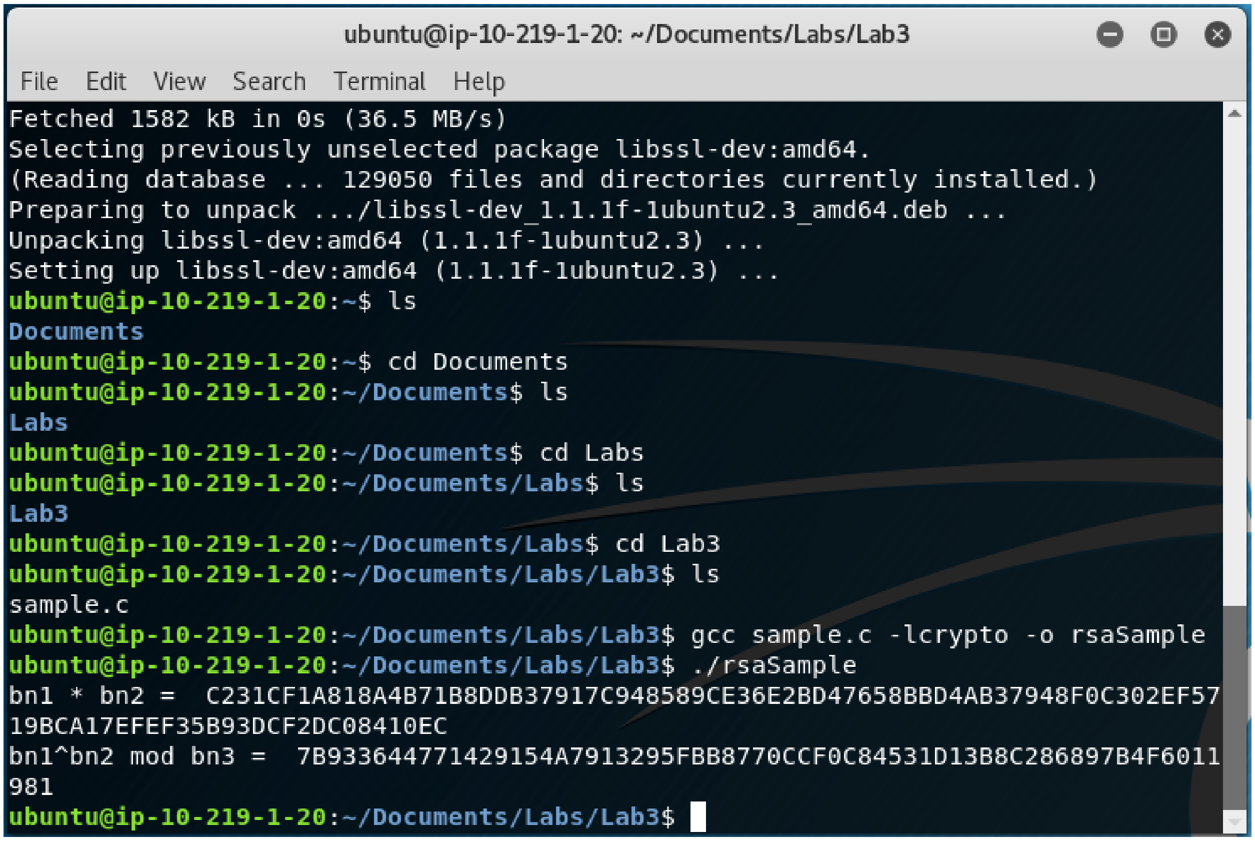
Lab 3 – RSA Encryption and Decryption Lab

