

Question 2.1:

Installation of gnupg:

```
root@fedora:~  
[root@fedora ~]# yum -y install gnupg  
Fedora 36 - x86_64                36 kB/s | 24 kB    00:00  
Fedora Modular 36 - x86_64        41 kB/s | 23 kB    00:00  
Fedora 36 - x86_64 - Updates      199 kB/s | 4.5 MB  00:23  
Fedora Modular 36 - x86_64 - Updates 39 kB/s | 23 kB    00:00  
Fedora Modular 36 - x86_64 - Updates 20 kB/s | 39 kB    00:02  
Package gnupg2-2.3.4-2.fc36.x86_64 is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[root@fedora ~]#
```

Question 2.2:

Generate the GPG Key Pair:

```
gpg: directory '/root/.gnupg' created  
gpg: keybox '/root/.gnupg/pubring.kbx' created  
Note: Use "gpg --full-generate-key" for a full featured key generation dialog.  
  
GnuPG needs to construct a user ID to identify your key.  
  
Real name: nazimz  
Email address: nazerrouki@gmail.com  
You selected this USER-ID:  
    "nazimz <nazerrouki@gmail.com>"  
  
Change (N)ame, (E)mail, or (O)kay/(Q)uit? o  
We need to generate a lot of random bytes. It is a good idea to perform  
some other action (type on the keyboard, move the mouse, utilize the  
disks) during the prime generation; this gives the random number  
generator a better chance to gain enough entropy.  
We need to generate a lot of random bytes. It is a good idea to perform  
some other action (type on the keyboard, move the mouse, utilize the  
disks) during the prime generation; this gives the random number  
generator a better chance to gain enough entropy.  
gpg: /root/.gnupg/trustdb.gpg: trustdb created  
gpg: directory '/root/.gnupg/openpgp-revocs.d' created  
gpg: revocation certificate stored as '/root/.gnupg/openpgp-revocs.d/B7C686D87A1FA1AB8AF2C59E7ADAAAD2DD934B63.rev'  
public and secret key created and signed.  
  
pub   ed25519 2022-11-19 [SC] [expires: 2024-11-18]  
       B7C686D87A1FA1AB8AF2C59E7ADAAAD2DD934B63  
uid           nazimz <nazerrouki@gmail.com>  
sub   cv25519 2022-11-19 [E] [expires: 2024-11-18]  
[root@fedora ~]#
```

Question 2.2.1:

As shown above, the newly generated public key pair can be found in the /root/.gnupg directory.

Question 2.3:

Signing a document with my certificate:

```
[root@fedora /]# nano document.txt
[root@fedora /]# gpg2 --sign document.txt
File 'document.txt.gpg' exists. Overwrite? (y/N) █
```

Verifying the signature using the public key:

```
[root@fedora /]# gpg2 --verify document.txt.gpg
gpg: Signature made Fri 18 Nov 2022 06:30:33 PM PST
gpg: using EDDSA key B7C686D87A1FA1AB8AF2C59E7ADAAAD2DD934B63
gpg: Good signature from "nazimz <nazerrouki@gmail.com>" [ultimate]
[root@fedora /]# █
```

Question 2.4:

Export Public Key:

```
[root@fedora .gnupg]# gpg2 --export -a B7C686D87A1FA1AB8AF2C59E7ADAAAD2DD934B63
> pgp_pub_key.asc
[root@fedora .gnupg]# ls
openpgp-revocs.d  private-keys-v1.d  pubring.kbx~
pgp_pub_key.asc   pubring.kbx        trustdb.gpg
[root@fedora .gnupg]#
```

Copy Public Key to Client:

```
[root@fedora .gnupg]# scp pgp_pub_key.asc root@10.0.2.15:/
root@10.0.2.15's password:
pgp_pub_key.asc                                100% 656    1.6MB/s   00:00
[root@fedora .gnupg]# █
```

Question 2.4.1:

You can extract the private key by using: `gpg --export-secret-keys`, command.

