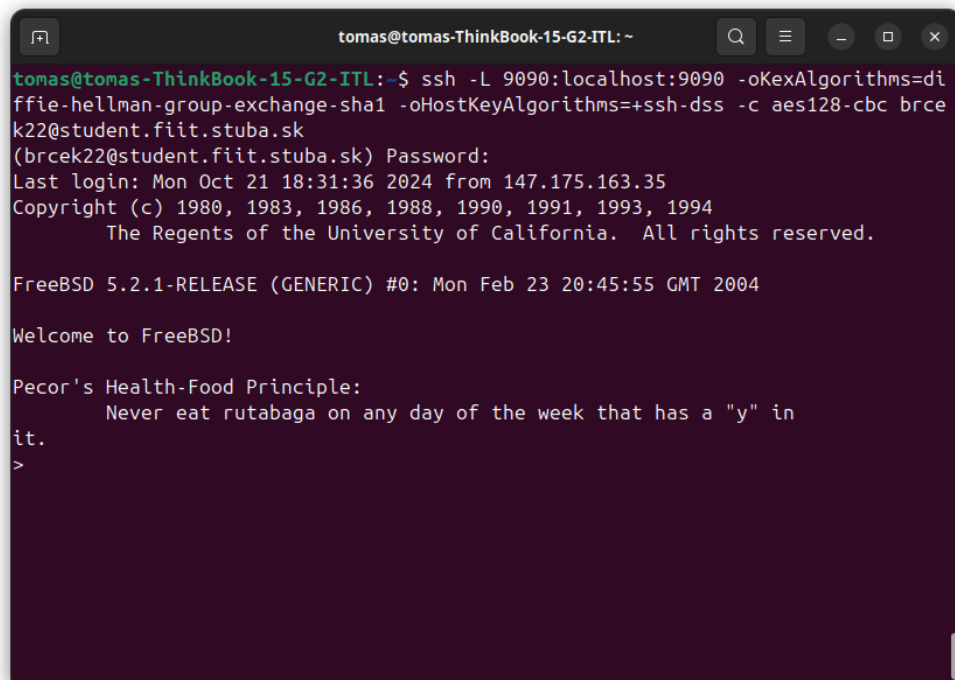
```
rocky@rocky-student-5:~  
[rocky@rocky-student-5 ~]$ ssh -R 9090:localhost:9090 -oKexAlgorithms=diffie-hellman-group-exchange-sha1 -oHostKeyAlgorithms=+ssh-dss -c aes128-cbc brcek22@student.fiit.stuba.sk  
Last login: Mon Oct 21 18:12:42 2024 from 147.175.163.35  
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994  
The Regents of the University of California. All rights reserved.  
  
FreeBSD 5.2.1-RELEASE (GENERIC) #0: Mon Feb 23 20:45:55 GMT 2004  
  
Welcome to FreeBSD!  
  
A jury consists of 12 persons chosen to decide  
who has the better lawyer.  
-- Robert Frost  
>
```

Tomáš Brček, ID:120761

Cvičenie: Pondelok 17:00

`ssh -L 9090:localhost:9090 -oKexAlgorithms=diffie-hellman-group-exchange-sha1 -oHostKeyAlgorithms=+ssh-dss -c aes128-cbc brcek22@student.fiit.stuba.sk`

- tento príkaz som spustil na mojom počítači
- tento príkaz vytvoril tunel medzi mojim počítačom a serverom student.fiit.stuba.sk



```
tomas@tomas-ThinkBook-15-G2-ITL: ~  
tomas@tomas-ThinkBook-15-G2-ITL:~$ ssh -L 9090:localhost:9090 -oKexAlgorithms=diffie-hellman-group-exchange-sha1 -oHostKeyAlgorithms=+ssh-dss -c aes128-cbc brcek22@student.fiit.stuba.sk  
(brcek22@student.fiit.stuba.sk) Password:  
Last login: Mon Oct 21 18:31:36 2024 from 147.175.163.35  
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994  
The Regents of the University of California. All rights reserved.  
  
FreeBSD 5.2.1-RELEASE (GENERIC) #0: Mon Feb 23 20:45:55 GMT 2004  
  
Welcome to FreeBSD!  
  
Pecor's Health-Food Principle:  
Never eat rutabaga on any day of the week that has a "y" in  
it.  
>
```