Task 1.1

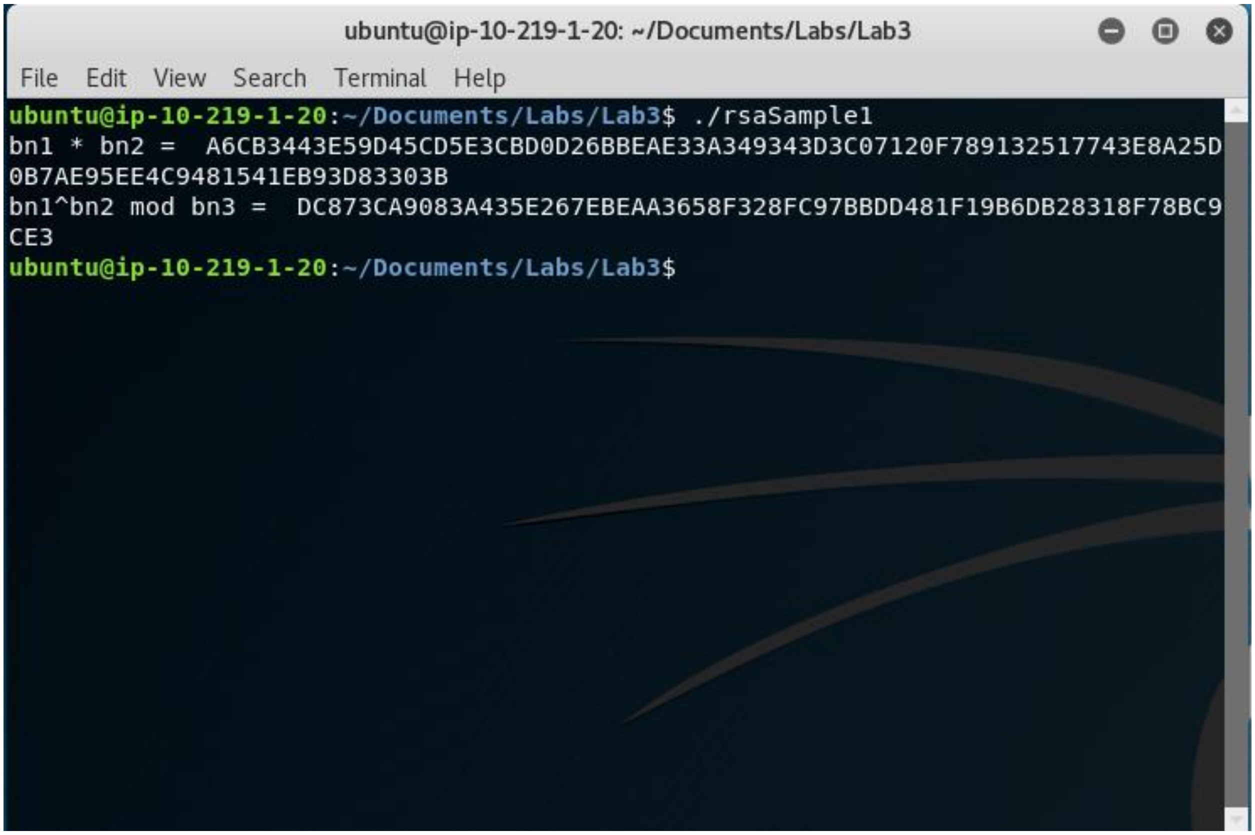


ubuntu@ip-10-219-1-20: ~/Documents/Labs/Lab3
File Edit View Search Terminal Help

```
Fetched 1582 kB in 0s (36.5 MB/s)
Selecting previously unselected package libssl-dev:amd64.
(Reading database ... 129050 files and directories currently installed.)
Preparing to unpack .../libssl-dev_1.1.1f-1ubuntu2.3_amd64.deb ...
Unpacking libssl-dev:amd64 (1.1.1f-1ubuntu2.3) ...
Setting up libssl-dev:amd64 (1.1.1f-1ubuntu2.3) ...
ubuntu@ip-10-219-1-20:~$ ls
Documents
ubuntu@ip-10-219-1-20:~$ cd Documents
ubuntu@ip-10-219-1-20:~/Documents$ ls
Labs
ubuntu@ip-10-219-1-20:~/Documents$ cd Labs
ubuntu@ip-10-219-1-20:~/Documents/Labs$ ls
Lab3
ubuntu@ip-10-219-1-20:~/Documents/Labs$ cd Lab3
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ ls
sample.c
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ gcc sample.c -lcrypto -o rsaSample
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ ./rsaSample
bn1 * bn2 =  C231CF1A818A4B71B8DDB37917C948589CE36E2BD47658BBD4AB37948F0C302EF57
19BCA17EFEF35B93DCF2DC08410EC
bn1^bn2 mod bn3 =  7B933644771429154A7913295FBB8770CCF0C84531D13B8C286897B4F6011
981
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$
```

