CSCI361 CRYPTOGRAPHY & SECURE APPLICATIONS
ASSIGNMENT 2

NAME: SALLY
UOW ID: 4603229

I HAVE READ THE POLICY FOR PLAGARISM AT UNIVERSITY OF WOLLONGONG.
I DECLARE THAT THIS ASSIGNMENT SOLUTION IS ENTIRELY MY OWN WORK.

Task 1
How to compile:

How to compile the program:

---

1. Open your command prompt
2. Navigate to folder where files are stored
3. javac RSA.java
4. java RSA
5. Choose the option accordingly on the console

Given p = 59, q = 47, e =15
n = 59 x 47 = 2773
Φ (n) = 58 x 46 = 2668

Public key e = (2773,15)
To compute d = e^{-1} mod Φ(n), 1 < d < Φ (n) such that ed ≡ 1 mod Φ(n)

n1	n2	r	q	a1	b1	a2	b2
2668	15	13	177	1	0	0	1
15	13	2	1	0	1	1	-177
13	2	1	6	1	-177	-1	178
2	1	0	2	-1	178	7	-1245

Since gcd (2668, 15) = 1
d = e^{-1} mod Φ(n) = -1245 mod 2668 = 1423
Private key d = (2773, 1423)

NAME: SALLY
UOW ID: 4603229

To encrypt by hand

$S = M^d \bmod n = 13^{1423} \bmod 2773$

Using Fast Exponentiation

Express 1423 as 0101 1000 1111

	2^{10} = 1024	2^9 = 512	2^8 = 256	2^7 = 128	2^6 = 64	2^5 = 32	2^4 = 16	2^3 = 8	2^2 = 4	2^1 = 2	2^0 = 1
0	1	0	1	1	0	0	0	1	1	1	1

$13^1 \bmod 2773 = 13$
$13^2 \bmod 2773 = 13^2 = 169$
$13^4 \bmod 2773 = 169^2 \bmod 2773 = 831$
$13^8 \bmod 2773 = 831^2 \bmod 2773 = 84$
$13^{16} \bmod 2773 = 84^2 \bmod 2773 = 1510$
$13^{32} \bmod 2773 = 1510^2 \bmod 2773 = 694$
$13^{64} \bmod 2773 = 694^2 \bmod 2773 = 1907$
$13^{128} \bmod 2773 = 1907^2 \bmod 2773 = 1246$
$13^{256} \bmod 2773 = 1246^2 \bmod 2773 = 2409$
$13^{512} \bmod 2773 = 2409^2 \bmod 2773 = 2165$
$13^{1024} \bmod 2773 = 2165^2 \bmod 2773 = 855$
$13^{1423} \bmod 2773 = 855 \times 2409 \times 1246 \times 84 \times 831 \times 169 \times 13 \bmod 2773 = 2722$

```
Please enter your choice: 1
====================================
+++++++++RSA KEY GENERATOR+++++++++
====================================
Please enter prime bit length: 6
Public key saved to pk.txt
Secret key saved to sk.txt


RSA Key Generation Info Tracing
------------------------------------------------
p               : 59
q               : 47
Modulus N       : 2773
Public Key e    : 15
Private Key d   : 1423
```

```
Please enter your choice: 2
=================================
+++++++RSA SIGNING ALGORITHM+++++++
=================================
Please enter filename to read secret keys <press ENTER for default sk.txt>:
Reading secret key from sk.txt
Please enter filename to read message <press ENTER for default msg.txt>:
Reading message from msg.txt
Please enter filename to store signature <press ENTER for default sig.txt>:
Signature saved to sig.txt

+++Message have been signed+++

RSA Signing Info Tracing
------------------------------------------------
sk                  : {p=59, q=47, d=1423, N=2773}
Original message m  : 13
Signature s         : 2722
Signing Key d       : 1423
Modulus N           : 2773
```

NAME: SALLY
UOW ID: 4603229

To decrypt by hand

$M = S^e \bmod n = 2722^{15} \bmod 2773$
Using Fast Exponentiation
Express 15 as 1111

$2722^1 \bmod 2773 = 2722$
$2722^2 \bmod 2773 = 2722^2 \bmod 2773 = 2601$
$2722^4 \bmod 2773 = 2601^2 \bmod 2773 = 1854$
$2722^8 \bmod 2773 = 1854^2 \bmod 2773 = 1569$

$2722^{15} \bmod 2773 = 1569 \times 1854 \times 2601 \times 2722 \bmod 2773 = 13$

```
Please enter your choice: 3
====================================
+++++++RSA VERIFYING ALGORITHM+++++++
====================================
Please enter filename to read public keys <press ENTER for default pk.txt>:
Reading public key from pk.txt
Please enter filename to read signature <press ENTER for default sig.txt>:
Reading signature from sig.txt
Please enter filename to read message <press ENTER for default msg.txt>:
Reading message from msg.txt

================================================
The verification of the signature returns: True
================================================

RSA Verification Info Tracing
------------------------------------------------
pk                  : {e=15, N=2773}
Original message m  : 13
Verified message m  : 13
Signature s         : 2722
Verification Key e  : 15
Modulus N           : 2773
```

RSA Key Generator Output Screenshot

```
RSA Algorithm
------------------------------------------------
1) Key Generator
2) Sign
3) Verify
4) Encrypt
5) Decrypt
6) Exit
Please enter your choice: 1
==================================
+++++++++RSA KEY GENERATOR+++++++++
==================================
Please enter prime bit length: 32
Public key saved to pk.txt
Secret key saved to sk.txt


RSA Key Generation Info Tracing
------------------------------------------------
p              : 3327606703
q              : 2498724119
Modulus N      : 8314771127332169657
Public Key e   : 2258187941
Private Key d  : 7427620284906925625
```

RSA Signing Output Screenshot

```
==================================
+++++++RSA SIGNING ALGORITHM+++++++
==================================
Please enter filename to read secret keys <press ENTER for default sk.txt>:
Reading secret key from sk.txt
Please enter filename to read message <press ENTER for default msg.txt>:
Reading message from msg.txt
Please enter filename to store signature <press ENTER for default sig.txt>:
Signature saved to sig.txt

+++Message have been signed+++

RSA Signing Info Tracing
------------------------------------------------
sk                 : {p=3327606703, q=2498724119, d=7427620284906925625, N=8314771127332169657}
Original message m  : 3709878397
Signature s        : 502089590539091913
Signing Key d      : 7427620284906925625
Modulus N          : 8314771127332169657
```

RSA Verifying Output Screenshot

```
======================================
+++++++RSA VERIFYING ALGORITHM+++++++
======================================
Please enter filename to read public keys <press ENTER for default pk.txt>:
Reading public key from pk.txt
Please enter filename to read signature <press ENTER for default sig.txt>:
Reading signature from sig.txt
Please enter filename to read message <press ENTER for default msg.txt>:
Reading message from msg.txt

================================================
The verification of the signature returns: True
================================================

RSA Verification Info Tracing
------------------------------------------------
pk                 : {e=2258187941, N=8314771127332169657}
Original message m  : 3709878397
Verified message m  : 3709878397
Signature s        : 502089590539091913
Verification Key e  : 2258187941
Modulus N          : 8314771127332169657
```