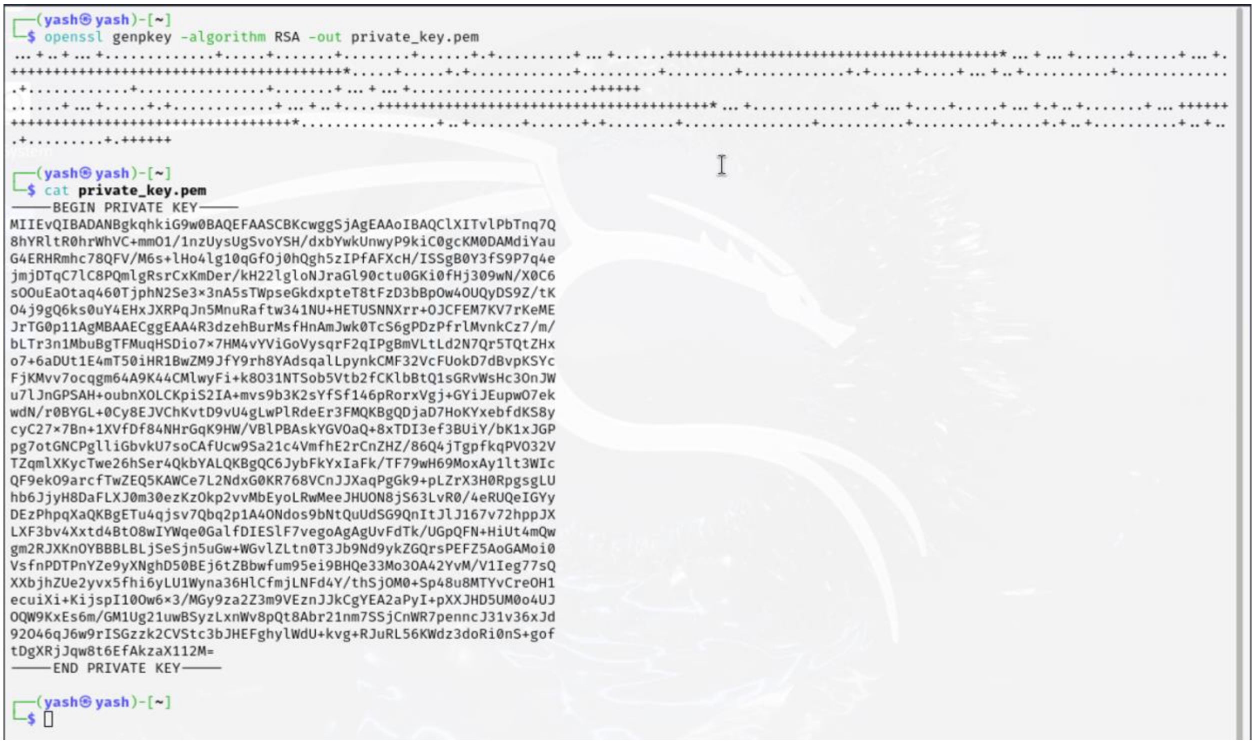
Digital Signature Project

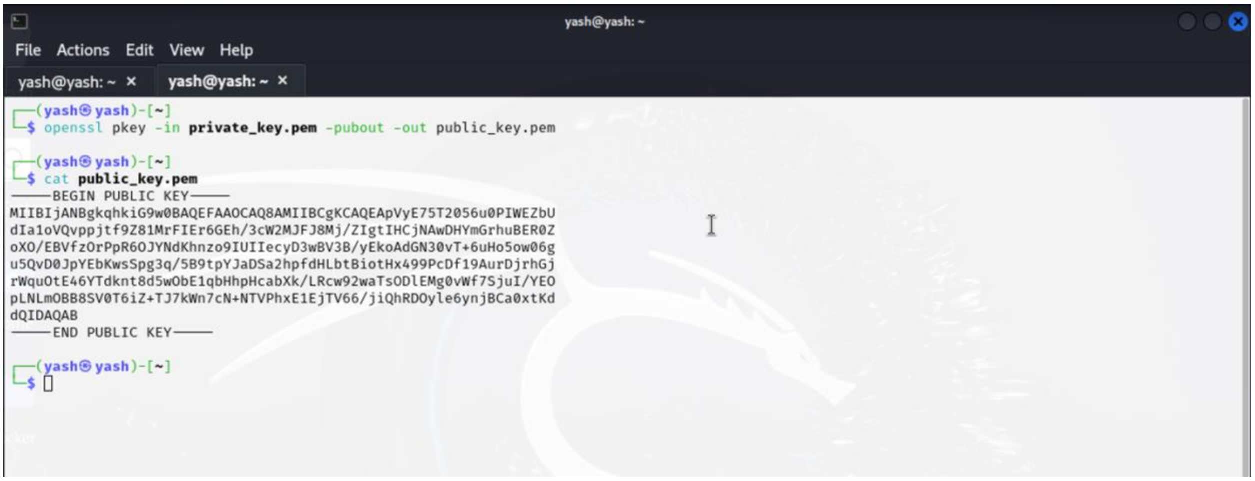
Objective: Securely sign a confidential file using an SHA256 digital signature and verify its integrity to detect any corruption or unauthorized modifications.