Task 1.2

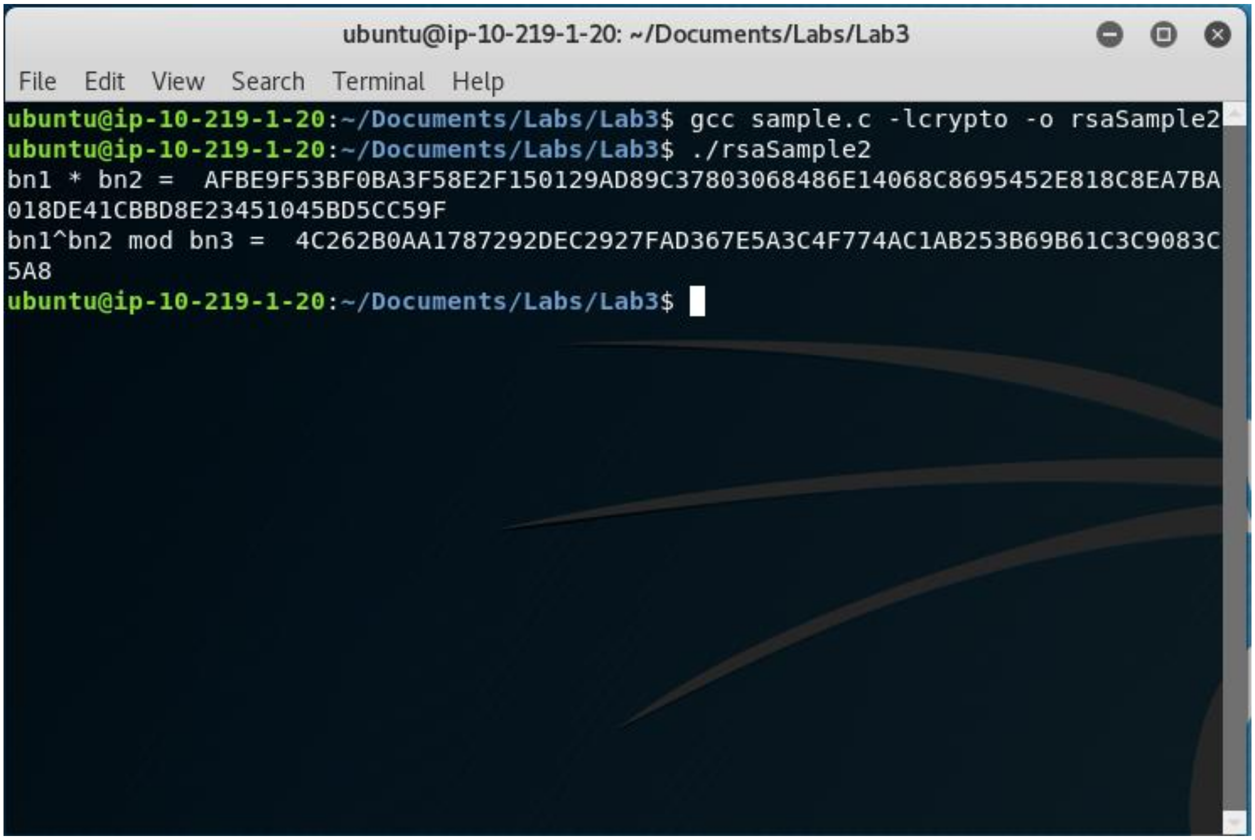
- Changing the last 9 digits of the string passed to bn2 to 123456789 (rsaSample1)



ubuntu@ip-10-219-1-20: ~/Documents/Labs/Lab3
File Edit View Search Terminal Help

```
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ ./rsaSample1
bn1 * bn2 =  A6CB3443E59D45CD5E3CBD0D26BBEAE33A349343D3C07120F789132517743E8A25D
0B7AE95EE4C9481541EB93D83303B
bn1^bn2 mod bn3 =  DC873CA9083A435E267EBEAA3658F328FC97BBDD481F19B6DB28318F78BC9
CE3
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$
```