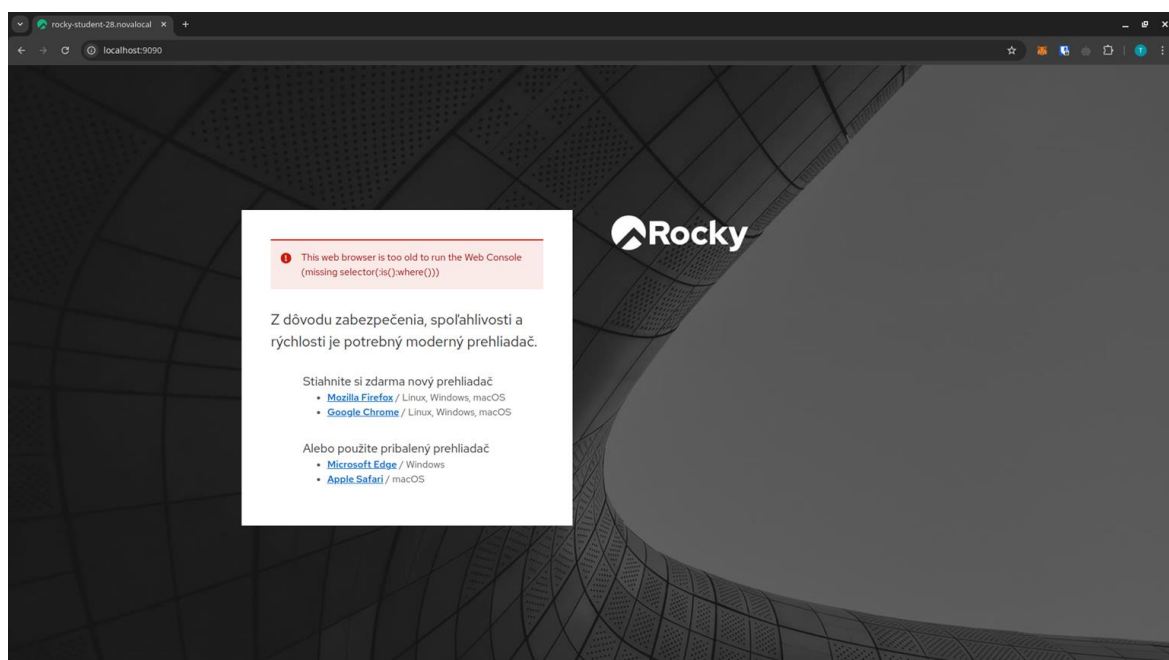
Vďaka týmto 2 tunelom som schopný pripojiť sa z môjho počítača na webovú konzolu cockpit, ktorá beží na rocky linuxe.

- Demonštruje správnu funkčnosť tunelu.

Do webového prehliadača na mojom počítači som zadal adresu:

<http://localhost:9090>

A v prehliadači mi načítalo stránku.



- Detailne vysvetlite fungovanie a význam takéhoto presmerovania.

Takéto SSH tunelovanie funguje tak, že prostredníctvom šifrovaného spojenia zabezpečí prístup k službám, ktoré nie sú priamo dostupné z verejnej siete. V tomto prípade umožňuje prístup k webovej konzole „Cockpit“ na virtuálnom stroji, ktorý je za NAT a nemá verejnú IP adresu.

Fungovanie:

SSH tunel vytvorí šifrovaný kanál medzi vaším počítačom a serverom, ku ktorému máte prístup (v tomto prípade student.fiit.stuba.sk). Okrem tohto kanála sa vytvára aj druhý šifrovaný kanál medzi daným serverom a virtuálnym strojom (rocky linux). Po vytvorení tunelov sa pripojenie na verejný server presmeruje na port, ktorý komunikáciu presmeruje na port virtuálneho stroja, kde beží „Cockpit“. To znamená, že keď na svojom počítači zadám `http://localhost:9090`, SSH spojenie presmeruje túto požiadavku na port 9090 na serveri, čo ďalej prepošle na port 9090 na virtuálnom stroji.

Význam:

Presmerovanie cez SSH tunel poskytuje bezpečnosť, pretože všetky dáta sú šifrované, čo chráni pred odpočúvaním. Zároveň umožňuje zjednodušený prístup k službám vo vnútornej sieti (ako je „Cockpit“) z vonkajšej siete.