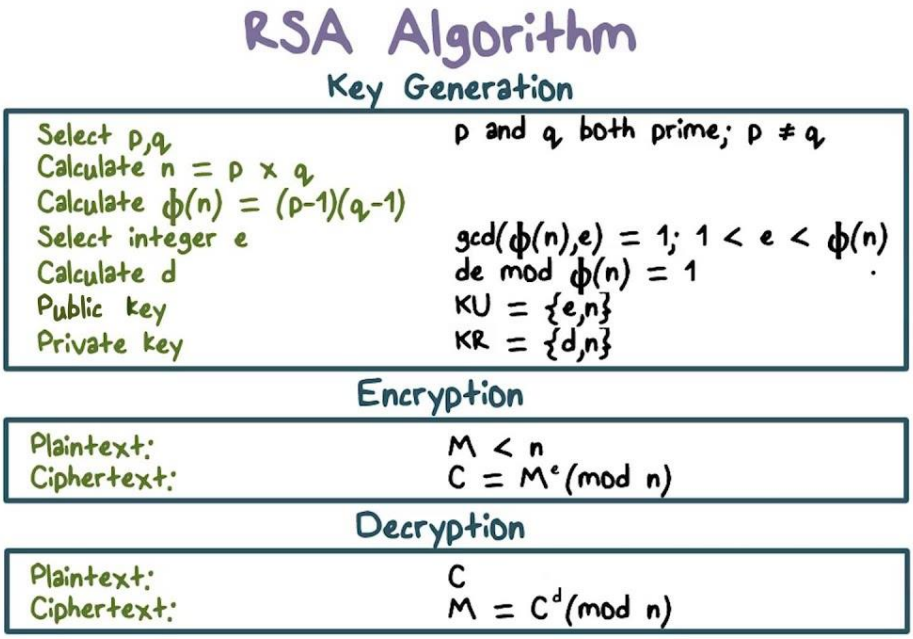
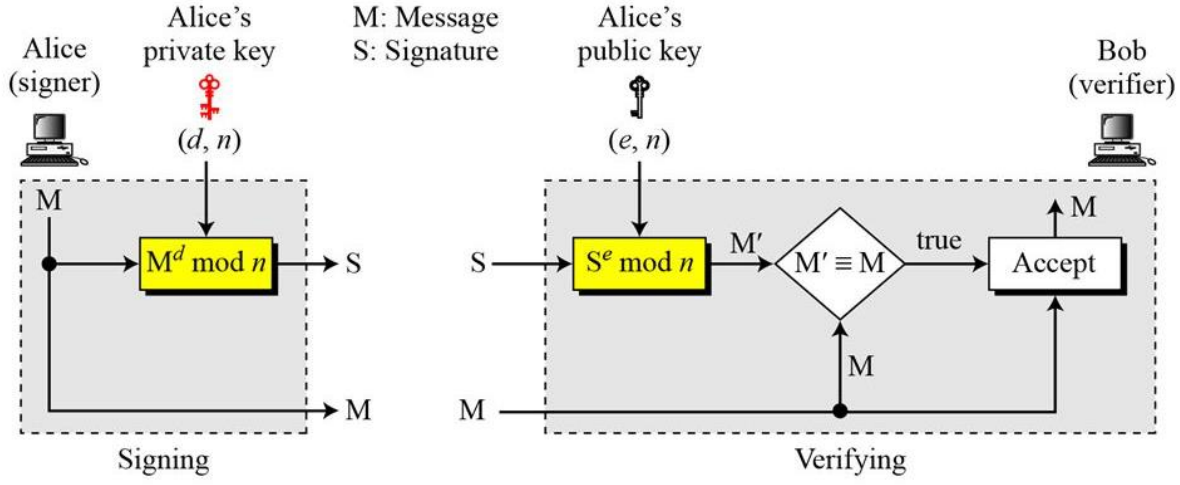
姓名：蔡佩蓉　　學號：109511286

RSA Public-Key Encryption and Signature Lab (Lab3)

RSA Encryption and Decryption:



RSA Signing and Verifying:



$$M' \equiv M \pmod{n} \quad \rightarrow \quad S^e \equiv M \pmod{n} \quad \rightarrow \quad M^{d \times e} \equiv M \pmod{n}$$