Step 1: Generate a private key



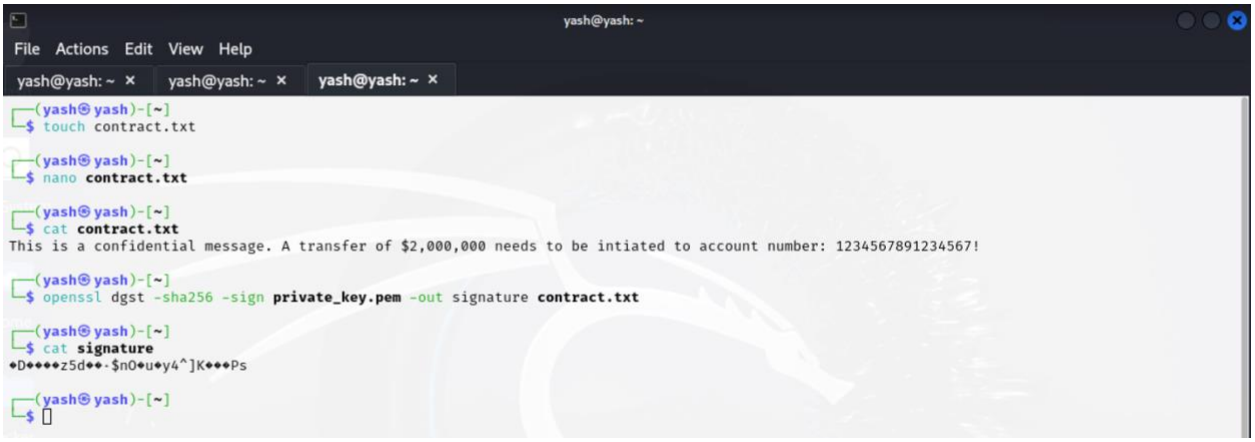
```
┌──(yash㉿yash)-[~]
└─$ openssl genpkey -algorithm RSA -out private_key.pem
...+..+...+.............+.....+.......+........+......+.+.........+...+......+++++++++++++++++++++++++++++++++++++++++*...+...+......+.....+...+.
+++++++++++++++++++++++++++++++++++++++*.....+.....+.+............+.........+.......+............+.+.....+....+...+..+..........+............
.+...........+...............+.......+...+...+......................++++++
......+...+.....+.+............+...+..+....+++++++++++++++++++++++++++++++++++++++++*...+.............+...+....+.....+...+.+..+.......+...++++++
+++++++++++++++++++++++++++++++++*...............+..+......+......+.+........+...............+.........+.........+.....+.+..+..........+..+..
.+.........+.++++++

┌──(yash㉿yash)-[~]
└─$ cat private_key.pem
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQClXITvlPbTnq7Q
8hYRltR0hrWhVC+mmO1/1nzUysUgSvoYSH/dxbYwkUnwyP9kiC0gcKM0DAMdiYau
G4ERHRmhc78QFV/M6s+lHo4lg10qGfOj0hQgh5zIPfAFXcH/ISSgB0Y3fS9P7q4e
jmjDTqC7lC8PQmlgRsrCxKmDer/kH22lgloNJraGl90ctu0GKi0fHj309wN/X0C6
sOOuEaOtaq460TjphN2Se3×3nA5sTWpseGkdxpteT8tFzD3bBpOw4OUQyDS9Z/tK
O4j9gQ6ks0uY4EHxJXRPqJn5MnuRaftw341NU+HETUSNNXrr+OJCFEM7KV7rKeME
JrTG0p11AgMBAAECggEAA4R3dzehBurMsfHnAmJwk0TcS6gPDzPfrlMvnkCz7/m/
bLTr3n1MbuBgTFMuqHSDio7×7HM4vYViGoVysqrF2qIPgBmVLtLd2N7Qr5TQtZHx
o7+6aDUt1E4mT50iHR1BwZM9JfY9rh8YAdsqalLpynkCMF32VcFUokD7dBvpKSYc
FjKMvv7ocqgm64A9K44CMlwyFi+k8O31NTSob5Vtb2fCKlbBtQ1sGRvWsHc3OnJW
u7lJnGPSAH+oubnXOLCKpiS2IA+mvs9b3K2sYfSf146pRorxVgj+GYiJEupwO7ek
wdN/r0BYGL+0Cy8EJVChKvtD9vU4gLwPlRdeEr3FMQKBgQDjaD7HoKYxebfdKS8y
cyC27×7Bn+1XVfDf84NHrGqK9HW/VBlPBAskYGVOaQ+8xTDI3ef3BUiY/bK1xJGP
pg7otGNCPglliGbvkU7soCAfUcw9Sa21c4VmfhE2rCnZHZ/86Q4jTgpfkqPVO32V
TZqmlXKycTwe26hSer4QkbYALQKBgQC6JybFkYxIaFk/TF79wH69MoxAy1lt3WIc
QF9ekO9arcfTwZEQ5KAWCe7L2NdxG0KR768VCnJJXaqPgGk9+pLZrX3H0RpgsgLU
hb6JjyH8DaFLXJ0m30ezKzOkp2vvMbEyoLRwMeeJHUON8jS63LvR0/4eRUQeIGYy
DEzPhpqXaQKBgETu4qjsv7Qbq2p1A4ONdos9bNtQuUdSG9QnItJlJ167v72hppJX
LXF3bv4Xxtd4BtO8wIYWqe0GalfDIESlF7vegoAgAgUvFdTk/UGpQFN+HiUt4mQw
gm2RJXKnOYBBBLBLjSeSjn5uGw+WGvlZLtn0T3Jb9Nd9ykZGQrsPEFZ5AoGAMoi0
VsfnPDTPnYZe9yXNghD50BEj6tZBbwfum95ei9BHQe33Mo3OA42YvM/V1Ieg77sQ
XXbjhZUe2yvx5fhi6yLU1Wyna36HlCfmjLNFd4Y/thSjOM0+Sp48u8MTYvCreOH1
ecuiXi+KijspI10Ow6×3/MGy9za2Z3m9VEznJJkCgYEA2aPyI+pXXJHD5UM0o4UJ
OQW9KxEs6m/GM1Ug21uwBSyzLxnWv8pQt8Abr21nm7SSjCnWR7penncJ31v36xJd
92O46qJ6w9rISGzzk2CVStc3bJHEFghylWdU+kvg+RJuRL56KWdz3doRi0nS+gof
tDgXRjJqw8t6EfAkzaX112M=
-----END PRIVATE KEY-----

┌──(yash㉿yash)-[~]
└─$ ▯
```

