ENCRYPTION IN LINUX

WHAT WILL WE USE?

- **UBUNTU**
- **A program called SeaHorse**
- We'll let's say that's it for now…

Ubuntu Hardening…

Keep System Up-To-Date

- apt-get update && apt-get upgrade

Check for Accounts with Empty Passwords

- cat /etc/shadow | awk -F: '($2==""){print $1}'

IpTables

- iptables -A INPUT -p tcp -m tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
- iptables -A INPUT -p tcp -m tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
- iptables -A INPUT -I lo -j ACCEPT
- iptables -A INPUT -j DROP
- (Or use iptables -P INPUT DROP to automatically drop all packets without a rule)

Disable root Login !!!

- PermitRootLogin no

Check for Rootkits !!!

- apt-get install rkhunter

  rkhunter -C

ENCRYPTION USING PGP KEYS

- OK for **ENCRYPTION**… but what are **PGP KEYS**?
  - ➢ Well **PGP** means **Pretty Good Privacy**…

- **NO KIDDING.**

They even have a Logo...

PRETTY GOOD PRIVACY

ORIGINAL AUTHOR(S): PHIL ZIMMERMANN

(PGP INC. NETWORK ASSOCIATES PGP CORP)

DEVELOPER(S): SYMANTEC

INITIAL RELEASE: 1991

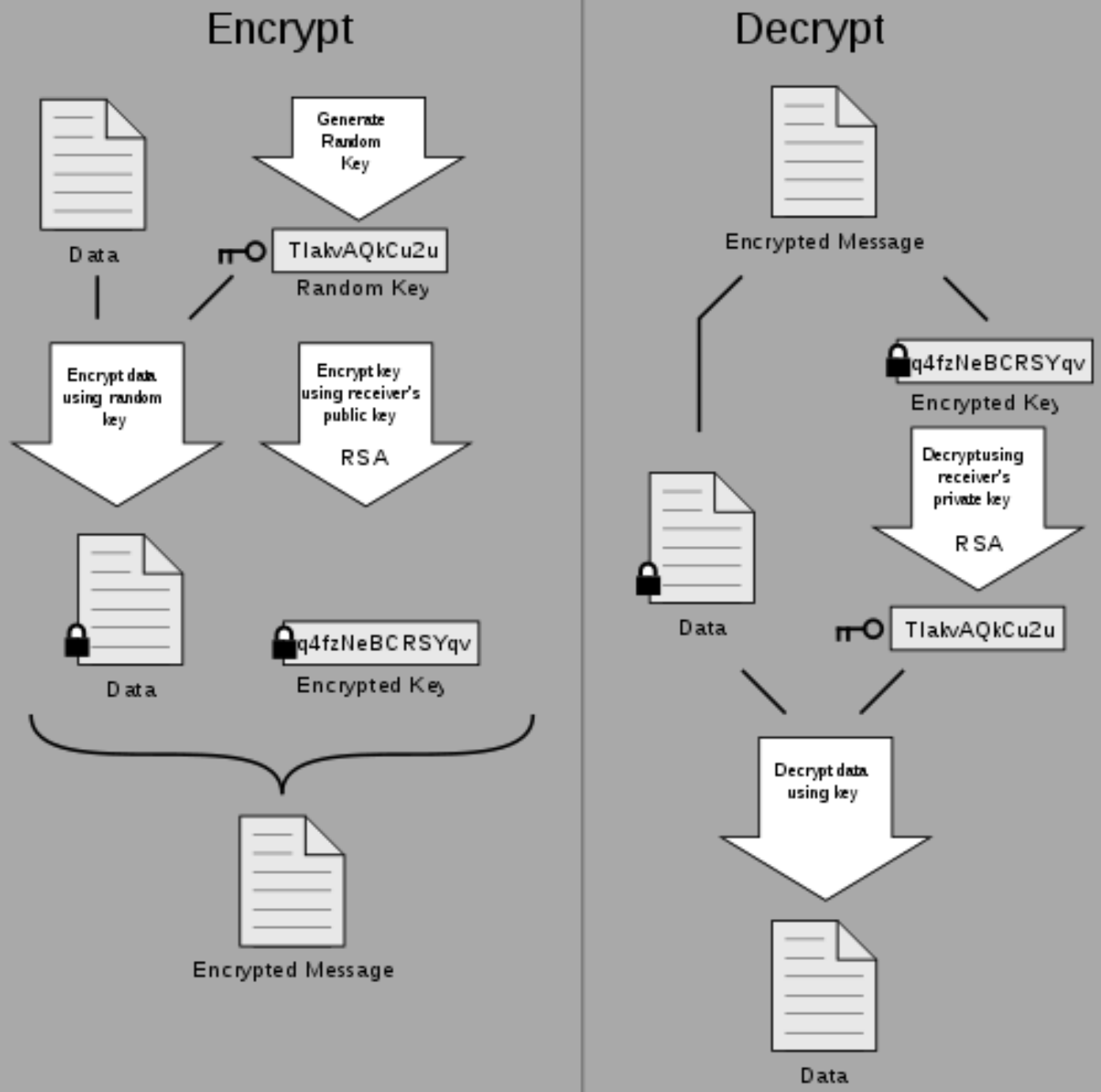
TYPE: ENCRYPTION SOFTWARE

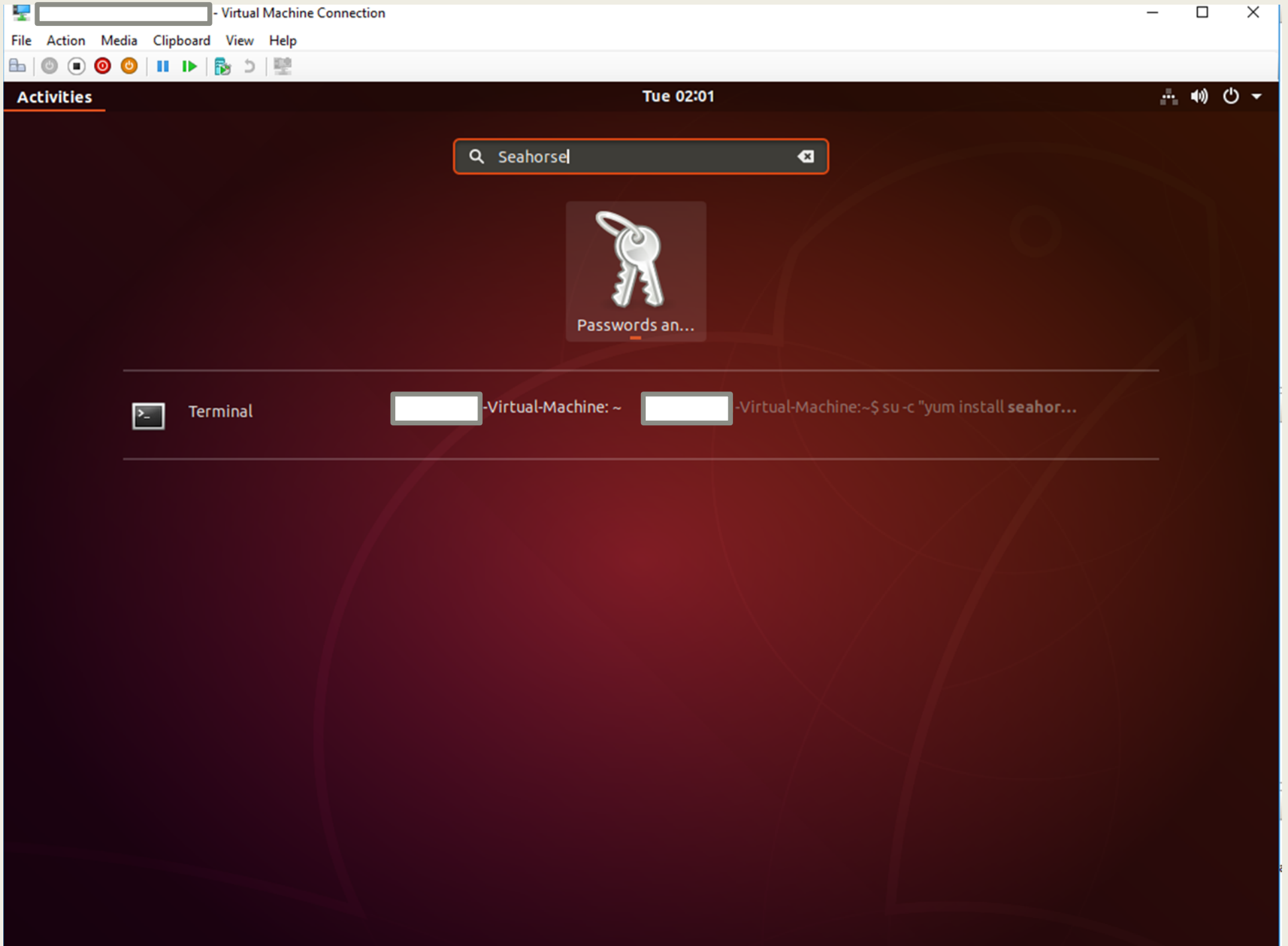
WEBSITE: WWW.PGP.COM

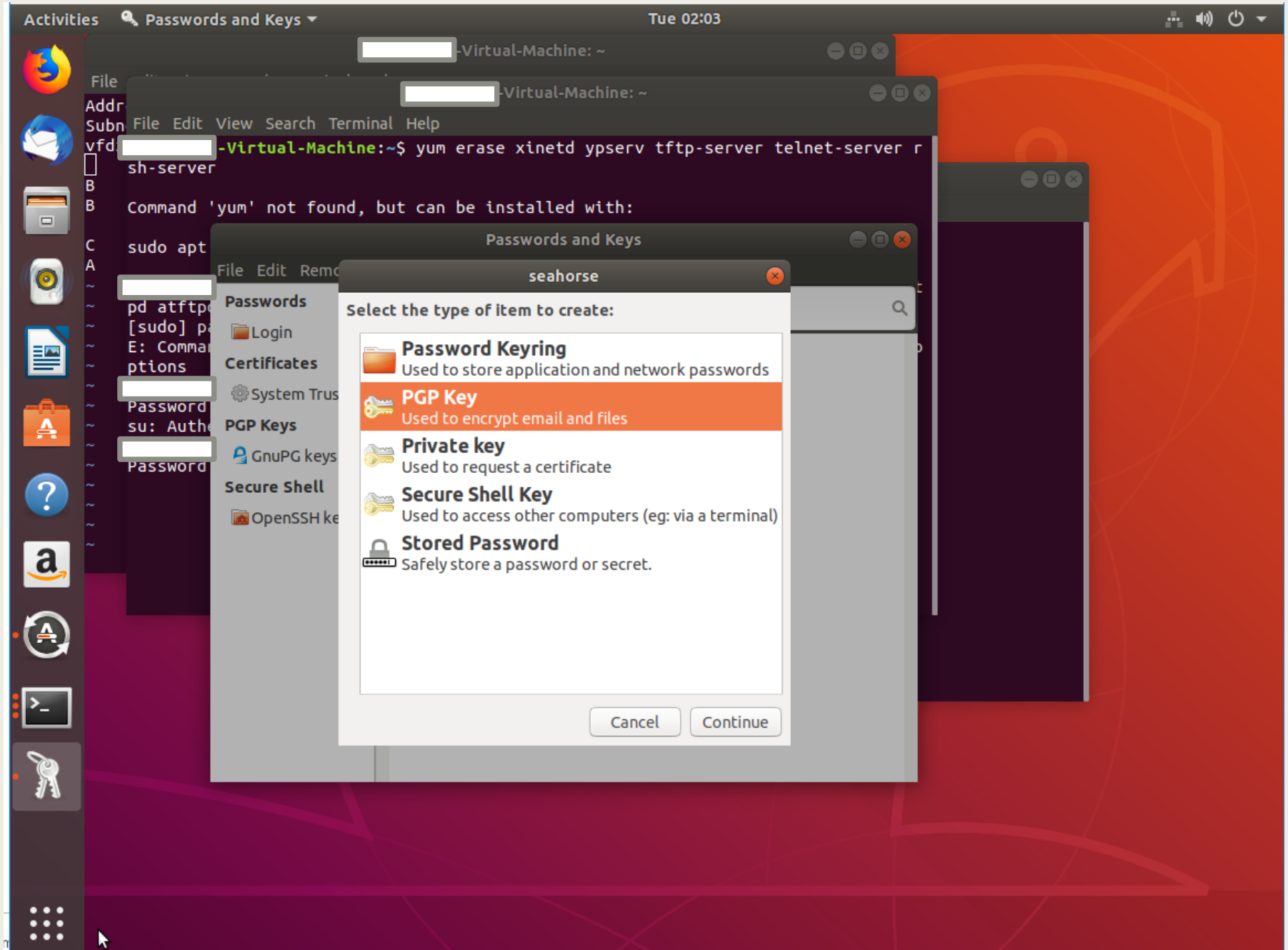
So PGP helps you to send messages securely.