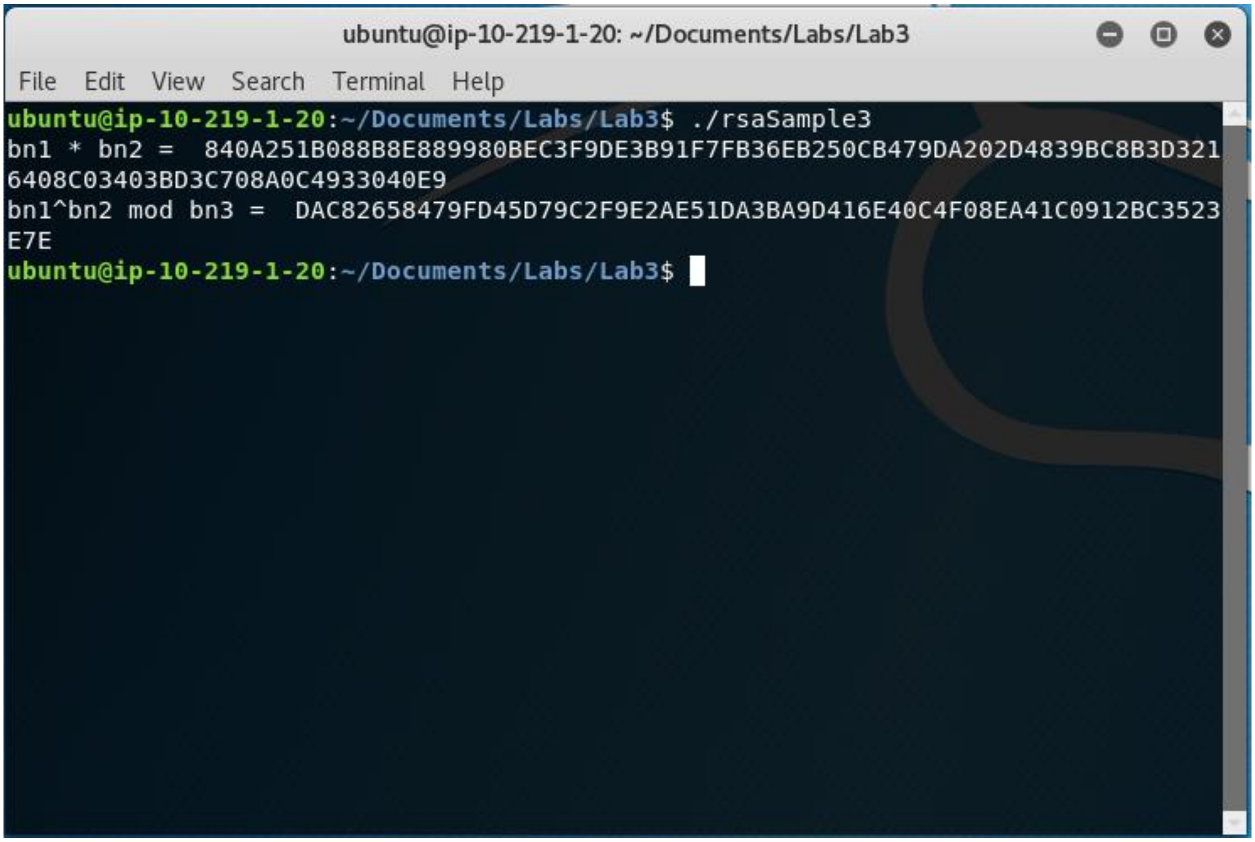
- Changing the last two parameters of the bn3 function to 1 and 2 (rsaSample2)



ubuntu@ip-10-219-1-20: ~/Documents/Labs/Lab3
File Edit View Search Terminal Help

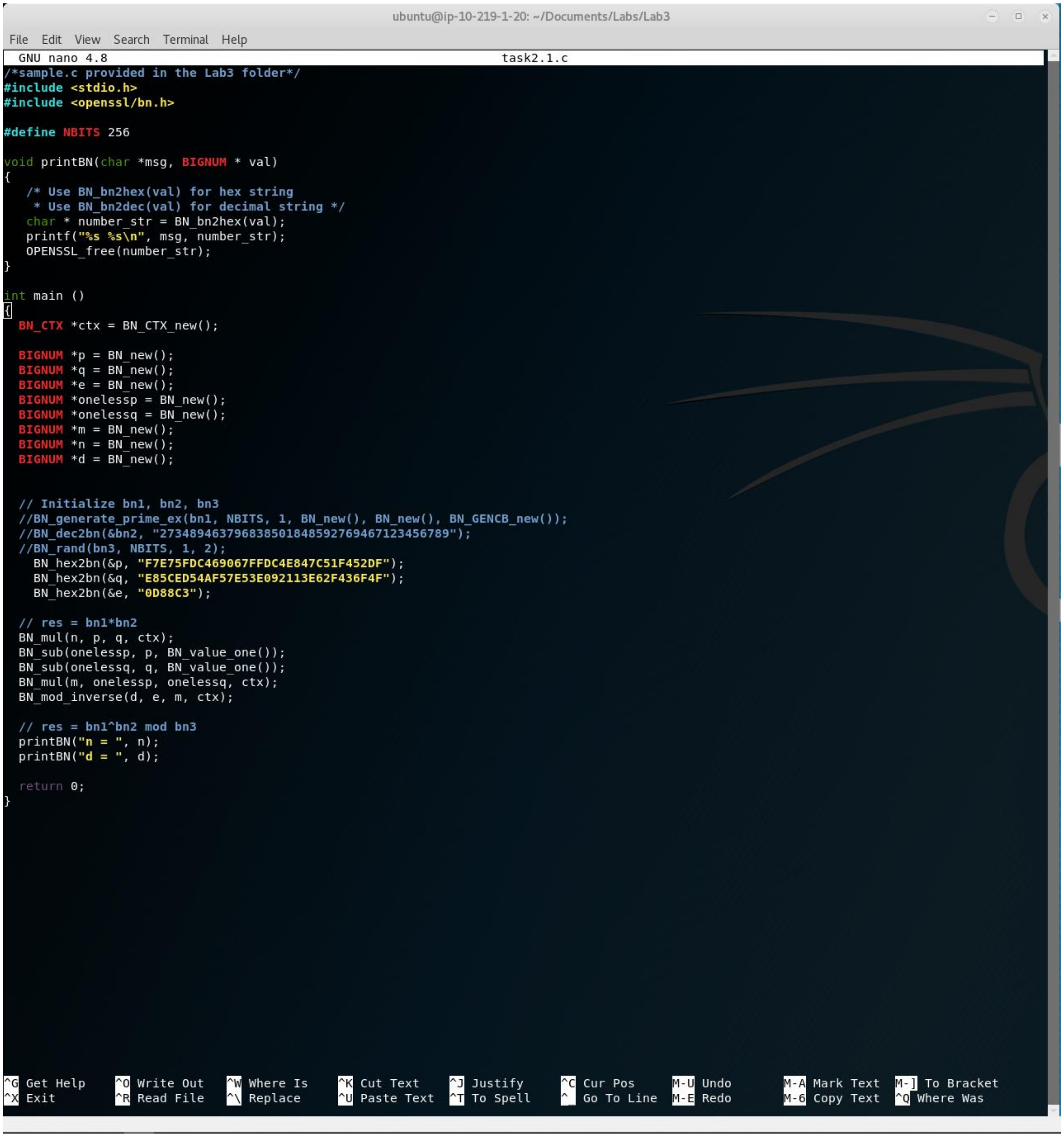
```
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ gcc sample.c -lcrypto -o rsaSample2
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ ./rsaSample2
bn1 * bn2 =  AFBE9F53BF0BA3F58E2F150129AD89C37803068486E14068C8695452E818C8EA7BA
018DE41CBBD8E23451045BD5CC59F
bn1^bn2 mod bn3 =  4C262B0AA1787292DEC2927FAD367E5A3C4F774AC1AB253B69B61C3C9083C
5A8
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ 
```

