ธนากร ชัยรัตนธนานนท์ 6409610620

กรกนก วรรณชมภู 6409682520

ปุณณ อัฉริยปัญญา 6409682801

CS324_Security_Lab01 -Cryptography-RSA_G18

Task 1: Deriving the Private Key Report

Let p, q, and e be three prime numbers. Let n = p*q. We will use (e, n) as the public key. Please

calculate the private key d. The hexadecimal values of p, q, and e are listed in the following. It should benoted that although p and q used in this task are quite large numbers, they are not large enough to be secure. We intentionally make them small for the sake of simplicity. In practice, these numbers should be at least 512 bits long (the one used here are only 128 bits).

p = F7E75FDC469067FFDC4E847C51F452DF

q = E85CED54AF57E53E092113E62F436F4F

e = 0D88C3

Task 1: Code

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

void printBN(char *msg, BIGNUM *a){
// แปลง BIGNUM กลับเป็น String ตัวเลข
char * number_str = BN_bn2hex(a);
// Print out String ตัวเลข
printf("%s %s\n", msg, number_str);
// Free the dynamically allocated memory
OPENSSL_free(number_str);
}

int main(){
BN_CTX *ctx = BN_CTX_new();
BIGNUM *p = BN_new();
BIGNUM *q = BN_new();
BIGNUM *e = BN_new();
BIGNUM *d = BN_new();
BIGNUM *res1 = BN_new();
BIGNUM *res2 = BN_new();
BIGNUM *res3 = BN_new();
BIGNUM *one = BN_new();
// กำหนดค่า p q e ตามที่โจทย์ให้

//โดยใช้ hex2bn เปลี่ยนเลขฐาน 16 เป็น Bignum
```

```
BN_hex2bn(&p, "F7E75FDC469067FFDC4E847C51F452DF");
BN_hex2bn(&q, "E85CED54AF57E53E092113E62F436F4F");
BN_hex2bn(&e, "0D88C3");

// Assign the Modulus
//ใช้ dec2bn เปลี่ยน decimal เป็น Bignum
//หา p-1 และ q-1 แล้วเก็บไว้ใน res1 และ res2 หลังจากนั้นใช้ res3 เก็บค่า (p-1)(q-1)
BN_dec2bn(&one,"1");
//res1 = p-1
BN_sub(res1, p, one);
//res2 = q-1
BN_sub(res2, q, one);
//res3=res1*res2
BN_mul(res3, res1, res2, ctx);
//ใช้ mod_inverse เพื่อ Generate Key
BN_mod_inverse(d, e, res3, ctx);
//print BN
printBN("d= ",d);
return 0;
}
```

ซึ่งการรันจะทำให้ได้ผลลัพธ์เป็น Private Key ดังนี้

```
gunzcats@Gunzcats:~/CS324_Security_Lab01-Cryptography-RSA_G18$ code .
gunzcats@Gunzcats:~/CS324_Security_Lab01-Cryptography-RSA_G18$ ./task1
d=  3587A24598E5F2A21DB007D89D18CC50ABA5075BA19A33890FE7C28A9B496AEB
gunzcats@Gunzcats:~/CS324_Security_Lab01-Cryptography-RSA_G18$
```