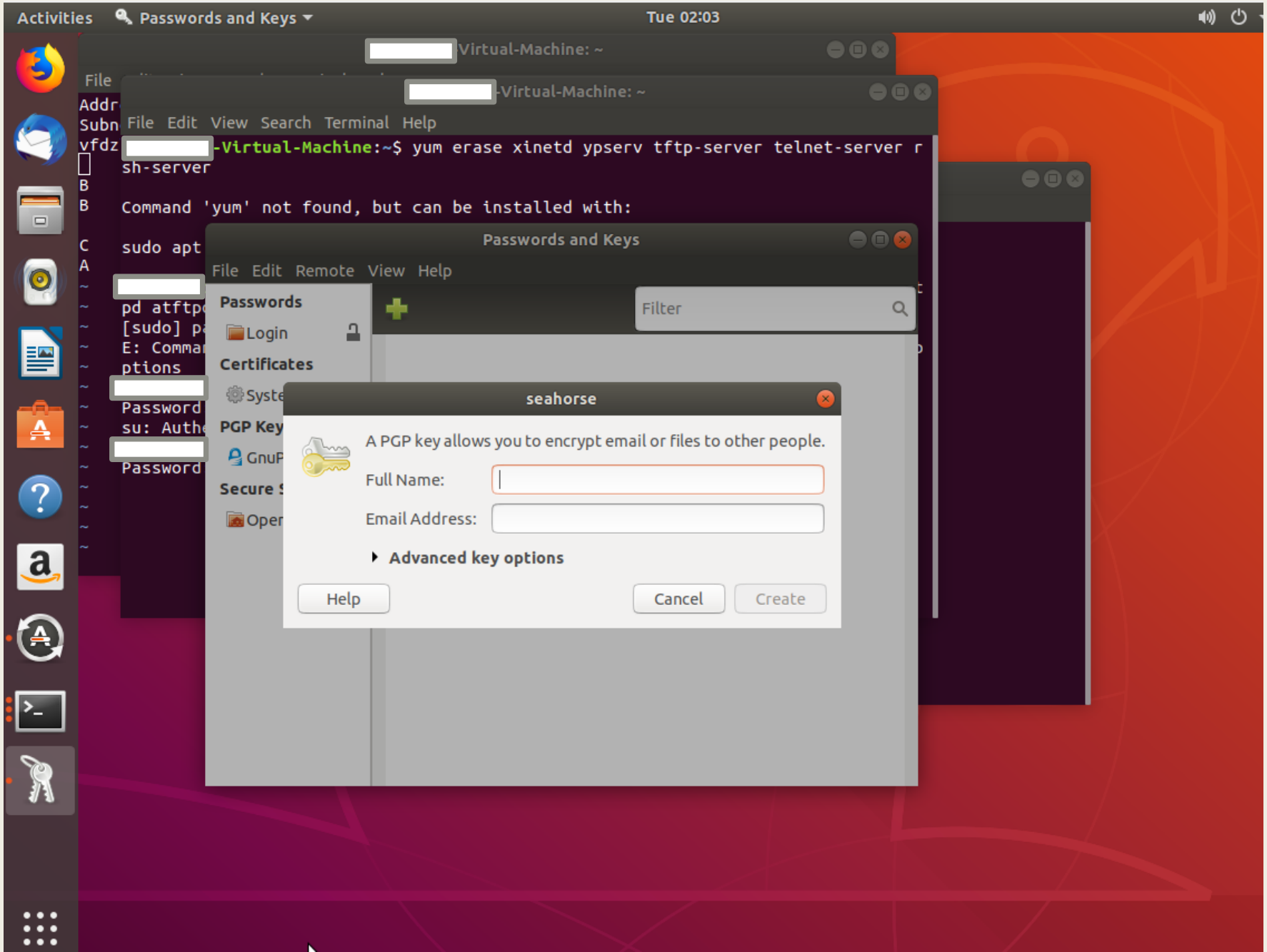
PGP create a pair of keys:
A public one to encrypt
A private one to decrypt

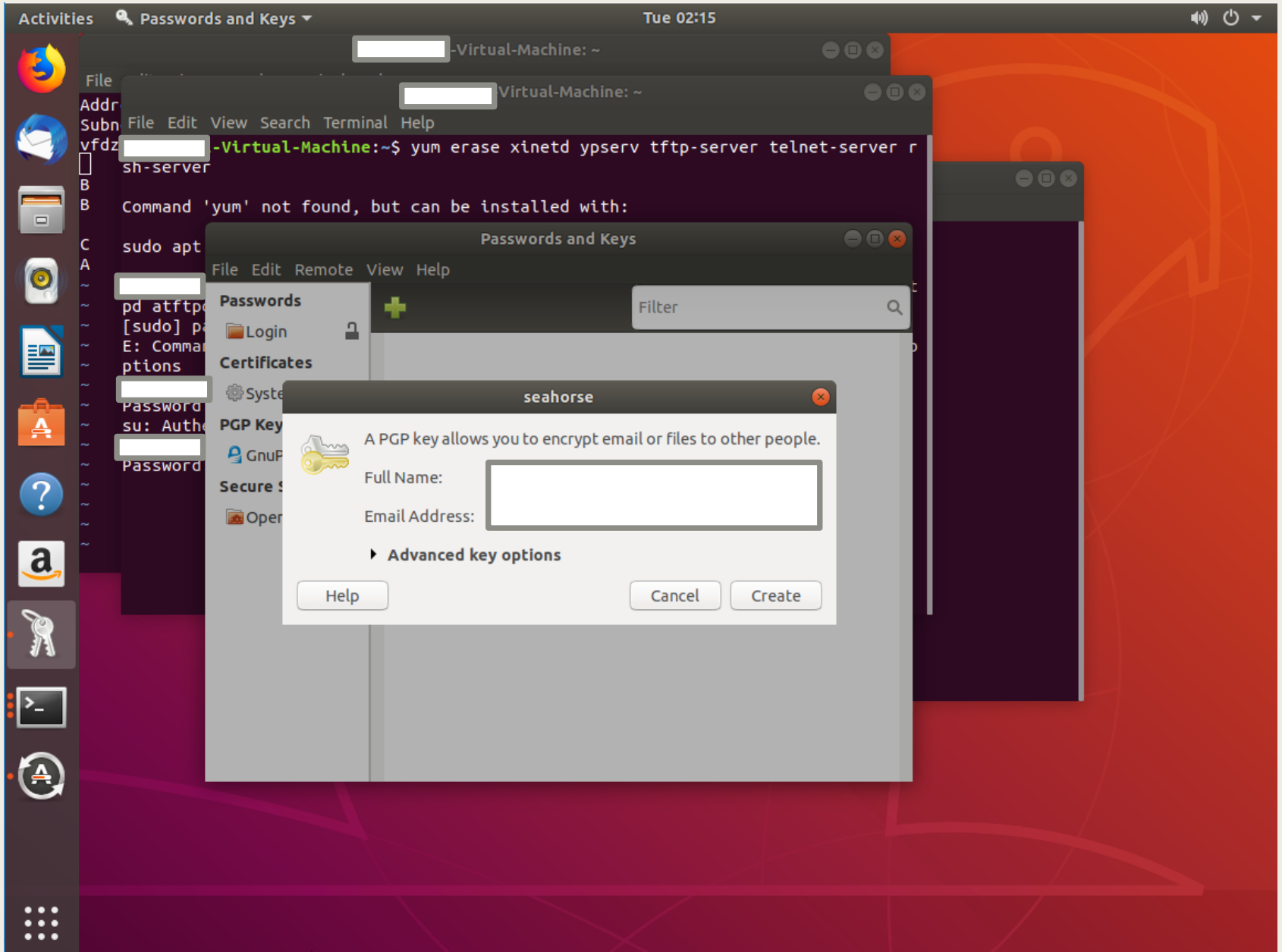
…SIMPLE RIGTH ?