- Changing the three null values for bn1 to BN_new(), BN_new(), and BN_GENCB_new() respectively (rsaSample3)
    - This was done with trial and error of reading the compiler error output to see what object types it was looking for and creating those new objects with the library functions respectively.


ubuntu@ip-10-219-1-20: ~/Documents/Labs/Lab3
File Edit View Search Terminal Help

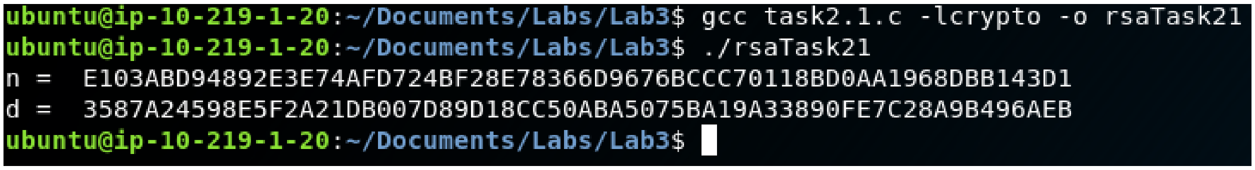
```
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ ./rsaSample3
bn1 * bn2 =  840A251B088B8E889980BEC3F9DE3B91F7FB36EB250CB479DA202D4839BC8B3D321
6408C03403BD3C708A0C4933040E9
bn1^bn2 mod bn3 =  DAC82658479FD45D79C2F9E2AE51DA3BA9D416E40C4F08EA41C0912BC3523
E7E
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ 
```