Step 2: Generate a private key



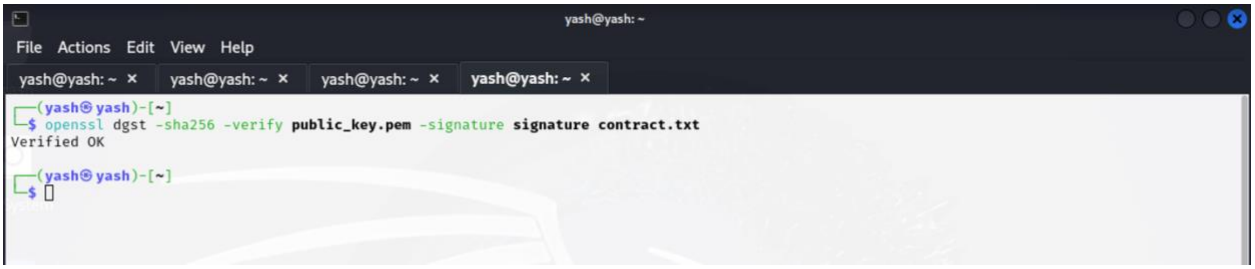
```
┌──(yash㉿yash)-[~]
└─$ openssl pkey -in private_key.pem -pubout -out public_key.pem

┌──(yash㉿yash)-[~]
└─$ cat public_key.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApVyE75T2056u0PIWEZbU
dIa1oVQvppjtf9Z81MrFIEr6GEh/3cW2MJFJ8Mj/ZIgtIHCjNAwDHYmGrhuBER0Z
oXO/EBVfzOrPpR6OJYNdKhnzo9IUIIecyD3wBV3B/yEkoAdGN30vT+6uHo5ow06g
u5QvD0JpYEbKwsSpg3q/5B9tpYJaDSa2hpfdHLbtBiotHx499PcDf19AurDjrhGj
rWquOtE46YTdknt8d5wObE1qbHhpHcabXk/LRcw92waTsODlEMg0vWf7SjuI/YEO
pLNLmOBB8SV0T6iZ+TJ7kWn7cN+NTVPhxE1EjTV66/jiQhRDOyle6ynjBCa0xtKd
dQIDAQAB
-----END PUBLIC KEY-----

┌──(yash㉿yash)-[~]
└─$ ▯
```