Import Private Key on Client:

```
root@fedora: /  
[root@fedora /]# ls  
afs boot etc lib lost+found mnt proc run srv tmp var  
bin dev home lib64 media opt root sbin sys usr  
[root@fedora /]# sudo dnf install gnupg  
Last metadata expiration check: 0:04:45 ago on Fri 18 Nov 2022 06:44:06 PM PST.  
Package gnupg2-2.3.4-2.fc36.x86_64 is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[root@fedora /]# cd /root/gnupg  
-bash: cd: /root/gnupg: No such file or directory  
[root@fedora /]# cd /root/.gnupg  
-bash: cd: /root/.gnupg: No such file or directory  
[root@fedora /]# ls  
afs boot etc lib lost+found mnt proc run srv tmp var  
bin dev home lib64 media opt root sbin sys usr  
[root@fedora /]# gpg2 --import pgp_pub_key.asc  
gpg: directory '/root/.gnupg' created  
gpg: keybox '/root/.gnupg/pubring.kbx' created  
gpg: /root/.gnupg/trustdb.gpg: trustdb created  
gpg: key 7ADAAAD2DD934B63: public key "nazimz <nazerrouki@gmail.com>" imported  
gpg: Total number processed: 1  
gpg: imported: 1  
[root@fedora /]#
```

Encrypt with Client using Exported Public Key:

```
[root@fedora /]# gpg2 --encrypt document.txt  
You did not specify a user ID. (you may use "-r")  
  
Current recipients:  
  
Enter the user ID. End with an empty line: nazimz  
gpg: 213087019299A04D: There is no assurance this key belongs to the named user  
  
sub cv25519/213087019299A04D 2022-11-19 nazimz <nazerrouki@gmail.com>  
Primary key fingerprint: B7C6 86D8 7A1F A1AB 8AF2 C59E 7ADA AAD2 DD93 4B63  
Subkey fingerprint: 6E1E AB2F F7DF ED8E ED7E 6D4D 2130 8701 9299 A04D  
  
It is NOT certain that the key belongs to the person named  
in the user ID. If you *really* know what you are doing,  
you may answer the next question with yes.  
  
Use this key anyway? (y/N) y  
  
Current recipients:  
cv25519/213087019299A04D 2022-11-19 "nazimz <nazerrouki@gmail.com>"
```

Question 2.4.2:

Yes, because the public key from the digital certificate is shared across both the server and client as shown above.

Question 2.4.3:

You can register your PGP keys using: `gpg2 --gen-key`

In the case of the client, our public key was registered when the server sent it via ssh protocol.

Question 2.4.4:

You can delete the pgp keys using `gpg --delete-key KEYID`

This can apply to multiple keys as well.

Question 3.1:

Installation of John the Ripper:

```
[root@fedora ~]# yum -y install john
Last metadata expiration check: 1:34:01 ago on Fri 18 Nov 2022 06:22:35 PM PST.
Dependencies resolved.
=====
Package            Architecture      Version           Repository        Size
=====
Installing:
john               x86_64            1.8.0-20.fc36     fedora            8.9 M
=====
Transaction Summary
=====
Install 1 Package

Total download size: 8.9 M
Installed size: 20 M
Downloading Packages:
john-1.8.0-20.fc36.x86_64.rpm                  1.5 MB/s | 8.9 MB    00:05
-----
Total                                           1.4 MB/s | 8.9 MB    00:06
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing     : john-1.8.0-20.fc36.x86_64      1/1
  Running scriptlet: john-1.8.0-20.fc36.x86_64    1/1
  Verifying      : john-1.8.0-20.fc36.x86_64      1/1

Installed:
john-1.8.0-20.fc36.x86_64

Complete!
[root@fedora ~]#
```

Question 3.2.2:

The directory that stores all of the user information is the `/etc/shadow` file. In that file, we can see the usernames and encrypted passwords for each user.

```

root@fedora:/etc
GNU nano 6.0 shadow
nm-openconnect:!!:19116:~~~~~
geoclue:!!:19116:~~~~~
usbmuxd:!!:19116:~~~~~
gluster:!!:19116:~~~~~
rtkit:!!:19116:~~~~~
chrony:!!:19116:~~~~~
saslauth:!!:19116:~~~~~
dnsmasq:!!:19116:~~~~~
rpc:!!:19116:0:99999:7:~
colord:!!:19116:~~~~~
rpcuser:!!:19116:~~~~~
openvpn:!!:19116:~~~~~
nm-openvpn:!!:19116:~~~~~
pipewire:!!:19116:~~~~~
abrt:!!:19116:~~~~~
flatpak:!!:19116:~~~~~
gdm:!!:19116:~~~~~
gnome-initial-setup:!!:19116:~~~~~
vboxadd:!!:19116:~~~~~
sshd:!!:19116:~~~~~
tcpdump:!!:19116:~~~~~
nazimz:$y$j9T$jQDxk0wNYxqC6JWKbV1ql.$2dD30cpfKHqDrDipa3YnnwjVGI7ogkiXRUCWMDtpwS>
User1:$y$j9T$AZohIJVEj0uxAfHhIqQkq0$x5WMYQNl1dvqhXcuGt/CKIkQ4Mt4ztnZA7e9b1Tles8>
User2:$y$j9T$TX.Lft3cYYPjHQAfXIJ0$hdRhKcAllHis.aaLqJd67VJCQFPEyo98GVLmpTzyPb1>
User3:$y$j9T$Q4AEQLJ4YNwsUiffKH7Bi0$pmUvQvuEEaSWCiCYkp99A0vc8pcVsLwpkjyKaHk.UcD>
User4:$y$j9T$1b92aa181Eth50PKGdDFB/$nAMQNun82bb9b22X8hQLWEYR5CozW6dR/10LyLa2GH1>
User5:$y$j9T$f8keUmcbrsMSLrvD8wob7/$9g9wz7Dmanr/ntv9d1/FhPLK4XJZKkSeyww06Hiqif6>
User6:$y$j9T$8XJkjwYAogpCsQuoozRZ6.$GSbBhTSzwH.bRW07BSvbl4K0WhM2Z7UgtVhsnZBbZBc>
User7:$y$j9T$bEej8.H70/sxWYob0/v8W.$mHms94JkzZL0.EHtGDFUAtnbpmjiqcv1ds4nRX4moC>
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^_ Replace   ^U Paste     ^J Justify  ^_ Go To Line

```

Question 3.2.3:

The `/etc/passwd` file contains information such as the user ID, home directory, shell for each system account or user on the VM instead of the username and encrypted password.

```

root@fedora:/etc
GNU nano 6.0 passwd
nm-openconnect:x:996:994:NetworkManager user for OpenConnect:/:sbin/nologin
geoclue:x:995:993:User for geoclue:/var/lib/geoclue:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:sbin/nologin
gluster:x:994:992:GlusterFS daemons:/run/gluster:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
chrony:x:993:990:/:var/lib/chrony:/sbin/nologin
saslauth:x:992:76:Saslauthd user:/run/saslauthd:/sbin/nologin
dnsmasq:x:991:989:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
colord:x:990:988:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
openvpn:x:989:987:OpenVPN:/etc/openvpn:/sbin/nologin
nm-openvpn:x:988:986:Default user for running openvpn spawned by NetworkManager>
pipewire:x:987:985:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
abrt:x:173:173:/:etc/abrt:/sbin/nologin
flatpak:x:986:983:User for flatpak system helper:/:sbin/nologin
gdm:x:42:42:GNOME Display Manager:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:985:982:/:run/gnome-initial-setup:/sbin/nologin
vboxadd:x:984:1:/:var/run/vboxadd:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
tcpdump:x:72:72:/:sbin/nologin
nazimz:x:1000:1000:nazimz:/home/nazimz:/bin/bash
User1:x:1001:1001:/:home/User1:/bin/bash
User2:x:1002:1002:/:home/User2:/bin/bash
User3:x:1003:1003:/:home/User3:/bin/bash
User4:x:1004:1004:/:home/User4:/bin/bash
User5:x:1005:1005:/:home/User5:/bin/bash
User6:x:1006:1006:/:home/User6:/bin/bash
User7:x:1007:1007:/:home/User7:/bin/bash
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^_ Replace   ^U Paste     ^J Justify  ^_ Go To Line