Task 2.1



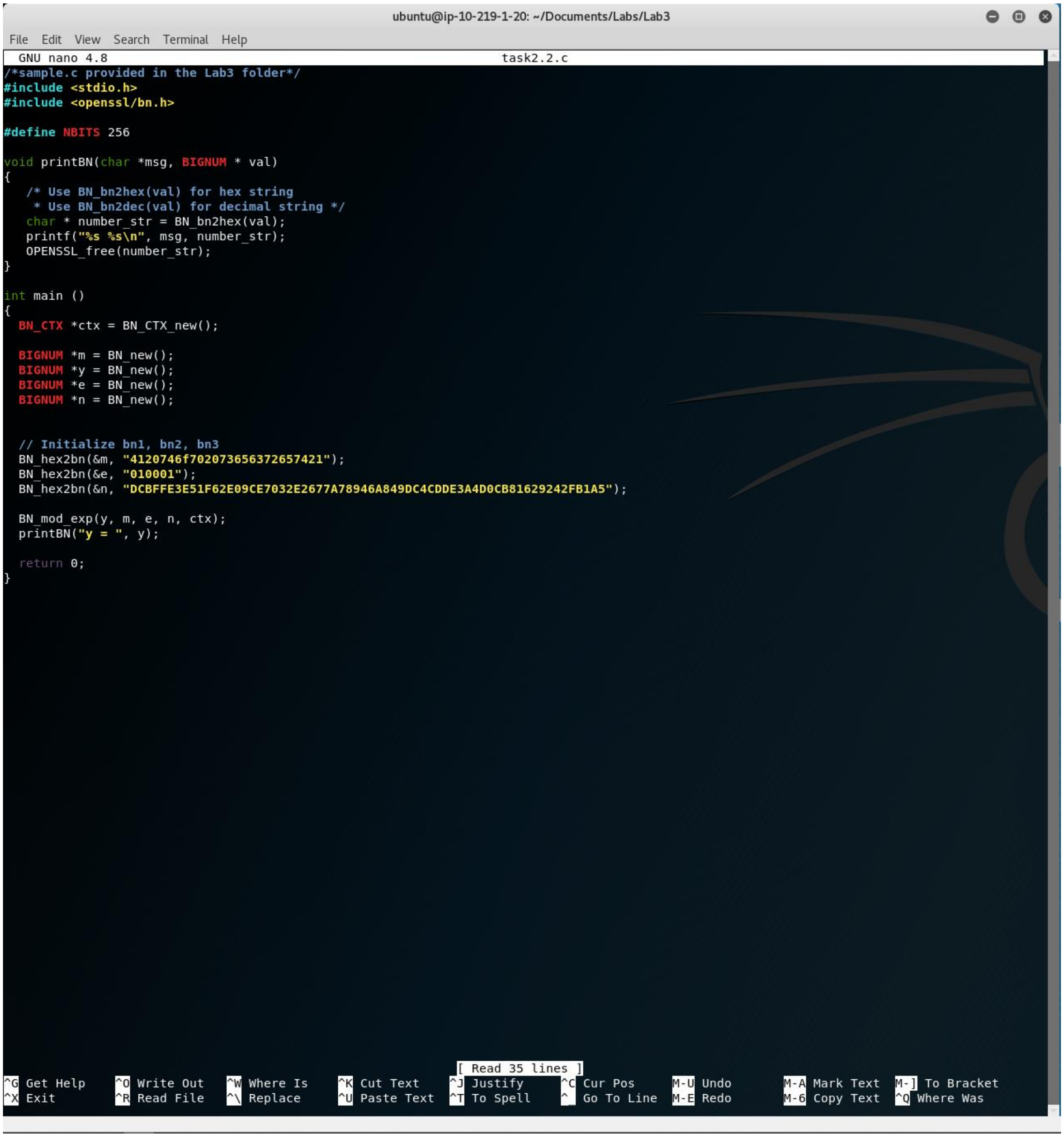
ubuntu@ip-10-219-1-20: ~/Documents/Labs/Lab3
File Edit View Search Terminal Help

```
  GNU nano 4.8                                          task2.1.c
/*sample.c provided in the Lab3 folder*/
#include <stdio.h>
#include <openssl/bn.h>

#define NBITS 256

void printBN(char *msg, BIGNUM * val)
{
   /* Use BN_bn2hex(val) for hex string
    * Use BN_bn2dec(val) for decimal string */
   char * number_str = BN_bn2hex(val);
   printf("%s %s\n", msg, number_str);
   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 *onelessp = BN_new();
  BIGNUM *onelessq = BN_new();
  BIGNUM *m = BN_new();
  BIGNUM *n = BN_new();
  BIGNUM *d = BN_new();


  // Initialize bn1, bn2, bn3
  //BN_generate_prime_ex(bn1, NBITS, 1, BN_new(), BN_new(), BN_GENCB_new());
  //BN_dec2bn(&bn2, "273489463796838501848592769467123456789");
  //BN_rand(bn3, NBITS, 1, 2);
    BN_hex2bn(&p, "F7E75FDC469067FFDC4E847C51F452DF");
    BN_hex2bn(&q, "E85CED54AF57E53E092113E62F436F4F");
    BN_hex2bn(&e, "0D88C3");

  // res = bn1*bn2
  BN_mul(n, p, q, ctx);
  BN_sub(onelessp, p, BN_value_one());
  BN_sub(onelessq, q, BN_value_one());
  BN_mul(m, onelessp, onelessq, ctx);
  BN_mod_inverse(d, e, m, ctx);

  // res = bn1^bn2 mod bn3
  printBN("n = ", n);
  printBN("d = ", d);

  return 0;
}
```