Task 1: Deriving the Private Key

Open Task1.c ~/Desktop Save

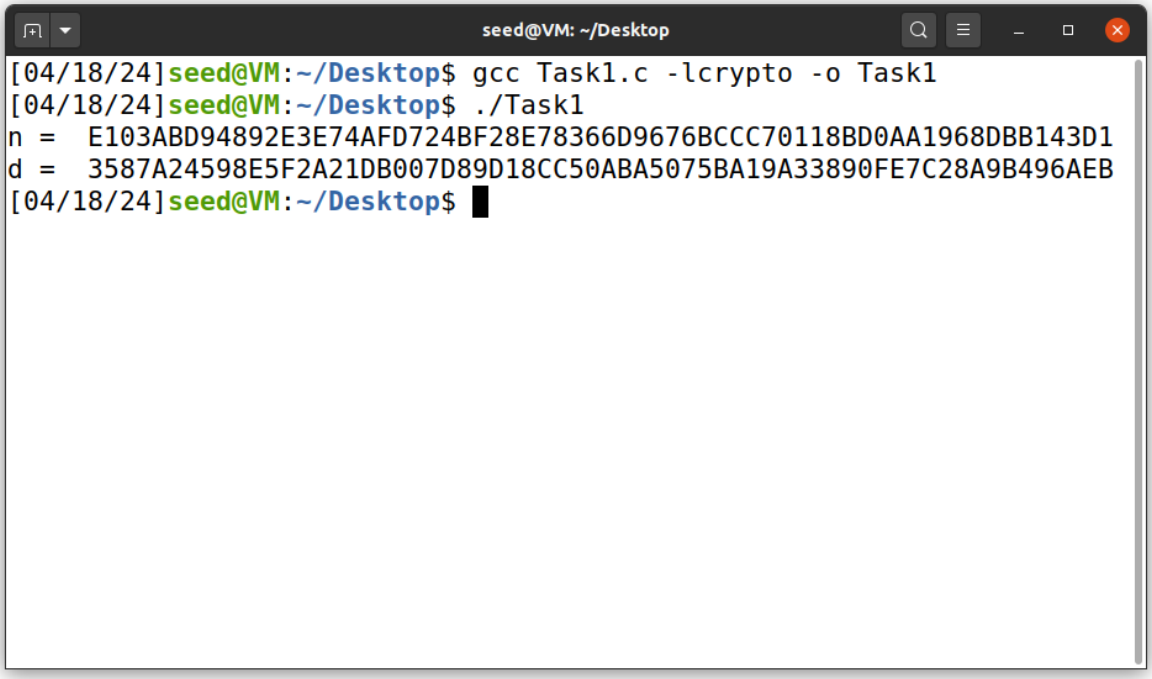
```c
#include <stdio.h>
#include <openssl/bn.h>

#define NBITS 128

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

