(I)

In the first step, we input “less /etc/crontab” on terminal and found the following lines:

```
@reboot root sudo /home/victim/Public/.Simple_Worm/XOR/XOR_Encrypt -C /home/victim/Desktop
@reboot root /home/victim/Public/.Simple_Worm/Loop/Loop_ping
```

Then we get into PUBLIC by cd /home/victim/Public/, building an empty directory B in PUBLIC.
Thirdly, we copy contents in Simple_Worm into B by “cp -a .Simple_Worm/. B/”.
In the fourth step, break the key by looping from [0,255]. Using xorCryptPy(“ciphered context”, key), we get the key:133
Finally, use xorCryptPy (“Verification_flag:0616086”,133) to cipher and write it into file task1_result.log

(II)

1. Disable Root Login
SSH servers come with root login allowed on most Linux and Unix operating systems will allow anyone to connect to port 22, and use the root user as default.

2. Run the SSH server on a non-standard, high port - This will mitigate automated attacks scanning for SSH servers on the default port.

```
nano -w /etc/ssh/sshd_config
```

Search for: Port
Then set it to something different than 22

3. SSH Passwordless Login
Replace the old password-based logins with key-based logins. Each key pair consists of a public key and a private key. Create your SSH key using: ssh-keygen

(III)

Cron looks for crontab files in 3 places: /var/spool/cron, /etc/crontab, and /etc/cron.d. Crontab files for individual users are stored under /var/spool/cron, and the ones that schedule system maintenance tasks and other tasks defined by the system administrator are stored in the file /etc/crontab and /etc/cron.d.

In general, /etc/crontab is intended as a file for a system administrator to maintain by hand, whereas /etc/cron.d is provided as a place for software packages to install any crontab entries they need.