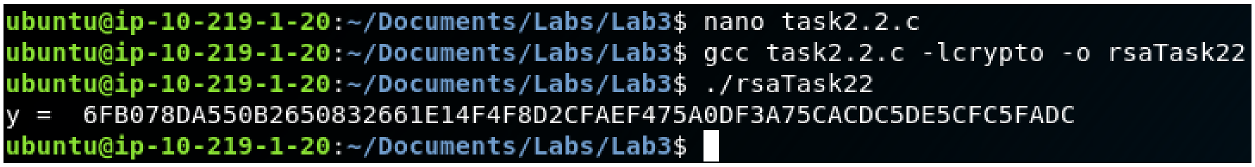


```
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ gcc task2.1.c -lcrypto -o rsaTask21
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ ./rsaTask21
n =  E103ABD94892E3E74AFD724BF28E78366D9676BCCC70118BD0AA1968DBB143D1
d =  3587A24598E5F2A21DB007D89D18CC50ABA5075BA19A33890FE7C28A9B496AEB
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ 
```

Task 2.2

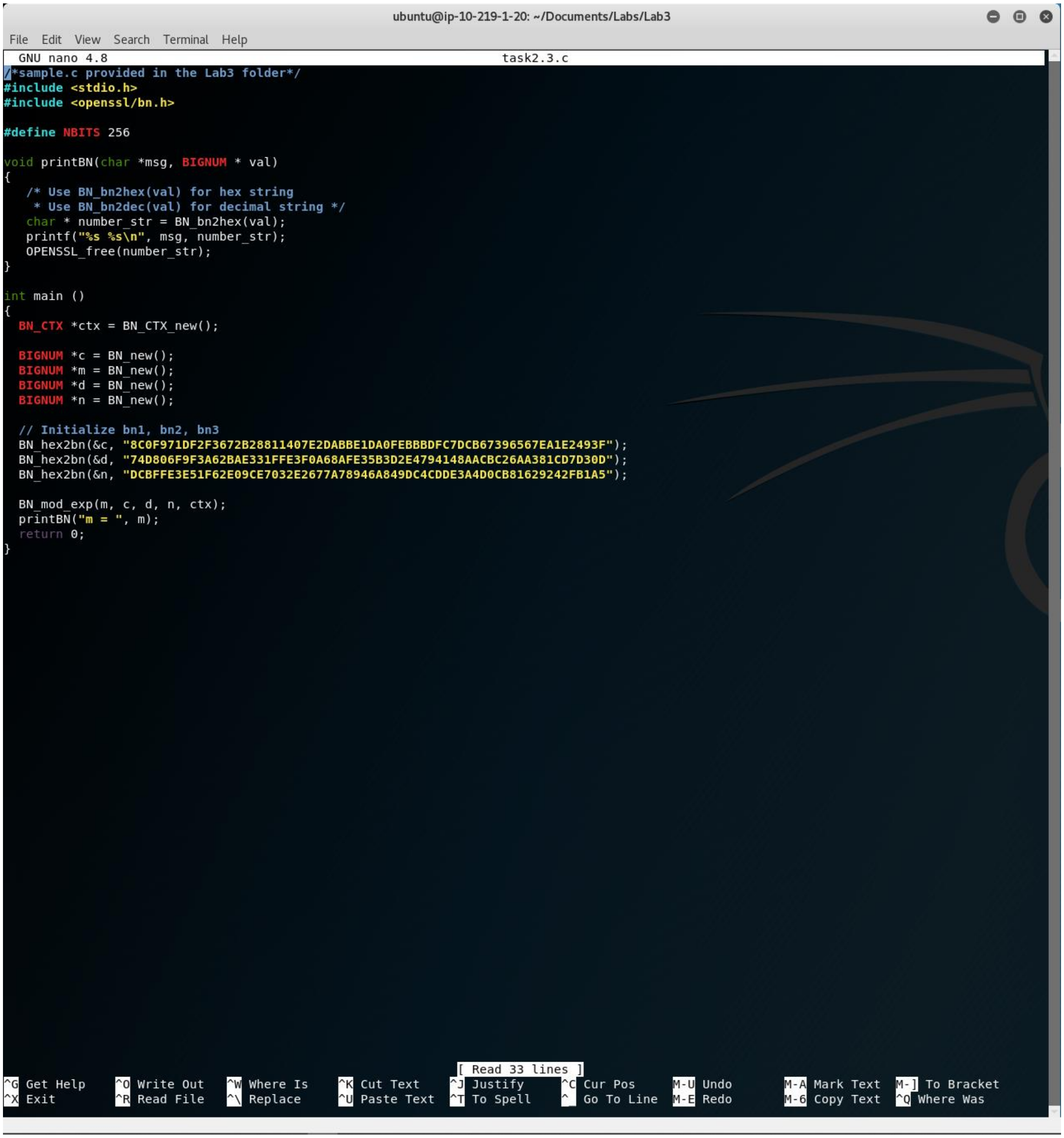


```
/*sample.c provided in the Lab3 folder*/
#include <stdio.h>
#include <openssl/bn.h>

#define NBITS 256

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

int main ()
{
  BN_CTX *ctx = BN_CTX_new();

  BIGNUM *m = BN_new();
  BIGNUM *y = BN_new();
  BIGNUM *e = BN_new();
  BIGNUM *n = BN_new();


  // Initialize bn1, bn2, bn3
  BN_hex2bn(&m, "4120746f702073656372657421");
  BN_hex2bn(&e, "010001");
  BN_hex2bn(&n, "DCBFFE3E51F62E09CE7032E2677A78946A849DC4CDDE3A4D0CB81629242FB1A5");

  BN_mod_exp(y, m, e, n, ctx);
  printBN("y = ", y);

  return 0;
}
```

