**Name:** Anshul Shirbhate

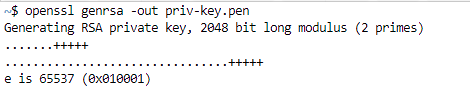
**Roll No:** D – 5

**Practical No:** 7

**Practical Aim:** Use openssl command to perform symmetric key encryption (RSA) and also implement RSA algorithm.

**Commands:**

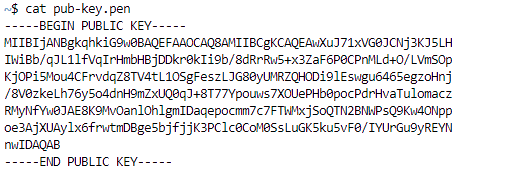
1. To generate a private key we need to type the command : openssl genrsa -out priv-key.pen



2. To generate a public key we need to run this command: openssl rsa -pubout -in priv-key.pen -out pub-key.pen



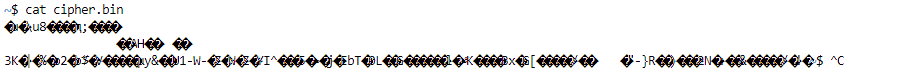
3. To view the generated public key: cat pub-key.pen



4. To encrypt the message file we need to type the command: openssl rsaut1 -encrypt -in Message.txt -pubin -inkey pub-key.pen -out cipher.bin



5. To view the cipher text type the command: cat cipher.bin



6. To decrypt the message that was encrypted type the command:



**Conclusion:**

In this practical, we learnt about the RSA algorithm and saw how to encrypt and decrypt messages using openssl command in linux terminal.