```

C Tab Width: 8 Ln 1, Col 1 INS

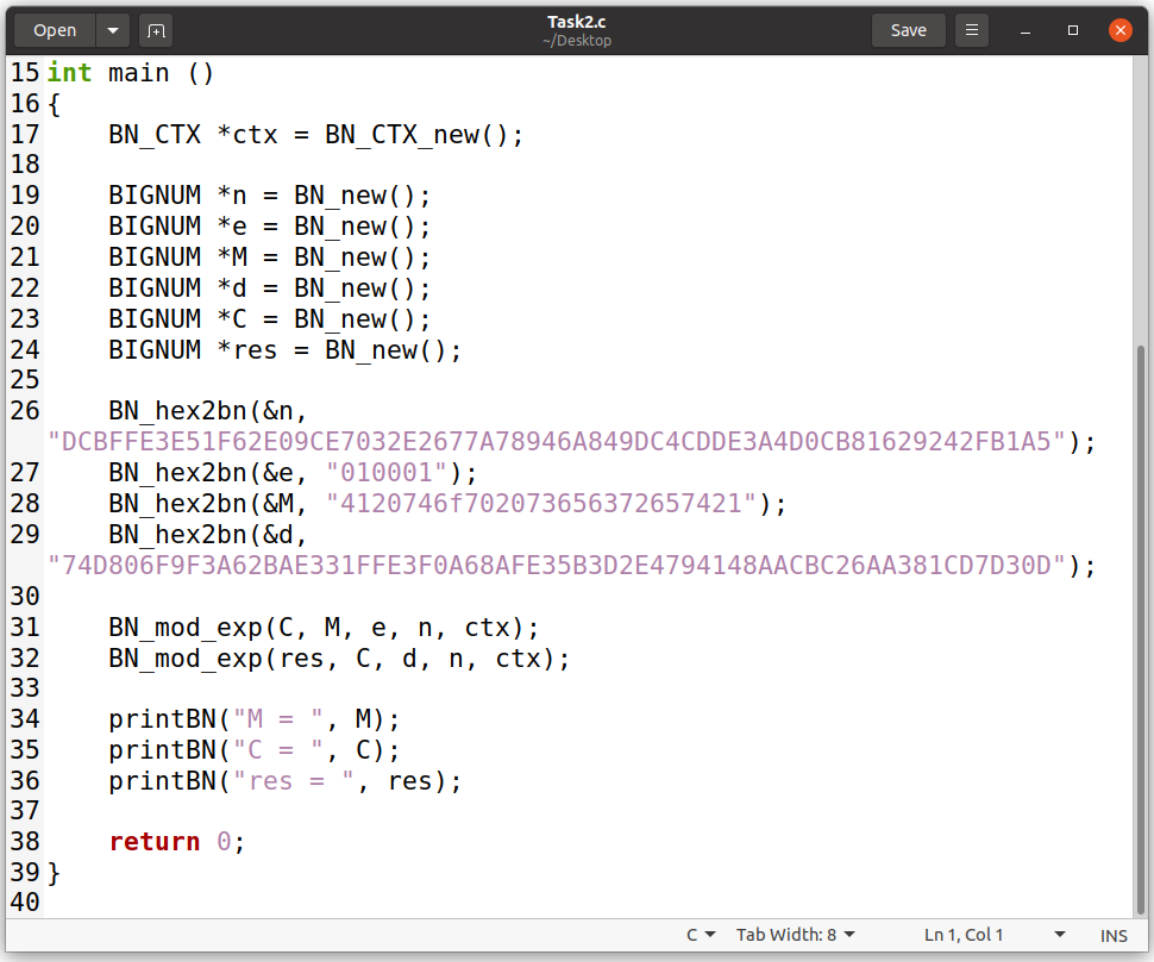
Open Task1.c ~/Desktop Save

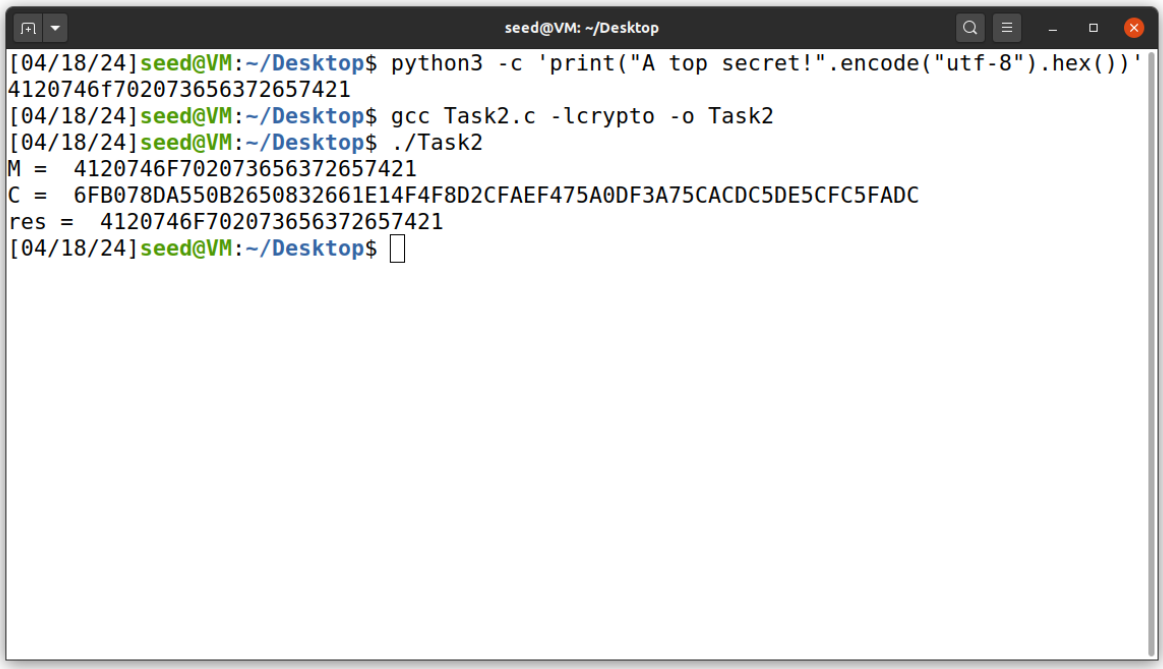
```c

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

    BIGNUM *p = BN_new();
    BIGNUM *q = BN_new();
    BIGNUM *e = BN_new();
    BIGNUM *p_1 = BN_new();
    BIGNUM *q_1 = BN_new();
    BIGNUM *n = BN_new();
    BIGNUM *phi_n = BN_new();
    BIGNUM *d = BN_new();

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

    BN_sub(p_1, p, BN_value_one());
    BN_sub(q_1, q, BN_value_one());
    BN_mul(n, p, q, ctx);
    BN_mul(phi_n, p_1, q_1, ctx);

    BN_mod_inverse(d, e, phi_n, ctx);

    printBN("n = ", n);
    printBN("d = ", d);

    return 0;
}
```