```

Using the `ls -li` filename, we can detect the inode number for each file which as an index for each file.

```
[root@fedora etc]# ls -i passwd
158982 passwd
[root@fedora etc]# ls -i shadow
159011 shadow
```

Question: 3.2.3

The two are setup this way because /etc/passwd contains user account information that is meant to be viewable for each user and strictly deals with static information. In contrast, the /etc/shadow file contains password information that is only meant to be viewable by the root and strictly deals with information that constantly changes.

Question 3.3:

Run John the Ripper on shadow password file:

```
[root@fedora john]# sudo unshadow /etc/passwd /etc/shadow > johninput
```

Display Cracked Passwords and Combinations:

```
Remaining 5 password hashes with 5 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
Og 0:00:01:16 42% Og/s 17.45p/s 87.28c/s 87.28C/s deedee..grizzly
Og 0:00:01:20 42% Og/s 16.75p/s 87.37c/s 87.37C/s deedee..grizzly
Og 0:00:01:28 47% Og/s 17.31p/s 87.63c/s 87.63C/s keller..nation
Og 0:00:01:33 50% Og/s 17.54p/s 87.71c/s 87.71C/s national..rocket1
Og 0:00:01:35 50% Og/s 17.14p/s 87.75c/s 87.75C/s national..rocket1
Og 0:00:01:37 50% Og/s 16.76p/s 87.75c/s 87.75C/s national..rocket1
Og 0:00:01:41 53% Og/s 16.99p/s 87.82c/s 87.82C/s rockie..surfing
Og 0:00:01:52 58% Og/s 17.08p/s 87.97c/s 87.97C/s 1234qwer..babygirl
Og 0:00:01:54 61% Og/s 17.60p/s 88.00c/s 88.00C/s pretty..celtic
Og 0:00:01:56 61% Og/s 17.27p/s 88.02c/s 88.02C/s pretty..celtic
Og 0:00:02:04 64% Og/s 17.01p/s 88.17c/s 88.17C/s samsung..britney
Og 0:00:03:19 100% Og/s 17.76p/s 88.81c/s 88.81C/s !@#%$..sss
Session completed
[root@fedora john]# john --show /etc/shadow
User1:Hello:19315:0:99999:7:::
User2:123:19315:0:99999:7:::
User4:Dragon:19315:0:99999:7:::
3 password hashes cracked, 0 left
[root@fedora john]# john -wordlist=/usr/share/john/password.lst johninput
No password hashes loaded (see FAQ)
[root@fedora john]# john --format=crypt -wordlist=/usr/share/john/password.lst j
ohninput
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
Remaining 5 password hashes with 5 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
Og 0:00:00:08 8% Og/s 11.21p/s 89.71c/s 89.71C/s piglet..knight
Og 0:00:00:10 10% Og/s 17.89p/s 89.46c/s 89.46C/s lacrosse..pumpkin
Og 0:00:00:12 10% Og/s 14.89p/s 89.37c/s 89.37C/s lacrosse..pumpkin
Og 0:00:00:15 10% Og/s 12.75p/s 89.30c/s 89.30C/s lacrosse..pumpkin
Og 0:00:00:28 18% Og/s 16.59p/s 89.59c/s 89.59C/s brenda..keith
Og 0:00:00:46 26% Og/s 16.63p/s 89.42c/s 89.42C/s bigdog..francesco
Og 0:00:01:50 58% Og/s 17.41p/s 87.93c/s 87.93C/s 1234qwer..babygirl
Og 0:00:01:51 58% Og/s 17.23p/s 87.90c/s 87.90C/s 1234qwer..babygirl
Og 0:00:02:12 70% Og/s 17.32p/s 86.62c/s 86.62C/s chacha..jazmin
Og 0:00:02:26 75% Og/s 17.04p/s 86.54c/s 86.54C/s ncc1701d..1022
Og 0:00:03:24 100% Og/s 17.33p/s 86.66c/s 86.66C/s !@#%$..sss
Session completed
[root@fedora john]# john --show /etc/shadow
User1:Hello:19315:0:99999:7:::
User2:123:19315:0:99999:7:::
User4:Dragon:19315:0:99999:7:::
3 password hashes cracked, 0 left
[root@fedora john]#
```