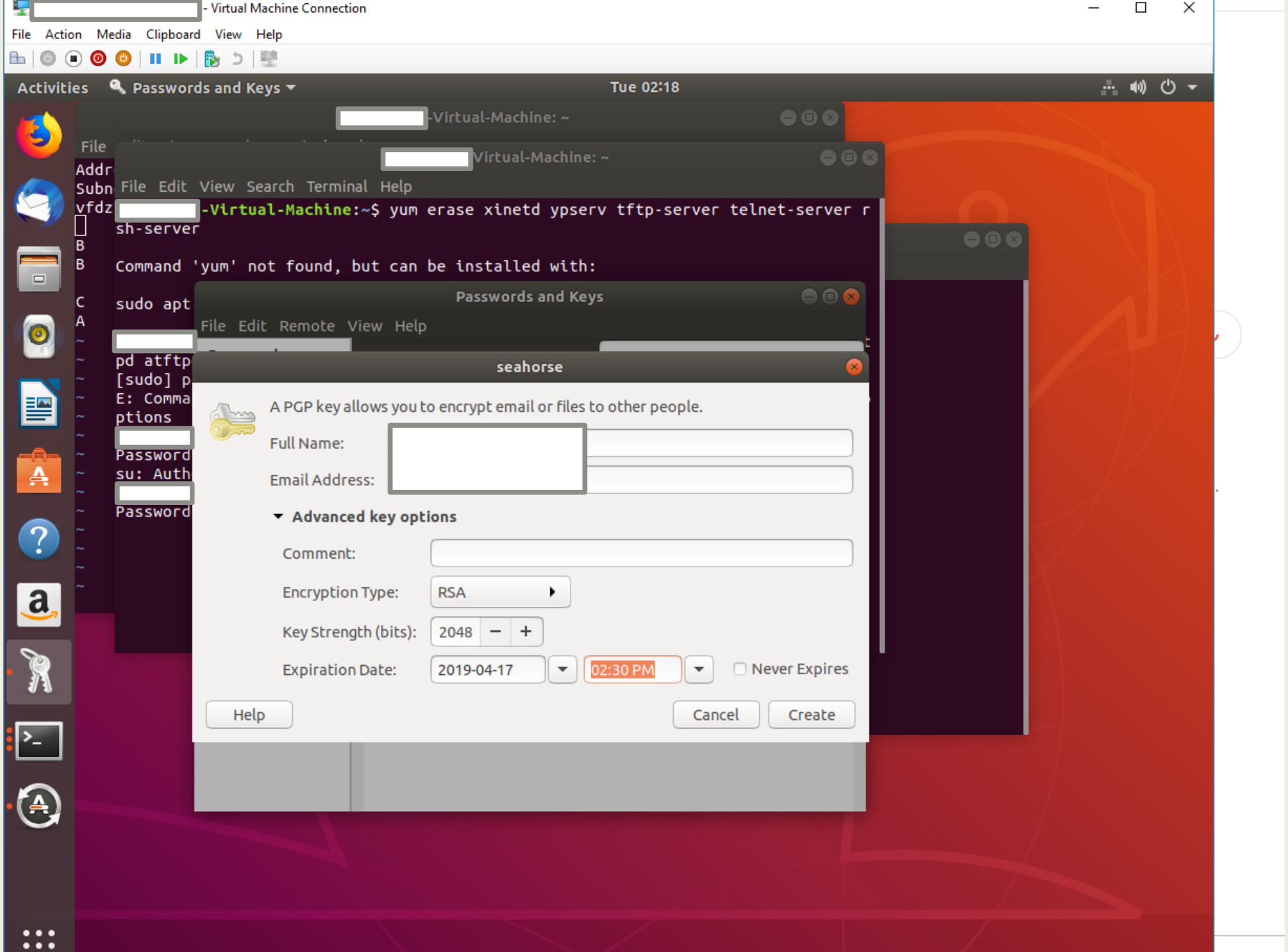

Encrypt
Data
Generate Random Key
TIakvAQkCu2u
Random Key
Encrypt data using random key
Encrypt key using receiver's public key
RSA
Data
q4fzNeBCRSYqv
Encrypted Key
Encrypted Message
Decrypt
Encrypted Message
q4fzNeBCRSYqv
Encrypted Key
Decrypt using receiver's private key
RSA
Data
TIakvAQkCu2u
Decrypt data using key
Data

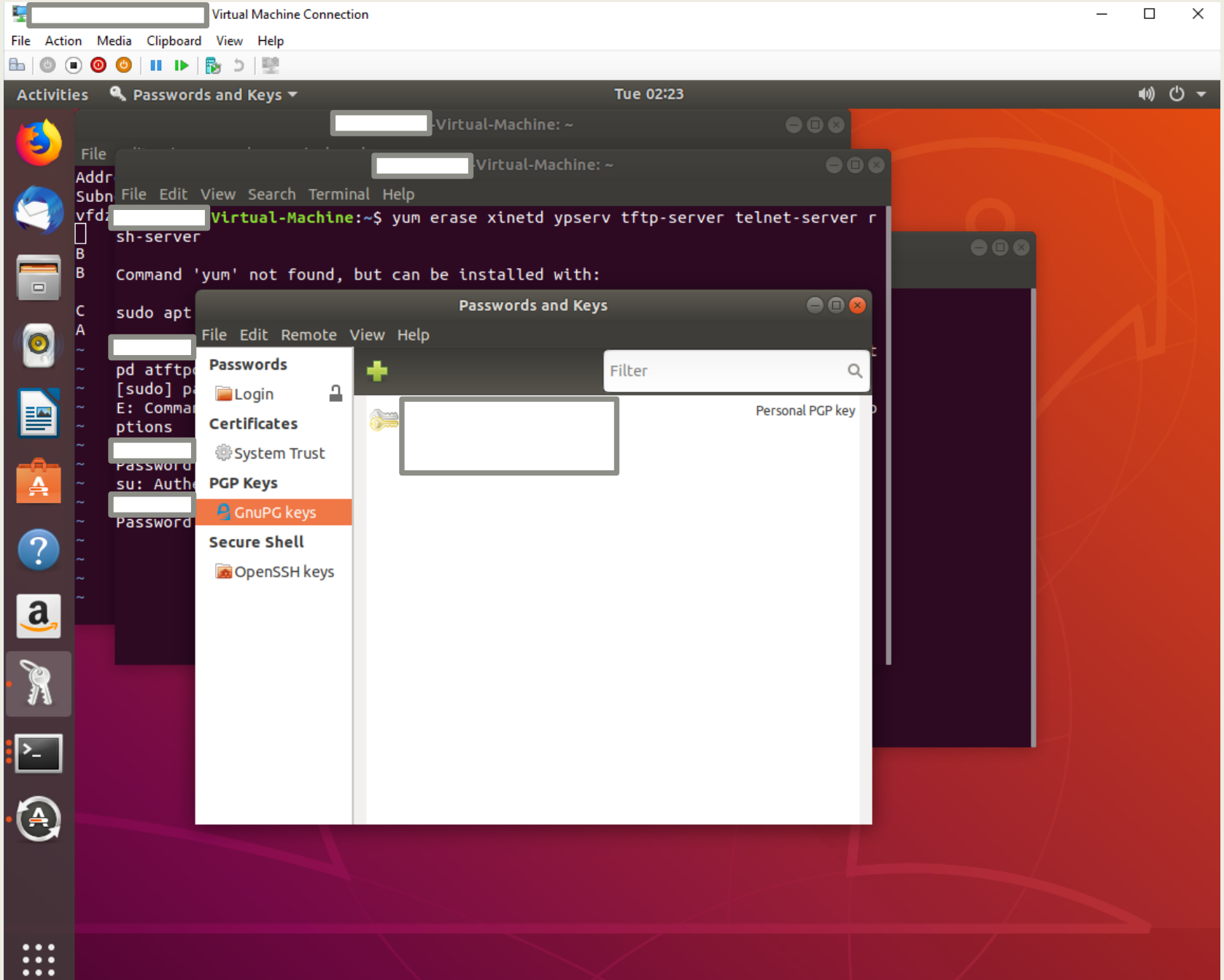

[redacted] - Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Tue 02:01
Seahorse
Passwords an...
Terminal
[redacted]-Virtual-Machine: ~
[redacted]-Virtual-Machine:~$ su -c "yum install seahor...