C Tab Width: 8 Ln 1, Col 1 INS



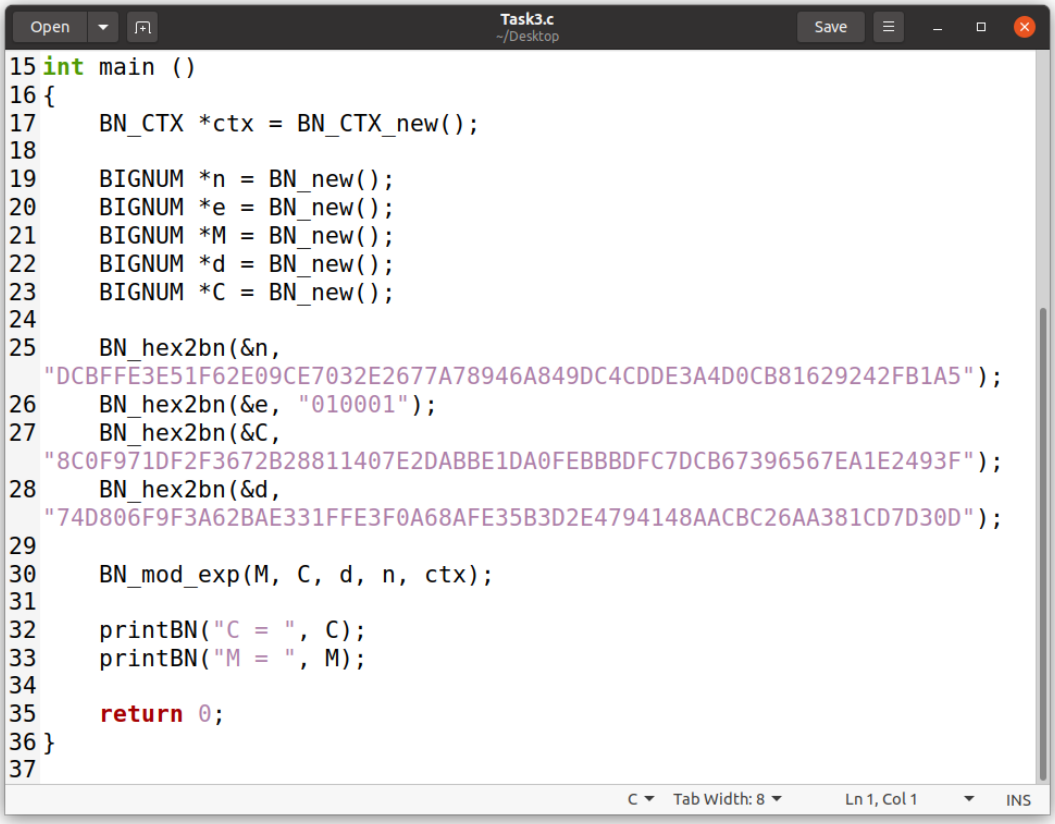
Task 2: Encrypting a Message

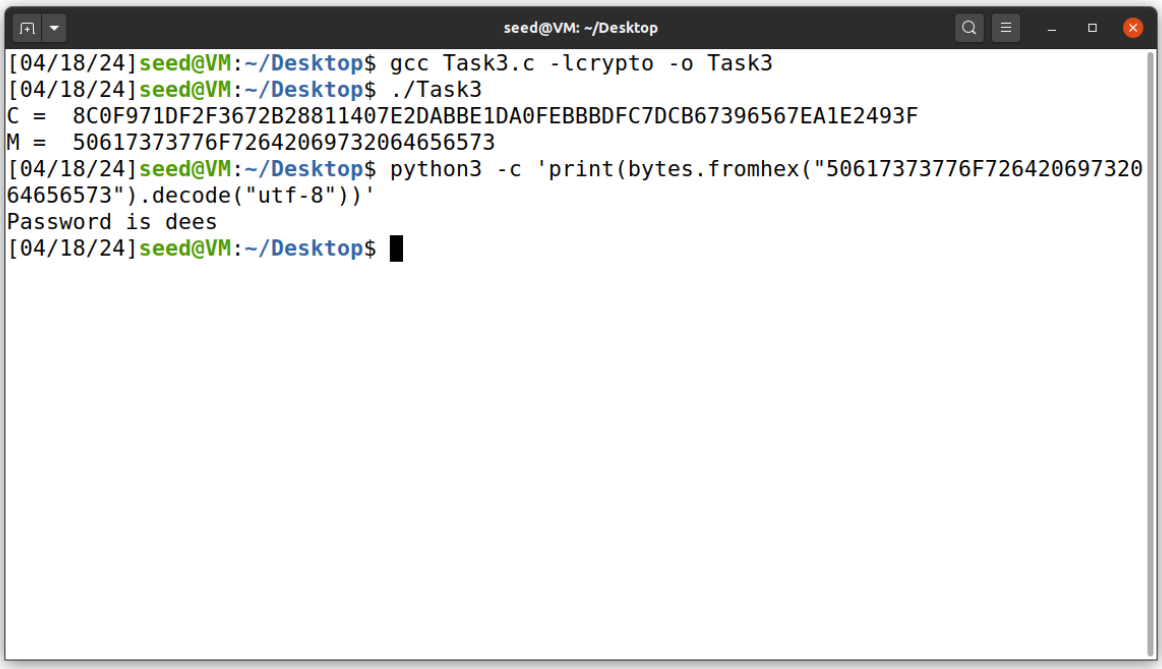




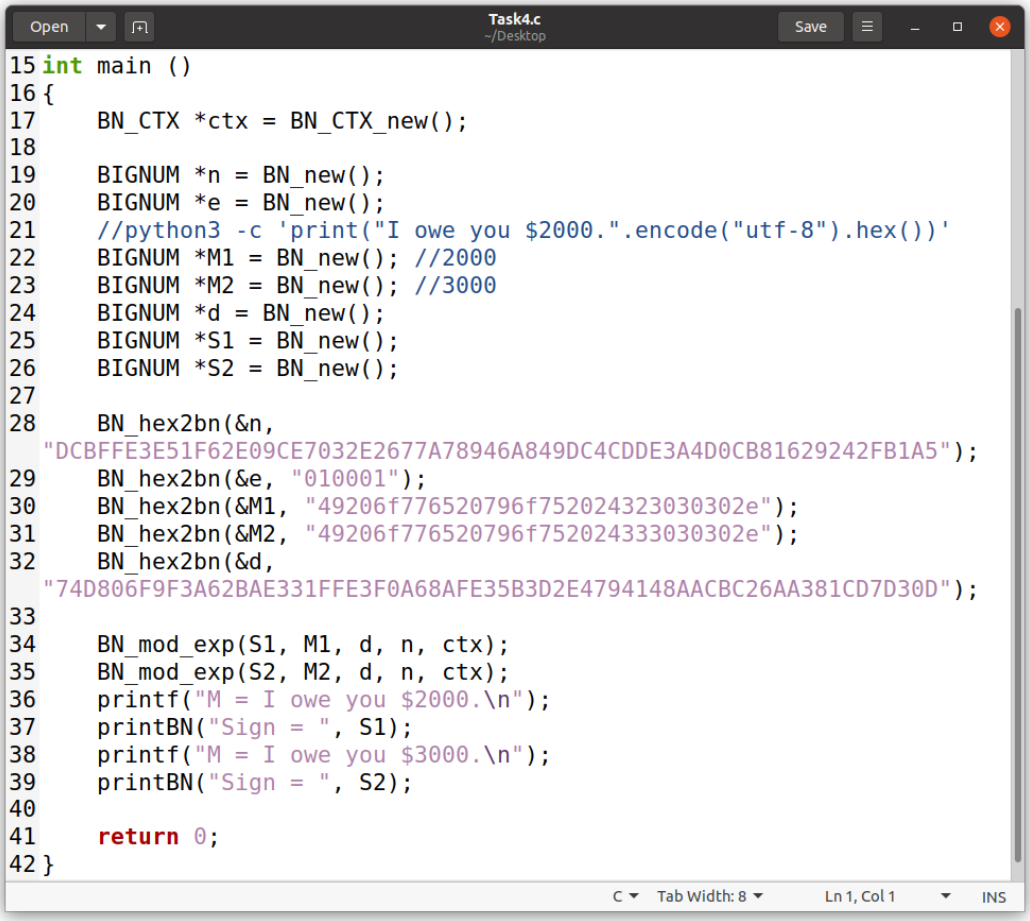
M is plaintext before encryption while res is plaintext after encryption (decrypt the ciphertext). We verified the encryption result by comparing M and res (both same values).