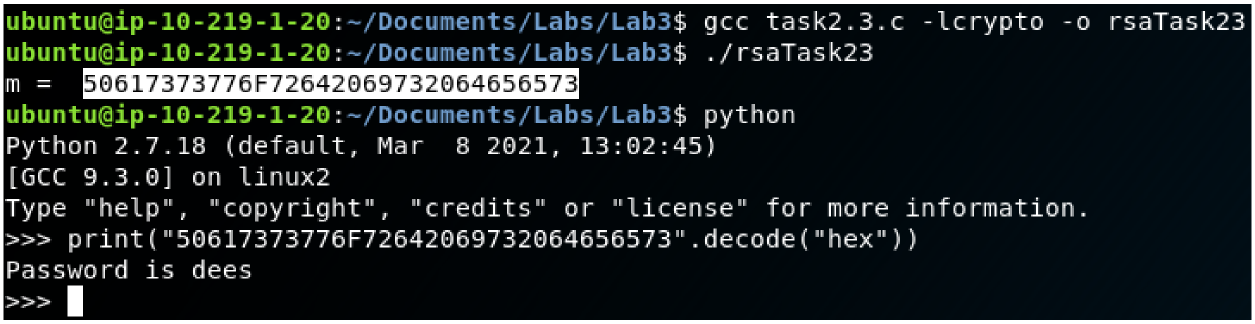


```
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ nano task2.2.c
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ gcc task2.2.c -lcrypto -o rsaTask22
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ ./rsaTask22
y =  6FB078DA550B2650832661E14F4F8D2CFAEF475A0DF3A75CACDC5DE5CFC5FADC
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ 
```

Task 2.3


ubuntu@ip-10-219-1-20: ~/Documents/Labs/Lab3
File Edit View Search Terminal Help

```
  GNU nano 4.8                                         task2.3.c
/*sample.c provided in the Lab3 folder*/
#include <stdio.h>
#include <openssl/bn.h>

#define NBITS 256

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

int main ()
{
  BN_CTX *ctx = BN_CTX_new();

  BIGNUM *c = BN_new();
  BIGNUM *m = BN_new();
  BIGNUM *d = BN_new();
  BIGNUM *n = BN_new();

  // Initialize bn1, bn2, bn3
  BN_hex2bn(&c, "8C0F971DF2F3672B28811407E2DABBE1DA0FEBBBDFC7DCB67396567EA1E2493F");
  BN_hex2bn(&d, "74D806F9F3A62BAE331FFE3F0A68AFE35B3D2E4794148AACBC26AA381CD7D30D");
  BN_hex2bn(&n, "DCBFFE3E51F62E09CE7032E2677A78946A849DC4CDDE3A4D0CB81629242FB1A5");

  BN_mod_exp(m, c, d, n, ctx);
  printBN("m = ", m);
  return 0;
}

                                                            [ Read 33 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text  M-] To Bracket
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo       M-6 Copy Text  ^Q Where Was
```



```
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ gcc task2.3.c -lcrypto -o rsaTask23
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ ./rsaTask23
m =  50617373776F72642069732064656573
ubuntu@ip-10-219-1-20:~/Documents/Labs/Lab3$ python
Python 2.7.18 (default, Mar  8 2021, 13:02:45)
[GCC 9.3.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> print("50617373776F72642069732064656573".decode("hex"))
Password is dees
>>> 
```