Step 3: Sign the confidential file with a SHA256 signature



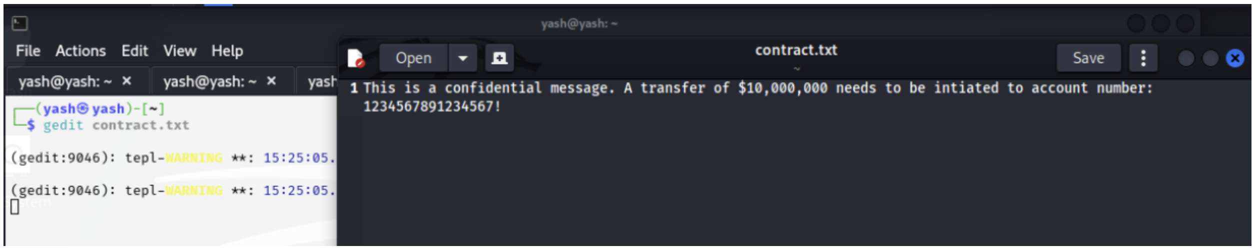
```
┌──(yash㉿yash)-[~]
└─$ touch contract.txt

┌──(yash㉿yash)-[~]
└─$ nano contract.txt

┌──(yash㉿yash)-[~]
└─$ cat contract.txt
This is a confidential message. A transfer of $2,000,000 needs to be intiated to account number: 1234567891234567!

┌──(yash㉿yash)-[~]
└─$ openssl dgst -sha256 -sign private_key.pem -out signature contract.txt

┌──(yash㉿yash)-[~]
└─$ cat signature
◆D◆◆◆◆z5d◆◆·$nO◆u◆y4^]K◆◆◆Ps

┌──(yash㉿yash)-[~]
└─$ 
```

Step 4: Verification shows “Verified OK” before the file is corrupted



```
┌──(yash㉿yash)-[~]
└─$ openssl dgst -sha256 -verify public_key.pem -signature signature contract.txt
Verified OK

┌──(yash㉿yash)-[~]
└─$ 
```

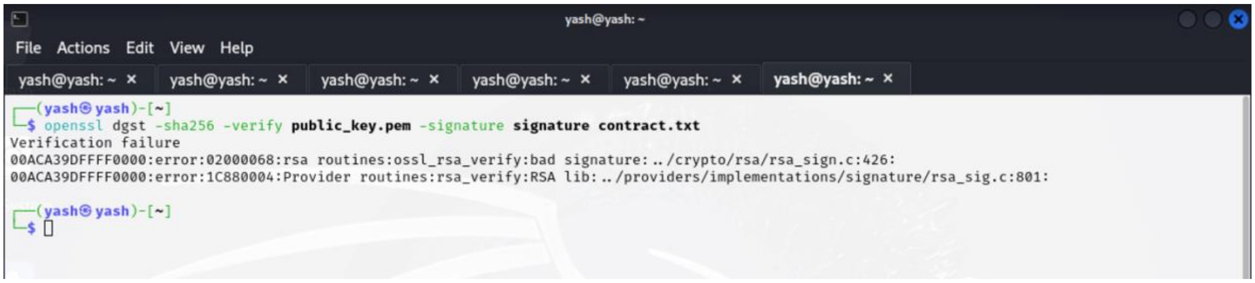
Malicious Attacker corrupts the file



```
┌──(yash㉿yash)-[~]
└─$ gedit contract.txt

(gedit:9046): tepl-WARNING **: 15:25:05.

(gedit:9046): tepl-WARNING **: 15:25:05.
```

```
This is a confidential message. A transfer of $10,000,000 needs to be intiated to account number:
1234567891234567!
```

Step 6: Re-verify to see that the verification displays “Verification Failure”



```
┌──(yash㉿yash)-[~]
└─$ openssl dgst -sha256 -verify public_key.pem -signature signature contract.txt
Verification failure
00ACA39DFFFF0000:error:02000068:rsa routines:ossl_rsa_verify:bad signature:../crypto/rsa/rsa_sign.c:426:
00ACA39DFFFF0000:error:1C880004:Provider routines:rsa_verify:RSA lib:../providers/implementations/signature/rsa_sig.c:801:

┌──(yash㉿yash)-[~]
└─$ 
```