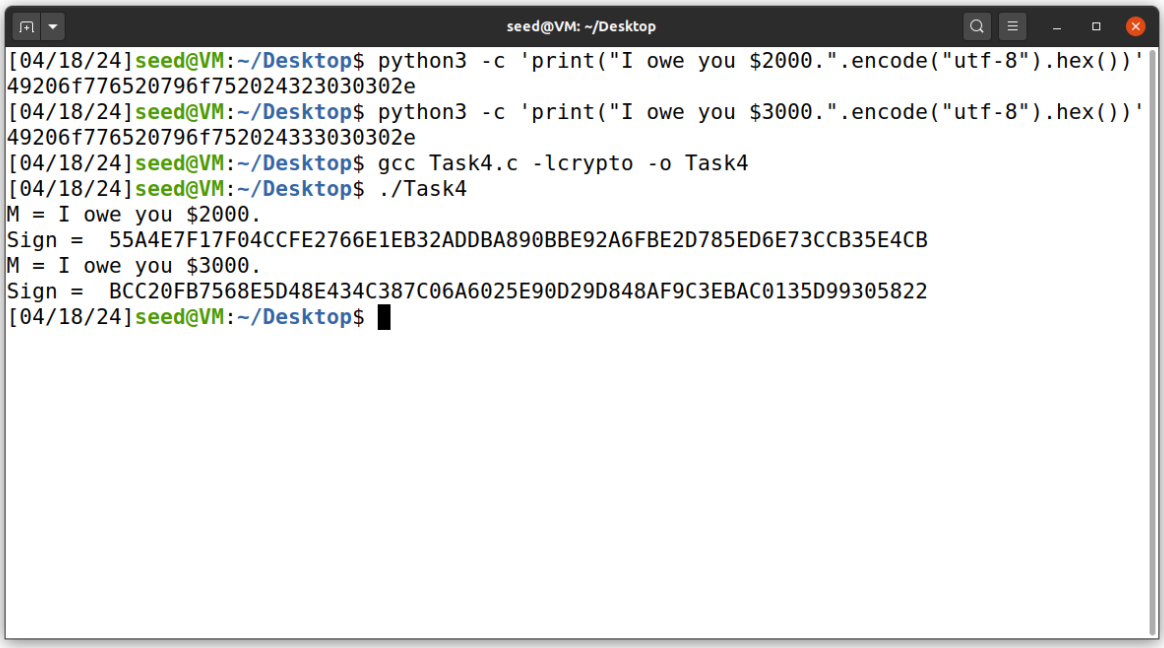
Task 3: Decrypting a Message





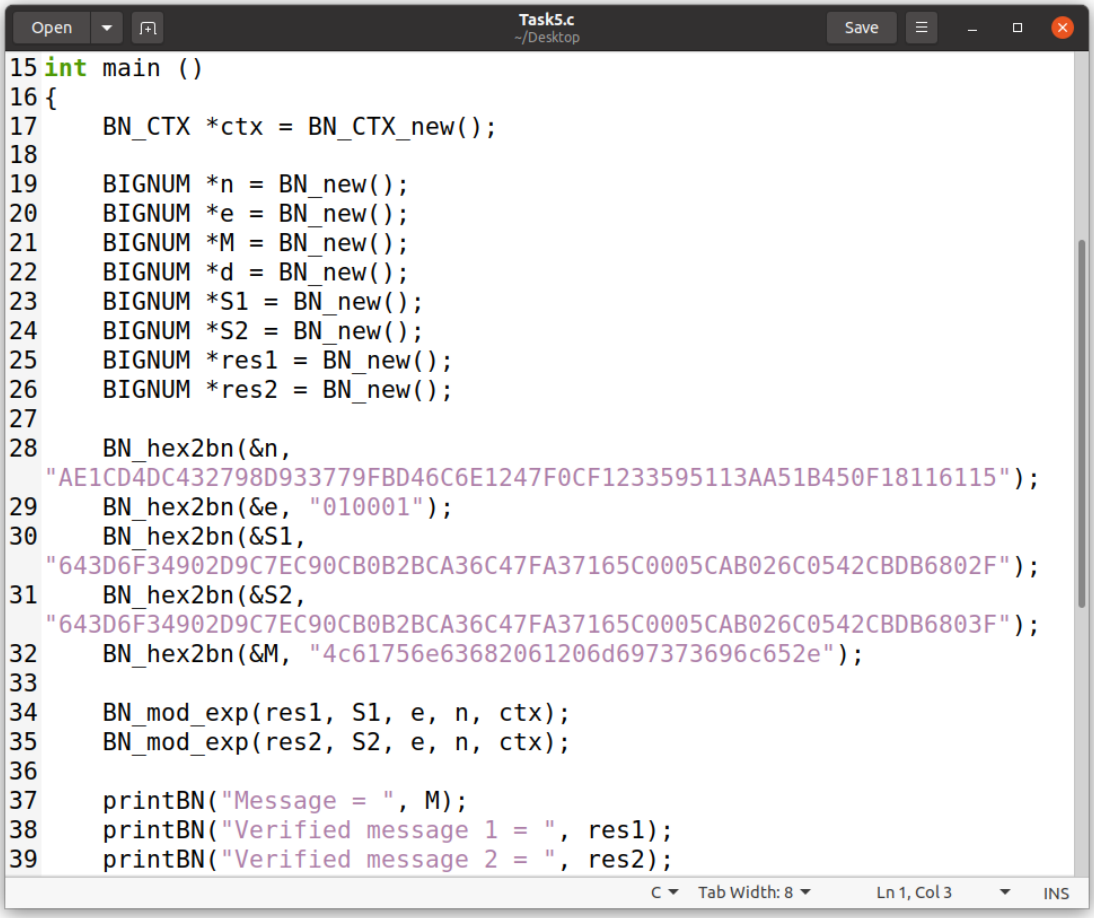
Task 4: Signing a Message

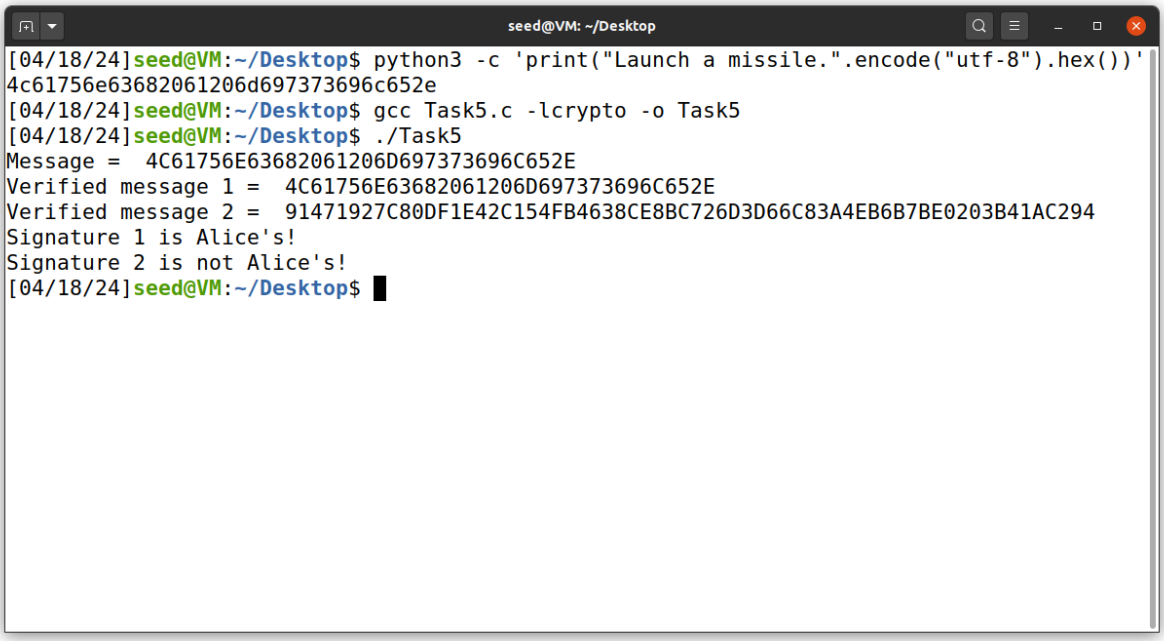




We observed that a slight change to the message M can result to totally different signatures.

Task 5: Verifying a Signature





Signature 1's last byte is 2F which generate Verified message 1; Signature 2's last byte is 3F which generate Verified message 2. Compare both Verified message 1 and 2 with Message, we observed that Verified message 1 is similar with Message while Verified message 2 not, hence we say that Signature 1 is Alice's while Signature 2 is not.

Task 6: Manually Verifying an X.509 Certificate

Open ▾ Task6.c ~/Desktop Save

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

#define NBITS 256

void printBN(char *msg, BIGNUM * a)
{
    /* Use BN_bn2hex(a) for hex string
    * Use BN_bn2dec(a) for decimal string */
    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 *e = BN_new();
    BIGNUM *n = BN_new();
    BIGNUM *S = BN_new();
    BIGNUM *res = BN_new();

    BN_hex2bn(&n,
"CCF710624FA6BB636FED905256C56D277B7A12568AF1F4F9D6E7E18FBD95ABF260411570DB1200FA270AB557385B7DB2519371950E6A41945B351BFA7BFABBC5BE2430FE56E
    BN_hex2bn(&e, "10001");
    BN_hex2bn(&S,
"04e16e023e0de32346f4e3963505933522020b845de27386d4744ffc1b27af3ecaadc3ce46d6fa0fe271f90d1a9a13b7d50848bd5058b35e20638629ca3ecccc7826e1598f5