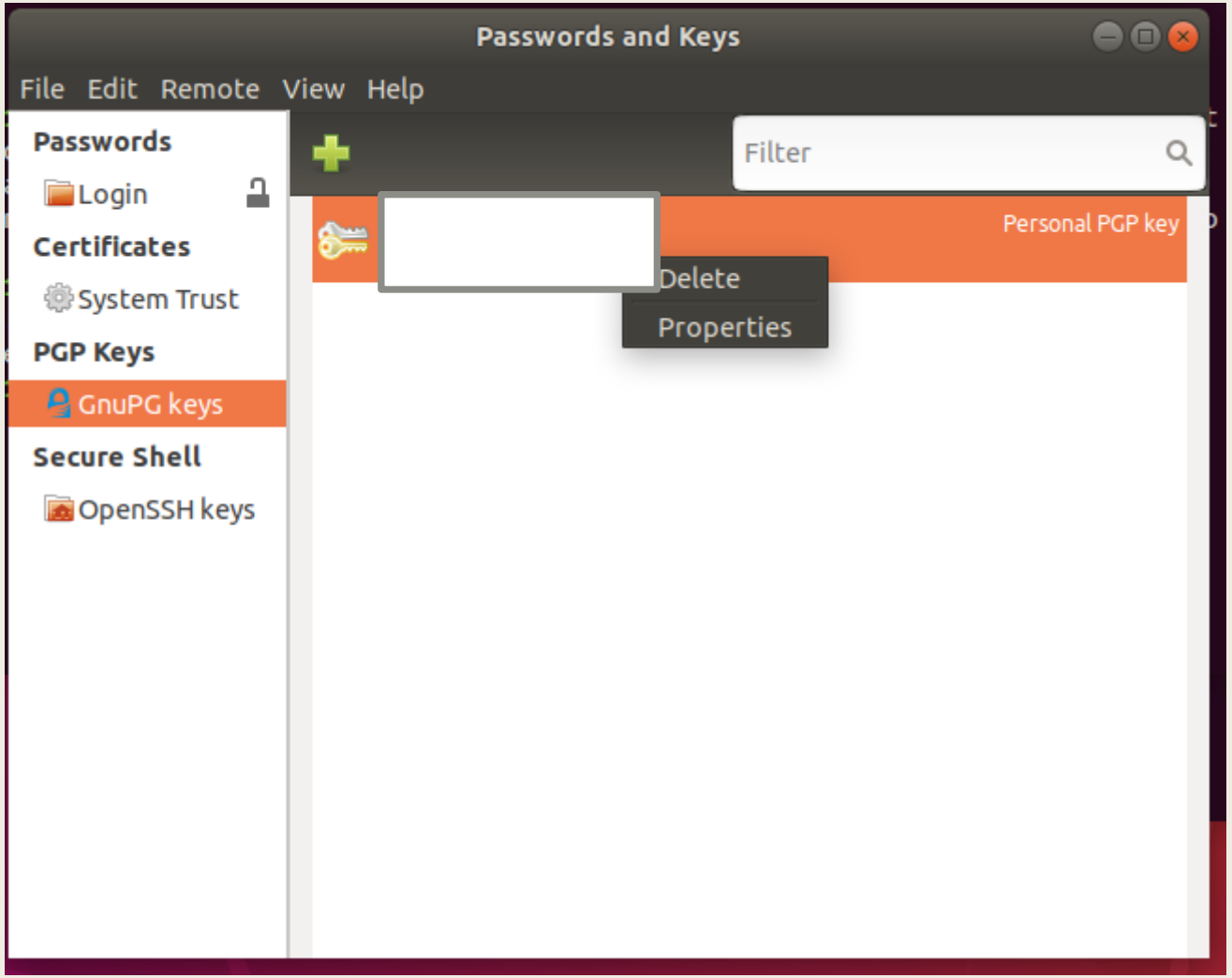

Activities
Passwords and Keys
Tue 02:03
-Virtual-Machine: ~
File Edit View Search Terminal Help
-Virtual-Machine:~$ yum erase xinetd ypserv tftp-server telnet-server r
sh-server
Command 'yum' not found, but can be installed with:
sudo apt
Passwords and Keys
File Edit Remo
Passwords
Login
Certificates
System Trus
PGP Keys
GnuPG keys
Secure Shell
OpenSSH ke
seahorse
Select the type of item to create:
Password Keyring
Used to store application and network passwords
PGP Key
Used to encrypt email and files
Private key
Used to request a certificate
Secure Shell Key
Used to access other computers (eg: via a terminal)
Stored Password
Safely store a password or secret.
Cancel
Continue

