RSA Encryption and Signature Lab

Task 1: Deriving the Private Key

```c
#include <stdio.h>
#include <openssl/bn.h>
#define NBITS 256

void printBN(char *msg, BIGNUM * a, BIGNUM * b)
{
/* Use BN_bn2hex(a) for hex string
* Use BN_bn2dec(a) for decimal string */
char * number_str_a = BN_bn2hex(a);
char * number_str_b = BN_bn2hex(b);
printf("%s (%s,%s)\n", msg, number_str_a, number_str_b);
OPENSSL_free(number_str_a);
OPENSSL_free(number_str_b);
}

int main ()
{
BN_CTX *ctx = BN_CTX_new();
BIGNUM *p = BN_new();
BIGNUM *q = BN_new();
BIGNUM *e = BN_new();
BIGNUM *phi = BN_new();
BIGNUM *n = BN_new();
BIGNUM *d = BN_new();
BIGNUM *pm1 = BN_new();
BIGNUM *qm1 =BN_new();

// assign values
BN_hex2bn(&p, "F7E75FDC469067FFDC4E847C51F452DF");
BN_hex2bn(&q, "E85CED54AF57E53E092113E62F436F4F");
BN_hex2bn(&e, "0D88C3");

// Solution: n = p*q for compute Public Key
BN_mul(n, p, q, ctx);
printBN("Public Key:", e, n);

// Solution: phi(n) = (p-1)*(q-1)
BN_sub(pm1, p, BN_value_one());
BN_sub(qm1, q, BN_value_one());
BN_mul(phi,pm1, qm1, ctx);
// Solution: e * d mod phi(n) = 1 for compute Private Key
BN_mod_inverse(d, e, phi, ctx);
printBN("Private Key:", d, n);
```

```
[04/15/22]seed@VM:~/.../Task1$ gcc CS234_Security_Lab03-Cryptography-RSA_S40_task-1.c -lcry
pto
[04/15/22]seed@VM:~/.../Task1$ ./a.out
Public Key: (0D88C3,E103ABD94892E3E74AFD724BF28E78366D9676BCCC70118BD0AA1968DBB143D1)
Private Key: (3587A24598E5F2A21DB007D89D18CC50ABA5075BA19A33890FE7C28A9B496AEB,E103ABD94892
E3E74AFD724BF28E78366D9676BCCC70118BD0AA1968DBB143D1)
[04/15/22]seed@VM:~/.../Task1$
```

ใน Task นี้จะเป็นการสร้าง Private Key โดยการนำ Public Key ที่สร้างก่อนหน้า ด้วยสูตรคำนวน **n = p * q** โดยสูตรนี้ต้องการ prime number ที่เป็นเลขฐานสิบหกทั้งคู่มาใช้คำนวน โดยหลังจากคำนวนจะได้ Public Key มาเพื่อใช้คำนวน โดยหลังจากนี้จะนำมาคำนวนหา **Ø(n) = (p-1) * (q-1)** เพื่อนำมาใช้ในการ คำนวน Private Key ต่อไป โดยสูตรที่ใช้คำนวน Private Key คือ **e * d mod Ø(n) = 1** โดยสูตร BIGNUM ของ Private Key คือ **BN_mod_inverse** หลังจากนั้นก็จะได้ Private Key ที่คู่กับ Public Key นั้น