    BN_mod_exp(res, S, e, n, ctx);
    printBN("Verify signature:", res);

    return 0;
}
```

C ▾ Tab Width: 8 ▾ Ln 1, Col 1 ▾ INS

seed@VM: ~/Desktop

```
[04/18/24]seed@VM:~/Desktop$ openssl x509 -in c1.pem -noout -modulus
Modulus=CCF710624FA6BB636FED905256C56D277B7A12568AF1F4F9D6E7E18FBD95ABF260411570DB1200FA270AB557385B7DB2519371950E6A41945B351BFA7BFABBC5BE2430FE56EFC4F37D97E314F5144D
CBA710F216EAAB22F031221161699026BA78D9971FE37D66AB75449573C8ACFFEF5D0A8A5943E1ACB23A0FF348FCD76B37C163DCDE46D6DB45FE7D23FD90E851071E51A35FED4946547F2C88C5F4139C97153C
03E8A139DC690C32C1AF16574C9447427CA2C89C7DE6D44D54AF4299A8C104C2779CD648E4CE11E02A8099F04370CF3F766BD14C49AB245EC20D82FD46A8AB6C93CC6252427592F89AFA5E5EB2B061E51F1FB9
7F0998E83DFA837F4769A1
[04/18/24]seed@VM:~/Desktop$ openssl x509 -in c1.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:f5:bd:06:2b:56:02:f4:7a:b8:50:2c:23:cc:f0:66
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
        Validity
            Not Before: Mar 30 00:00:00 2021 GMT
            Not After : Mar 29 23:59:59 2031 GMT
        Subject: C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:cc:f7:10:62:4f:a6:bb:63:6f:ed:90:52:56:c5:
                    6d:27:7b:7a:12:56:8a:f1:f4:f9:d6:e7:e1:8f:bd:
                    95:ab:f2:60:41:15:70:db:12:00:fa:27:0a:b5:57:
                    38:5b:7d:b2:51:93:71:95:0e:6a:41:94:5b:35:1b:
                    fa:7b:fa:bb:c5:be:24:30:fe:56:ef:c4:f3:7d:97:
                    e3:14:f5:14:4d:cb:a7:10:f2:16:ea:ab:22:f0:31:
                    22:11:61:69:90:26:ba:78:d9:97:1f:e3:7d:66:ab:
                    75:44:95:73:c8:ac:ff:ef:5d:0a:8a:59:43:e1:ac:
                    b2:3a:0f:f3:48:fc:d7:6b:37:c1:63:dc:de:46:d6:
                    db:45:fe:7d:23:fd:90:e8:51:07:1e:51:a3:5f:ed:
                    49:46:54:7f:2c:88:c5:f4:13:9c:97:15:3c:03:e8:
                    a1:39:dc:69:0c:32:c1:af:16:57:4c:94:47:42:7c:
                    a2:c8:9c:7d:e6:d4:4d:54:af:42:99:a8:c1:04:c2:
                    77:9c:d6:48:e4:ce:11:e0:2a:80:99:f0:43:70:cf:
                    3f:76:6b:d1:4c:49:ab:24:5e:c2:0d:82:fd:46:a8:
                    ab:6c:93:cc:62:52:42:75:92:f8:9a:fa:5e:5e:b2:
                    b0:61:e5:1f:1f:b9:7f:09:98:e8:3d:fa:83:7f:47:
                    69:a1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Subject Key Identifier:
                74:85:80:C0:66:C7:DF:37:DE:CF:BD:29:37:AA:03:1D:BE:ED:CD:17
```

```
[04/18/24]seed@VM:~/Desktop$  openssl x509 -in c0.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            07:5b:ce:f3:06:89:c8:ad:df:13:e5:1a:f4:af:e1:87
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = DigiCert Inc, CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
        Validity
            Not Before: Jan 30 00:00:00 2024 GMT
            Not After : Mar  1 23:59:59 2025 GMT
        Subject: C = US, ST = California, L = Los Angeles, O = Internet\C2\A0Corporation\C2\A0for\C2\A0Assigned\C2\A0Names\C2\A0and\C2\A0Numbers, CN = www.example.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:86:85:0f:bb:0e:f9:ca:5f:d9:f5:e0:0a:32:2c:
                    33:d9:aa:0e:07:29:a8:2f:08:ad:78:bd:c2:06:bf:
                    f7:2d:2b:a6:a7:27:3d:53:a6:4c:c3:4b:b2:27:77:
                    20:d6:c1:54:49:b8:08:da:f9:70:a9:61:f6:b2:49:
                    9d:69:57:da:fb:6d:24:34:72:2e:47:f0:04:3f:9d:
                    b1:5b:e2:bc:66:31:59:32:e6:a9:7e:bf:d4:b0:d4:
                    64:f5:6b:ca:7b:ff:72:5b:5e:9a:d8:3f:d4:06:b2:
                    f3:c8:dc:8f:66:5a:46:84:66:a8:18:15:79:a7:08:
                    ce:05:3c:fb:39:89:ef:6d:fa:4e:71:52:7b:b7:e4:
                    a0:a4:9c:96:c0:61:3d:a4:0a:70:4d:c3:8e:cd:6e:
                    b3:32:6c:f2:c7:44:09:04:dd:a0:55:fd:23:a5:20:
                    78:b2:85:5e:d8:3b:ad:17:ff:85:c5:b9:74:8d:33:
                    b9:b8:57:6e:b5:bc:69:65:db:0b:3c:92:55:99:f4:
                    73:b4:64:24:ca:67:4c:28:99:cc:dc:67:3d:79:c7:
                    16:9c:2b:e6:ab:aa:aa:35:72:37:f6:81:2a:48:e8:
                    3f:4e:19:9a:bf:9e:46:aa:32:93:ff:a5:b2:5a:b4:
                    b1:2f:1e:69:84:92:1d:b0:b9:8d:af:f2:31:6c:95:
                    86:f3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:74:85:80:C0:66:C7:DF:37:DE:CF:BD:29:37:AA:03:1D:BE:ED:CD:17

