Lab 2 Part 4: Digital Signature of the asciinema file

A. We signed our Team8_lab2.cast file by generating a hash using openssl dgst, then we used openssl rsault to sign and verify the signature file as shown below.

```
user@ubuntu:~$
user@ubuntu:~$ openssl dgst -sha256 Team8_lab2.cast > hash
user@ubuntu:~$
user@ubuntu:~$ cat hash
SHA256(Team8_lab2.cast)= 713b3fdc201585188e5da69b42ff04d715f009d967bac34ada600fb7ac82e44f
user@ubuntu:~$
user@ubuntu:~$
user@ubuntu:~$ openssl rsautl -sign -inkey receiver_privatekey.priv -in hash >team8_lab2_cast.signed
user@ubuntu:~$
user@ubuntu:~$
user@ubuntu:~$ openssl rsautl -verify -inkey receiver_publickey.pub -pubin -in team8_lab2_cast.signe
d
SHA256(Team8_lab2.cast)= 713b3fdc201585188e5da69b42ff04d715f009d967bac34ada600fb7ac82e44f
user@ubuntu:~$
user@ubuntu:~$
```

B. We also created a resubmit subfolder inside lab2 folder on the Master server.

Created another signed file named team8_lab2_cast2.signed by using openssl dgst only with the same sha256 algorithm and the same private key as seen below.

```
user@ubuntu:~$
user@ubuntu:~$ openssl dgst -sha256 -sign receiver_privatekey.priv -out team8_lab2_cast2.signed Team
8_lab2.cast
user@ubuntu:~$ openssl dgst -sha256 -verify receiver_publickey.pub -signature team8_lab2_cast2.signe
d Team8_lab2.cast
Verified OK
user@ubuntu:~$
```