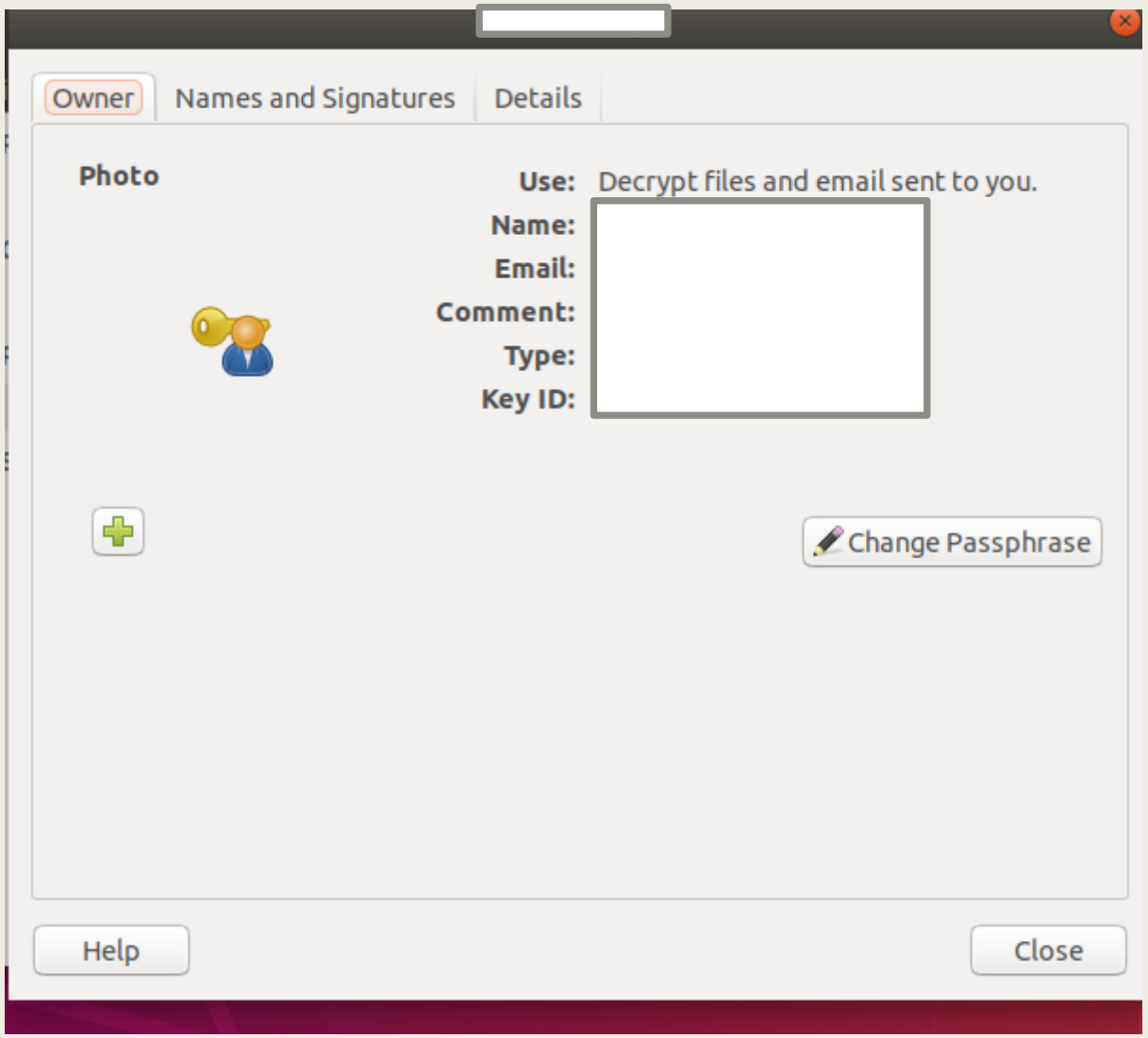

Activities
Passwords and Keys
Tue 02:03
Virtual-Machine: ~
File Edit View Search Terminal Help
-Virtual-Machine:~$ yum erase xinetd ypserv tftp-server telnet-server r
sh-server
Command 'yum' not found, but can be installed with:
sudo apt
Passwords and Keys
File Edit Remote View Help
Passwords
Login
Certificates
PGP Key
Secure
Filter
seahorse
A PGP key allows you to encrypt email or files to other people.
Full Name:
Email Address:
Advanced key options
Help
Cancel
Create

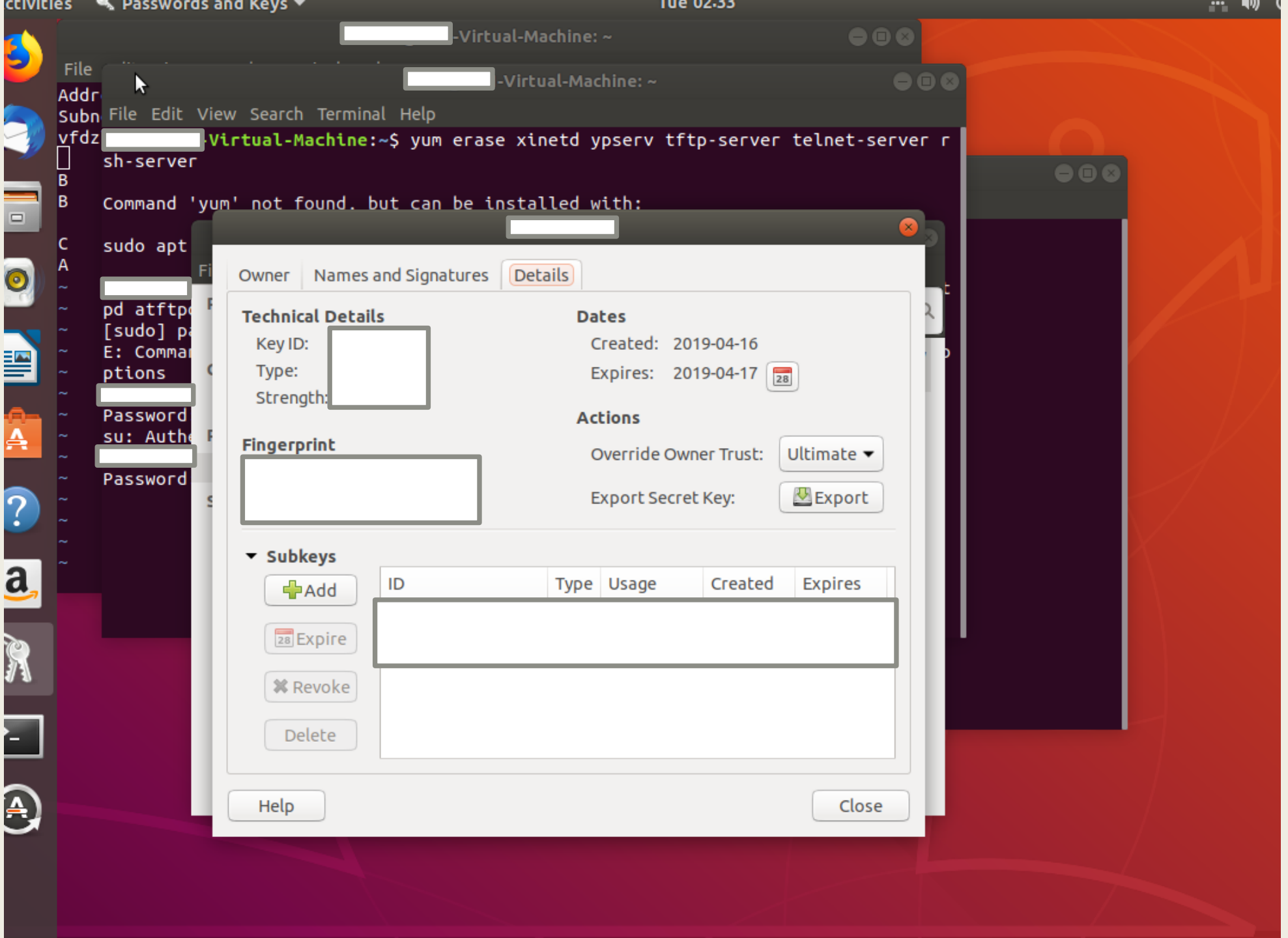

Activities
Passwords and Keys
Tue 02:15
-Virtual-Machine: ~
File Edit View Search Terminal Help
-Virtual-Machine:~$ yum erase xinetd ypserv tftp-server telnet-server r
sh-server
Command 'yum' not found, but can be installed with:
sudo apt
Passwords and Keys
File Edit Remote View Help
Passwords
Login
Certificates
PGP Key
Secure
Filter
seahorse
A PGP key allows you to encrypt email or files to other people.
Full Name:
Email Address:
Advanced key options
Help
Cancel
Create