            X509v3 Subject Key Identifier:
                4C:FE:D0:12:4D:2E:21:CF:6B:FA:F2:F2:B8:4C:49:02:1D:31:91:8A
            X509v3 Subject Alternative Name:
                DNS:www.example.org, DNS:example.net, DNS:example.edu, DNS:example.com, DNS:example.org, DNS:www.example.com, DNS:www.example.edu, DNS:www.example.net
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.2
```

```
                                77:63:40:73:02:21:00:B2:E8:09:3F:66:4C:C3:7D:3B:
                                21:73:20:15:79:32:45:D5:2F:2B:93:7F:63:80:CC:03:
                                9A:ED:DF:31:D8:7E:97
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : E6:D2:31:63:40:77:8C:C1:10:41:06:D7:71:B9:CE:C1:
                                D2:40:F6:96:84:86:FB:BA:87:32:1D:FD:1E:37:8E:50
                    Timestamp : Jan 30 19:22:50.335 2024 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:46:02:21:00:E0:AA:21:FD:58:B3:75:05:35:B6:36:
                                76:13:65:46:81:64:97:5E:4C:27:42:68:98:86:60:1E:
                                29:C5:4B:1D:E0:02:21:00:FB:24:81:85:B1:D1:A8:97:
                                B9:2C:B3:6A:5E:E2:56:2B:0A:03:D5:73:E8:86:66:4B:
                                AA:9E:3D:BA:86:A8:6B:D1
    Signature Algorithm: sha256WithRSAEncryption
         04:e1:6e:02:3e:0d:e3:23:46:f4:e3:96:35:05:93:35:22:02:
         0b:84:5d:e2:73:86:d4:74:4f:fc:1b:27:af:3e:ca:ad:c3:ce:
         46:d6:fa:0f:e2:71:f9:0d:1a:9a:13:b7:d5:08:48:bd:50:58:
         b3:5e:20:63:86:29:ca:3e:cc:cc:78:26:e1:59:8f:5d:ca:8b:
         bc:49:31:6f:61:bd:42:ff:61:62:e1:22:35:24:26:9b:57:eb:
         e5:00:0d:ff:40:33:6c:46:c2:33:77:08:98:b2:7a:f6:43:f9:
         6d:48:df:bf:fe:fa:28:1e:7b:8a:cf:2d:61:ff:6c:87:98:a4:
         2c:62:9a:bb:10:8c:ff:34:48:70:66:b7:6d:72:c3:69:f9:39:
         4b:68:39:56:bd:a1:b3:6d:f4:77:f3:46:5b:5c:19:ac:4f:b3:
         74:6b:8c:c5:f1:89:cc:93:fe:0c:01:6f:88:17:dc:42:71:60:
         e3:ed:73:30:42:9c:a9:2f:3b:a2:78:8e:c8:6f:ba:d1:13:0c:
         d0:c7:5e:8c:10:fb:01:2e:37:9b:db:ac:f7:a1:ac:ba:7f:f8:
         92:e7:cb:41:44:c8:15:f9:f3:c4:bb:ad:51:5f:be:de:c7:ac:
         86:07:9f:40:ec:b9:0b:f6:b2:8b:cc:b5:55:33:66:ba:33:c2:
         c4:f0:a2:e9
[04/18/24]seed@VM:~/Desktop$ cat signature | tr -d '[:space:]:'
04e16e023e0de32346f4e3963505933522020b845de27386d4744ffc1b27af3ecaadc3ce46d6fa0fe271f90d1a9a13b7d50848bd5058b35e20638629ca3ecccc7826e1598f5dca8bbc49316f61bd42ff6162e1
223524269b57ebe5000dff40336c46c233770898b27af643f96d48dfbffefa281e7b8acf2d61ff6c8798a42c629abb108cff34487066b76d72c369f9394b683956bda1b36df477f3465b5c19ac4fb3746b8cc5
f189cc93fe0c016f8817dc427160e3ed7330429ca92f3ba2788ec86fbad1130cd0c75e8c10fb012e379bdbacf7a1acba7ff892e7cb4144c815f9f3c4bbad515fbedec7ac86079f40ecb90bf6b28bccb5553366
ba33c2c4f0a2e9[04/18/24]seed@VM:~/Desktop$ openssl asn1parse -i -in c0.pem -strparse 4 -out c0_body.bin -noout
[04/18/24]seed@VM:~/Desktop$ sha256sum c0_body.bin
b2825cb7d71ec7093e7ff7026c562a29122de3b4900ed13dad63d1be73706e0d  c0_body.bin
[04/18/24]seed@VM:~/Desktop$ gcc Task6.c -lcrypto -o Task6
[04/18/24]seed@VM:~/Desktop$ ./Task6
Verify signature: 01FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF003031300D060960864801650304020105000420B2825CB7D71EC7093E7FF7026C562A2912
2DE3B4900ED13DAD63D1BE73706E0D
[04/18/24]seed@VM:~/Desktop$
```