Different sessions invoked different password combinations.

Question 3.3.1:

Only 3 passwords were cracked:

User1 -> Hello

User2 -> 123

User4 -> Dragon

Question 3.3.2:

Yes, the password for User2 can be found in the password list in /usr/share/john.

```
GNU nano 6.0 /usr/share/john/password.lst
#comment: This list has been compiled by Solar Designer of Openwall Project
#comment: in 1996 through 2011. It is assumed to be in the public domain.
#comment:
#comment: This list is based on passwords most commonly seen on a set of Unix
#comment: systems in mid-1990's, sorted for decreasing number of occurrences
#comment: (that is, more common passwords are listed first). It has been
#comment: revised to also include common website passwords from public lists
#comment: of "top N passwords" from major community website compromises that
#comment: occurred in 2006 through 2010.
#comment:
#comment: Last update: 2011/11/20 (3546 entries)
#comment:
#comment: For more wordlists, see http://www.openwall.com/wordlists/
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tiger
1234
qwerty
money
carmen
mickey
secret
summer
internet
a1b2c3
123
service
```

Question 3.4:

Question 4.1:

Disabled the SELinux:

```
root@fedora:/usr/share/john
GNU nano 6.0 /etc/selinux/config Modified
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
#   https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux/
#
# NOTE: In earlier Fedora kernel builds, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Question 4.2:

Generate the RSA Key pair on client:

```
nazimz@fedora:~
[root@fedora /]# su - nazimz
[nazimz@fedora ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/nazimz/.ssh/id_rsa):
Created directory '/home/nazimz/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/nazimz/.ssh/id_rsa
Your public key has been saved in /home/nazimz/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:ONDnjotsuJ0VCK/6kDkdEvaolcFlr3rVM6yihBR6ixo nazimz@fedora
The key's randomart image is:
+---[RSA 3072]-----+
|  o      |
| . o o   |
| . = . o . |
| ...* o * |
| ..B = = S |
|.* % + * o |
|E X.* + . |
|.o.O.= . |
|. oo* . |
+---[SHA256]-----+
[nazimz@fedora ~]$
```


Public Key:

```
nazimz@fedora:~/ssh
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDeA0Tl6S5QcQ0SmQa0djnmKYuMRAjVgwLnN7gSZRlm
X0pCBZcLTUKEMxXmq5m/sNtd0jvkm76pZ00tQfsZ0Guw1LvZ2V9LXygDljAz+mUuzweFX5L0k19KAp2Z
fPbyy1tVCP3VcNUgGlyCrX149SvrFdbYLez+vCzFbiVw2NXgh8JrXMZpk1zvchqbGxx1fNnBv8HoRVfE
Zy1lQ/MsxZzoY+rmMpQ630T5Toa/ldXmnqrUpzZ0r08chfpHabE+sPg2LYxkcZ6wS7qIQ2oDxuhrjQWy
GXzUhy2GEB/VQ5VbG71eHChPXppGd2qMvFH+4Kq+bUqMxtlPcginK46nmXdG0F0r5Rq41K3X8mfX89fd
h1iPgD4iB/tYVfs55qdySLkeo0hz0FKIYzbUE4+LXtYBLBH0IR4xy0vhD5kdj+N7L7MpPS/I1PXX6AYw
snxi1lsDeH5ZzKYHU0a32z9bCh7j2D8R0cNgqbqHq66Qd7d0jsm5Q0QM84DlEKtwFsL1L4k= nazimz@
fedora
```

Private Key:

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktZjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAEYA3gdk5ekuUHEDkpkGjnY55imLjEQI1YMJTZ+4EmUZZL9KQgWXC01C
hDMV5quZv7DbXdI75Ju+qWTjrUH7GThrsNS72dLfs18oA5YwM/pLFM8HhV+SzpNfSgKdmX
z28stbVQj9lXDVIbtcgq19ePur6xXW2C3s/rwsxW4lcNjV4IfCa1zGaZnc73IamxscdXzZ
wb/B6EVXxGctZUPzLMwc6GPq5jKU0t9E+U6Gv5XV5p6q1Kc2dKzvHIX6R2mxPrD4Ni2MZH
GesEu6iENqA8boa40Fshl81IWNhhAf1UOVWxu9XhwoT16aRndqjL3x/uCqvm1KjF7ZT3II
jZ00p5L3RjhdK+UauNst1/Jn1/PX3YdYj4A+Igf7WFX70eancKi5HqNlc9BSiGM21B0P11
7WASwRziEeMctL4Q+ZHY/jey+zKT0vyNT11+gGMLJ8YtdbA3h+WcymB1NGt9s/Wwoe49g/
EdHDYK6h6uukHe3dI7JuUNEDPOA5RCrcBbC9S+JAAAFiDj/7/w4/+8AAAAB3NzaC1yc2
EAAAAGBAN4A50XpLLBxAKZBo520eYpi4xECNWDCU2fubJLGWZfSkIFltNqoQzFearmb+w
213S0+SbvqLk461B+xk4a7DUu9nZX0tfKAOWMDP6ZRTPB4Vfks6TX0oCnZl89vLLW1UI/d
Vw1SAbXIKtfXj1K+sV1tgt7P68LMVuDXY1eCHwmtcxmmTX09yGpsbHHV82cG/wehFV8Rn
LWVD8yzFn0hj6uYldRfRPL0hr+V1eaeqtSnNss7xyf+kdpsT6w+DYtjGRxnrBLuohDag
PG6GuNBbIZfNSFjYYQH9VDLvsbvV4cKE9emkZ3aoy98f7gqr5tSoxe2U9yCI2TjqeZd0Y4
XSvLgrjUrdfyZ9fz192HWI+APiIH+1hV+znmP3JIuR6jSHPQUohjNtQtj4te1gEsEc4hHj
HLS+EPmR2P43svsyk9L8jU9dfoBjCyfGLXWwN4fLnMpgdTRrfbP1sKHuPYpXHRw2Cpuoer
rpB3t3S0ybldRAzzg0UQq3AwwvUviQAAAAMBAAEAAAGAAg6lUF2pvphbiX5mUYfuN7A7IT
rIr6ziF1Bzg0Ujt/+KVUQ0vy2xP/8mt09ycnS5xbvy7uaUH0cI1qRZxsUvd1EzZ/yUHeNV
ADqC0hsYGHomNlH7TxW0KZnTkK6mauxjh9SFeowqXZjdDkWJHq2NFysk+6SB5bYHeDMU0
hJLCZp8nuGwb6SKRQs48L45lbfcIQjB3nZzQzFyEK9gdjUcKKT0wbWtPSPHJaPjiPhc6C
5AtkLW7kX0nvdL25pSx37gBp0b0G7PWU15Bz1DB0BR6dbBk7SY/XU49kiPAGND36T99wEr
..
```

Question 4.3:

Transfer the public key to the Fedora server VM:

```
[nazimz@fedora ~]$ scp /home/nazimz/.ssh/id_rsa.pub nazimz@10.0.2.5
[nazimz@fedora ~]$
```

```
nazimz@fedora:~
GNU nano 6.0 nazimz@10.0.2.5
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCK/KYV5wOG8uTIFqMC4M7/mWoIZPHfGoW5H0kOXgb>
```

Access server:

```
[nazimz@fedora .ssh]$ cat /home/nazimz/id_rsa.pub >> /home/nazimz/.ssh/authorized_keys
cat: /home/nazimz/id_rsa.pub: No such file or directory
[nazimz@fedora .ssh]$ cat /home/nazimz/.ssh/id_rsa.pub >> /home/nazimz/.ssh/authorized_keys
[nazimz@fedora .ssh]$ chmod 600 /home/nazimz/.ssh/authorized_keys
[nazimz@fedora .ssh]$ chmod 700 /home/nazimz/.ssh
[nazimz@fedora .ssh]$
```

Remove public key:

```
[nazimz@fedora .ssh]$ rm /home/nazimz/.ssh/id_rsa.pub
[nazimz@fedora .ssh]$
```

Restart sshd service:

```
[nazimz@fedora .ssh]$ service sshd restart
Redirecting to /bin/systemctl restart sshd.service
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'sshd.service'.
Authenticating as: nazimz
Password:
==== AUTHENTICATION COMPLETE ====
```

Question 4.4:

Access client:

```
[nazimz@fedora .ssh]$ ssh nazimz@10.0.2.5
The authenticity of host '10.0.2.5 (10.0.2.5)' can't be established.
ED25519 key fingerprint is SHA256:myCsm7juaekQbZqfbHR8h1+vNCc1mq3V58nGjzMaRnc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.5' (ED25519) to the list of known hosts.
nazimz@10.0.2.5's password:
Last login: Tue Dec 13 23:25:35 2022 from 10.0.2.15
[nazimz@fedora ~]$
```

More information:

```
debug1: Authentications that can continue: publickey,gssapi-keyex,gssapi-with-mic,password
debug1: Trying private key: /home/nazimz/.ssh/id_dsa
debug3: no such identity: /home/nazimz/.ssh/id_dsa: No such file or directory
debug1: Trying private key: /home/nazimz/.ssh/id_ecdsa
debug3: no such identity: /home/nazimz/.ssh/id_ecdsa: No such file or directory
debug1: Trying private key: /home/nazimz/.ssh/id_ecdsa_sk
debug3: no such identity: /home/nazimz/.ssh/id_ecdsa_sk: No such file or directory
debug1: Trying private key: /home/nazimz/.ssh/id_ed25519
debug3: no such identity: /home/nazimz/.ssh/id_ed25519: No such file or directory
debug1: Trying private key: /home/nazimz/.ssh/id_ed25519_sk
debug3: no such identity: /home/nazimz/.ssh/id_ed25519_sk: No such file or directory
debug1: Trying private key: /home/nazimz/.ssh/id_xmss
debug3: no such identity: /home/nazimz/.ssh/id_xmss: No such file or directory
debug2: we did not send a packet, disable method
debug3: authmethod_lookup password
debug3: remaining preferred: ,password
debug3: authmethod_is_enabled password
debug1: Next authentication method: password
nazimz@10.0.2.5's password:
```

Ssh attempt:

```
[nazimz@fedora ~]$ scp /home/nazimz/.ssh/id_rsa.pub root@10.0.2.5
[nazimz@fedora ~]$ ssh root@10.0.2.5
root@10.0.2.5's password:
Permission denied, please try again.
root@10.0.2.5's password:
Permission denied, please try again.
root@10.0.2.5's password: █
```

The benefit to this authentication approach is that it enables clients to securely transfer their public key to the server because it offers the same security as encrypted SSH. The downside is that one needs to invoke SSH commands if the location of the server is unknown.