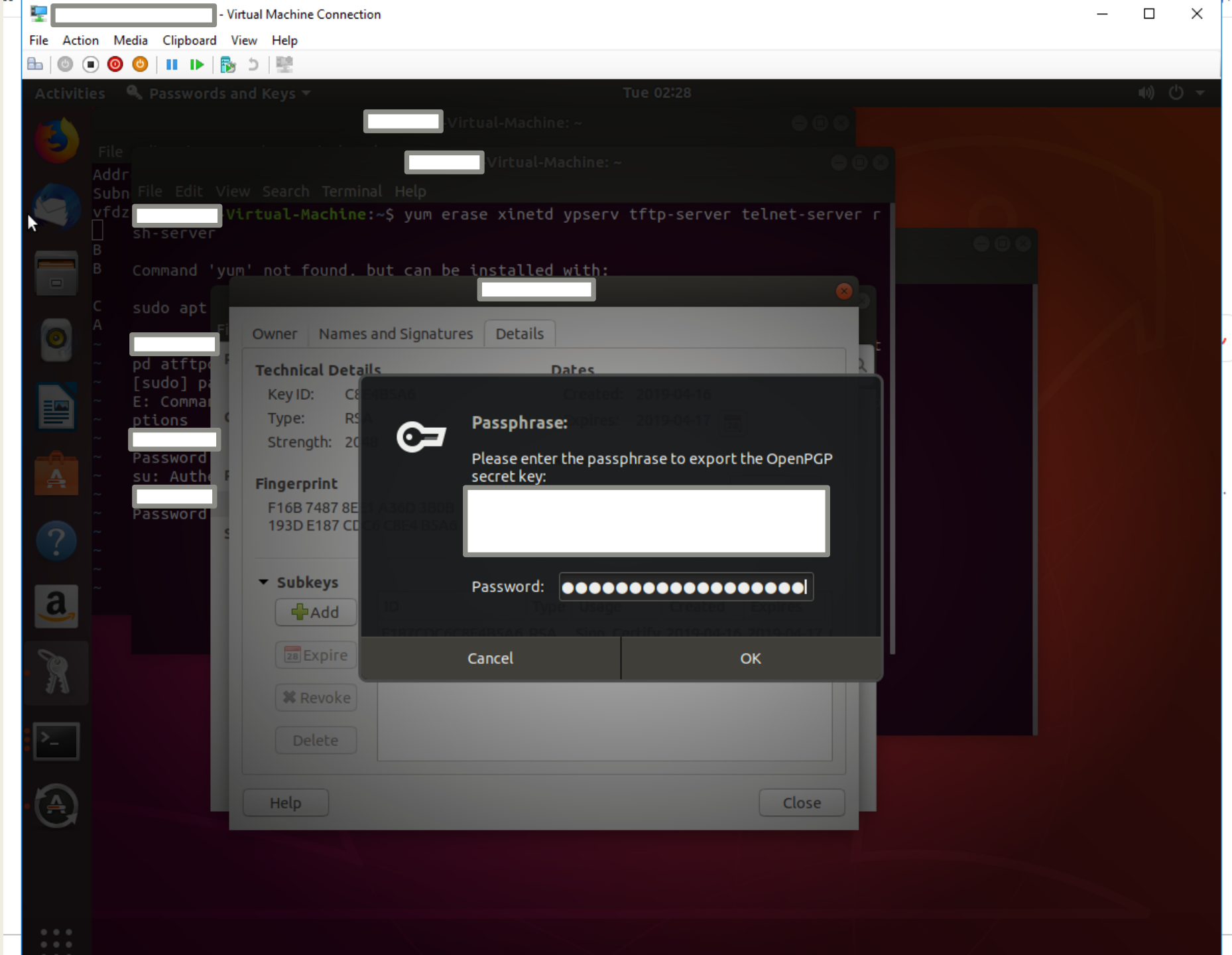

- Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Passwords and Keys
Tue 02:18
-Virtual-Machine: ~
File Edit View Search Terminal Help
-Virtual-Machine:~$ yum erase xinetd ypserv tftp-server telnet-server r
sh-server
Command 'yum' not found, but can be installed with:
sudo apt
Passwords and Keys
File Edit Remote View Help
seahorse
A PGP key allows you to encrypt email or files to other people.
Full Name:
Email Address:
Advanced key options
Comment:
Encryption Type:
RSA
Key Strength (bits):
2048
Expiration Date:
2019-04-17
02:30 PM
Never Expires
Help
Cancel
Create

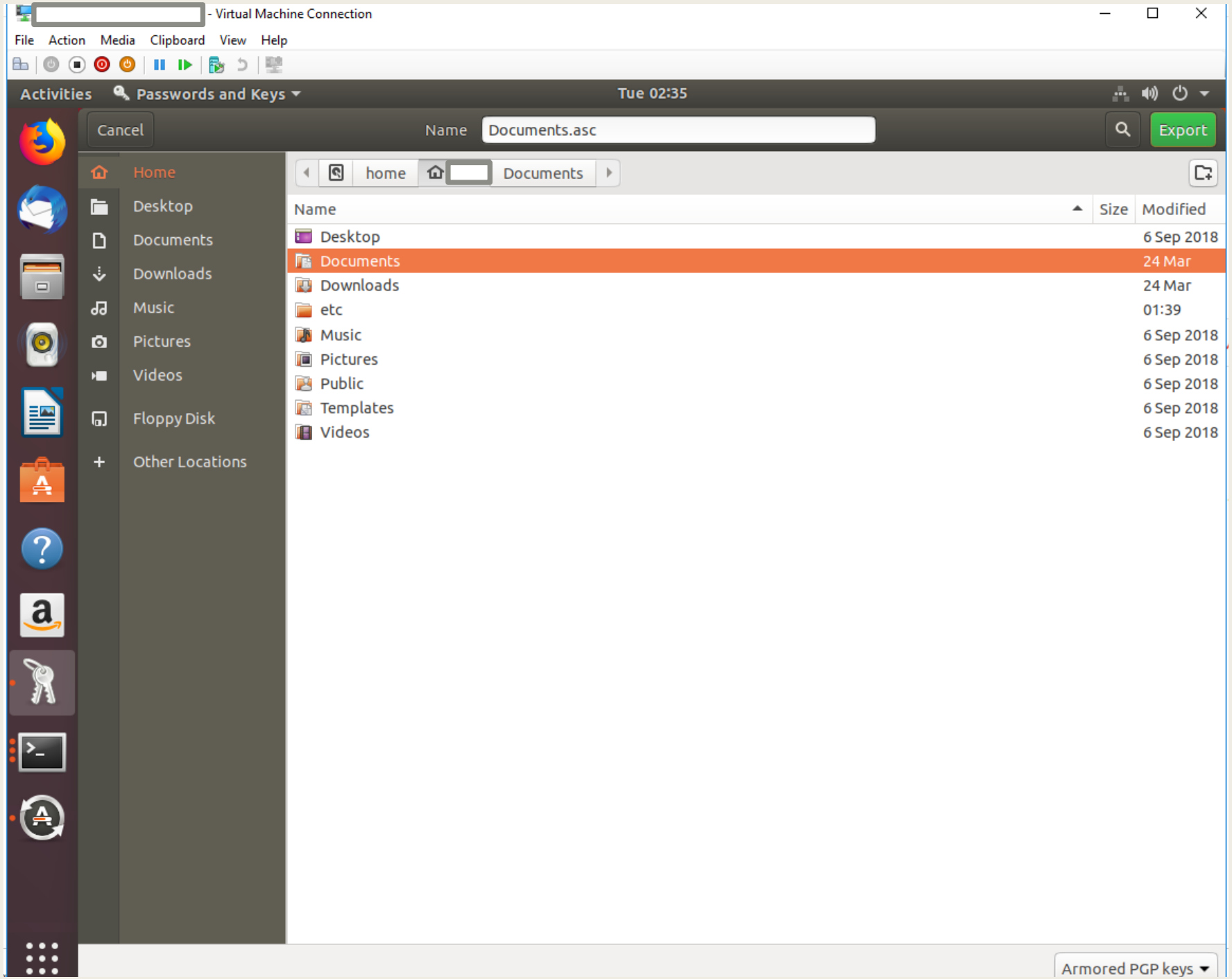

Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Passwords and Keys
Tue 02:23
Virtual-Machine: ~
File Edit View Search Terminal Help
Virtual-Machine:~$ yum erase xinetd ypserv tftp-server telnet-server r
sh-server
Command 'yum' not found, but can be installed with:
sudo apt
Passwords and Keys
File Edit Remote View Help
Passwords
Login
Certificates
System Trust
PGP Keys
GnuPG keys
Secure Shell
OpenSSH keys
Filter
Personal PGP key

