Task 4: Signing a Message

หา hex value ของ I owe you $2000. โดยคำสั่ง

```
[02/29/24]seed@VM:~/Pictures$ python3 -c 'print(bytes("I owe you $2000.", "utf-8").hex())'
49206f776520796f752024323030302e
```

Source code สำหรับการ sign message

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


void printBN(char *msg, BIGNUM *a){
        char * number_str = BN_bn2hex(a);
        printf("%s %s\n", msg, number_str);
        OPENSSL_free(number_str);
}

int main(){
         BN_CTX *ctx = BN_CTX_new();
         BIGNUM *n = BN_new();
         BIGNUM *d = BN_new();
         BIGNUM *c = BN_new();
         BIGNUM *dec = BN_new();

         BN_hex2bn(&n, "DCBFFE3E51F62E09CE7032E2677A78946A849DC4CDDE3A4D0CB81629242FB1A5");
         BN_hex2bn(&c, "49206f776520796f752024323030302e"); //HEX value of I owe you $2000.
         BN_hex2bn(&d, "74D806F9F3A62BAE331FFE3F0A68AFE35B3D2E4794148AACBC26AA381CD7D30D");

         //encryption and print the result
         BN_mod_exp(dec, c, d, n, ctx);

         printBN("encrypt message = ", dec);

         return 0;
}
```

Compile และ run code เพื่อทำการ sign message

```
[02/29/24]seed@VM:~$ gcc -o task4 task4.c -lcrypto
[02/29/24]seed@VM:~$ ./task4
encrypt message =  55A4E7F17F04CCFE2766E1EB32ADDBA890BBE92A6FBE2D785ED6E73CCB35E4CB
```

หา hex value ของ I owe you $3000. โดยคำสั่ง

```
[02/29/24]seed@VM:~$ python3 -c 'print(bytes("I owe you $3000.", "utf-8").hex())'
49206f776520796f752024333030302e
```

เปลี่ยน c ใน source code เป็น HEX value ของ I owe you $3000. แทน

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


void printBN(char *msg, BIGNUM *a){
        char * number_str = BN_bn2hex(a);
        printf("%s %s\n", msg, number_str);
        OPENSSL_free(number_str);
}

int main(){
         BN_CTX *ctx = BN_CTX_new();
         BIGNUM *n = BN_new();
         BIGNUM *d = BN_new();
         BIGNUM *c = BN_new();
         BIGNUM *dec = BN_new();

         BN_hex2bn(&n, "DCBFFE3E51F62E09CE7032E2677A78946A849DC4CDDE3A4D0CB81629242FB1A5");
         BN_hex2bn(&c, "49206f776520796f752024333030302e"); //HEX value of I owe you $3000.
         BN_hex2bn(&d, "74D806F9F3A62BAE331FFE3F0A68AFE35B3D2E4794148AACBC26AA381CD7D30D");

         //encryption and print the result
         BN_mod_exp(dec, c, d, n, ctx);

         printBN("encrypt message = ", dec);

         return 0;
}
```

Compile และ run code เพื่อทำการ sign message

```
[02/29/24]seed@VM:~$ gcc -o task4 task4.c -lcrypto
[02/29/24]seed@VM:~$ ./task4
encrypt message =  BCC20FB7568E5D48E434C387C06A6025E90D29D848AF9C3EBAC0135D99305822
[02/29/24]seed@VM:~$
```

พบว่าแม้ว่า message จะต่างกันแค่ตัวเดียวนั้นแต่ตัว encrypt message ที่ได้ออกมาแตกต่างอย่างเห็นได้ชัดเจนมาก