In this lab I will encrypt and decrypt files using RSA encryption with OpenSSL.
Like with AES I will begin by creating a text file using the echo command.
echo "This is a test file for RSA encryption." > test_file.txt
Next I will start generating a RSA private key using the command:
openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048

- openssl genpkey: Invokes OpenSSL's general-purpose key generation utility14
- algorithm RSA: specifies RSA algorithm for key generation
- out private_key.pem: output file for key to be stored
- pkeyopt rsa_keygen_bits:2048: Defines generation key size. This defines an RSA key size of 2048 bits.

Now I need to extract the public key of my created RSA private key using the following command:
openssl rsa -pubout -in private_key.pem -out public_key.pem

- openssl rsa: openssl rsa tool used for key management
- -pubout: Oppenssl command to extract public key from private key
- -in private_key.pem: file extracting from
- out public_key.pem: save extracted public key to

Using the created public key I will encrypt my test file with the following command:
openssl pkeyutl -encrypt -in test_file.txt -pubin -inkey public_key.pem -out test_file_encrypted.bin

- openssl pkeyutl: openssl public key utility tool (encrypt, decrypt, ext)
- -encrypt: specifies that the public key is being used for encryption
- -in test_file.txt: specifies file for encryption
- -pubin: specifies the input is the public key (by default it is the private key)
- inkey public_key.pem: the public key used for encryption
- -out test_file_encrypted.bin: encrypted file

Using the cat command on both files shows a successful encryption

```
theia@theia-bradleyrroff:/home/project$ cat test_file.txt
This is a test file for RSA encryption.
theia@theia-bradleyrroff:/home/project$ cat test_file_encrypted.bin
r\:i$+hR_5k
/6x;
n?(_AoE\[!wg)*0N8;[
qEw5n:Xtheia@theia-bradleyrroff:/home/project$
```

Finally I will decrypt the file using the private key in the following command:
openssl pkeyutl -decrypt -in test_file_encrypted.bin -inkey private_key.pem -out test_file_decrypted.bin

- -decrypt: specifies decryption
- -in test_file_encrypted.bin: the input is the encrypted file
- -inkey private_key.pem: specifies the private key used for decryption
    - Note: because private key is default there is no need for an extra command like -pubin for public key
- Test_file_decrypted.bin: decrypted file

Finally using the cat command we can see our final results.