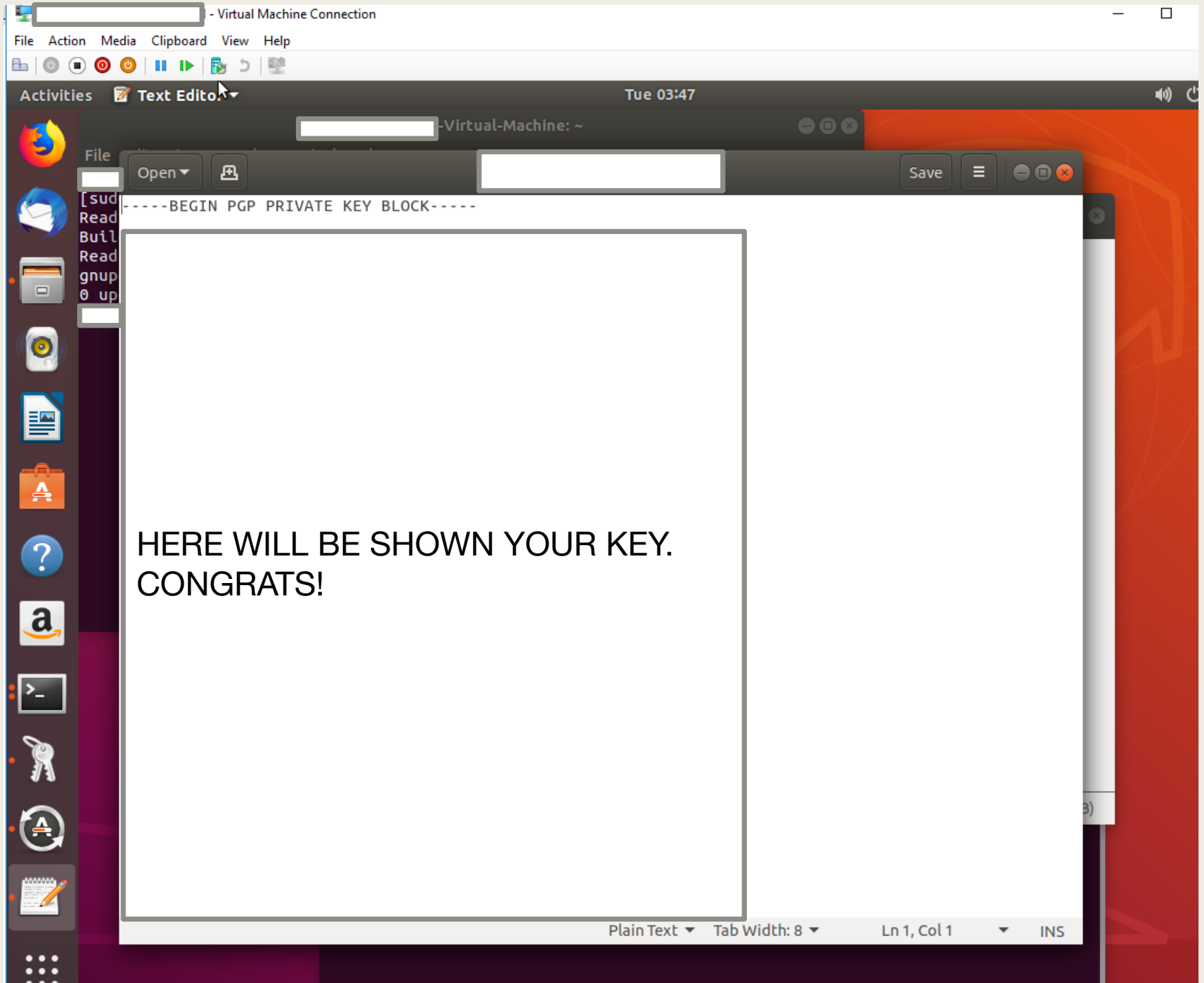

Passwords and Keys
File Edit Remote View Help
Passwords
Login
Certificates
System Trust
PGP Keys
GnuPG keys
Secure Shell
OpenSSH keys
Filter
Personal PGP key
Delete
Properties


Owner
Names and Signatures
Details
Photo
Use:
Decrypt files and email sent to you.
Name:
Email:
Comment:
Type:
Key ID:
Change Passphrase
Help
Close


Passwords and Keys
Tue 02:33
-Virtual-Machine: ~
File Edit View Search Terminal Help
-Virtual-Machine:~$ yum erase xinetd ypserv tftp-server telnet-server r
sh-server
Command 'yum' not found, but can be installed with:
sudo apt
Owner
Names and Signatures
Details
Technical Details
Key ID:
Type:
Strength:
Dates
Created: 2019-04-16
Expires: 2019-04-17
Actions
Override Owner Trust:
Ultimate
Export Secret Key:
Export
Fingerprint
Subkeys
Add
Expire
Revoke
Delete
ID
Type
Usage
Created
Expires
Help
Close


- Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Passwords and Keys
Tue 02:28
Virtual-Machine: ~
File Edit View Search Terminal Help
Virtual-Machine:~$ yum erase xinetd ypserv tftp-server telnet-server r
sh-server
Command 'yum' not found, but can be installed with:
sudo apt
Owner
Names and Signatures
Details
Technical Details
Dates
Key ID:
Type:
Strength:
Fingerprint
Subkeys
Add
Expire
Revoke
Delete
Help
Close
Passphrase:
Please enter the passphrase to export the OpenPGP secret key:
Password:
Cancel
OK


- Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Passwords and Keys
Tue 02:35
Cancel
Name
Documents.asc
Export
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Floppy Disk
Other Locations
home
Documents
Name
Size
Modified
Desktop 6 Sep 2018
Documents 24 Mar
Downloads 24 Mar
etc 01:39
Music 6 Sep 2018
Pictures 6 Sep 2018
Public 6 Sep 2018
Templates 6 Sep 2018
Videos 6 Sep 2018
Armored PGP keys


- Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Text Editor
Tue 03:47
-Virtual-Machine: ~
File
Open
Save
-----BEGIN PGP PRIVATE KEY BLOCK-----
HERE WILL BE SHOWN YOUR KEY.
CONGRATS!
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

YOU HAVE AN ENCRYPTION KEY...GREAT! SO WHAT'S NEXT???

First, you can share it with those you trust (THE PUBLIC ONE ONLY)

```
gpg2 --export --armor [          ]@example.com > [          ]-pubkey.asc
```

Or You Can Keep It Safe!

https://www.yubico.com/products/yubikey-5-overview/

https://blog.josefsson.org/2014/06/23/offline-gnupg-master-key-and-subkeys-on-yubikey-neo-smartcard/

CONCLUSION

- ENCRYPTION SEEMS HARD BUT ONCE YOU FIGURE IT OUT IT'S FUN!
- YES, LINUX IS AN OPEN-SOURCE SOFTWARE, BUT YOU STILL HAVE SOME OS HARDENING TO DO!
- THAT'S IT, HAVE FUN ENCRYPTING! (HOPEFULLY)

RESOURCES

https://www.nuharborsecurity.com/ubuntu-server-hardening-guide-2/

http://pgp.mit.edu/

https://fedoraproject.org/wiki/Creating_GPG_Keys#Safeguarding