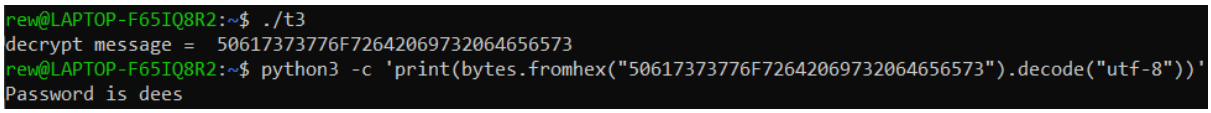
Task 3: Decrypting a Message

3.1ชุดคำสั่งภาษา C และ Python

```
#include <stdio.h>

#include <openssl/bn.h>

#define NBITS 256

// ฟังก์ชั่นสำหรับรับข้อความ, แปลงค่า BIGNUM -> String และ ปริ้นท์ค่า String ที่ได้ พร้อม message

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() { //ประกาศตัวแปรที่ใช้ใน Main

    BN_CTX *ctx = BN_CTX_new();

    BIGNUM *n = BN_new();

    BIGNUM *d = BN_new();

    BIGNUM *c = BN_new();

    BIGNUM *dec = BN_new(); //decrypt result

//from task2

BN_hex2bn(&n,

"DCBFFE3E51F62E09CE7032E2677A78946A849DC4CDDE3A4D0CB81629242FB1A5");

//given ciphertext c

BN_hex2bn(&c,

"8C0F971DF2F3672B28811407E2DABBE1DA0FEBBBDFC7DCB67396567EA1E2493F");
```

```
//private key from task2

BN_hex2bn(&d,
"74D806F9F3A62BAE331FFE3F0A68AFE35B3D2E4794148AACBC26AA381CD7D30D");

    BN_mod_exp(dec, c, d, n, ctx);  //decrypt function

    printBN("decrypt message = ", dec); //ส่งค่าไปแปลงและปริ้นท์

    return 0;

}
```

3.2 ภาพหน้าจอแสดงผลลัพธ์ของการทำงาน



3.3 อภิปราย ผลลัพธ์ / สิ่งที่สังเกตได้

เมื่อรันคำสั่ง ./t3 จะนำค่าใน โจทย์ไปคำนวณ Decrypt ด้วยสูตร c^d mod n ใน

BN_mod_exp(dec, c, d, n, ctx); และส่งค่า 50617373776F72642069732064656573 ออกมา

จากนั้นเราใช้ คำสั่ง python3 -c

'print(bytes.fromhex("50617373776F72642069732064656573").decode("utf-8"))' ในการแปลง hexadecimal ไปเป็น utf-8 เพื่อให้เราสามารถอ่านได้ ซึ่งได้คำตอบเป็น Password is dees ออกมา