CS789 Cryptography
Zuowen Tang

Autorun Samples

RSA Algorithm

Sample One

```
Starting autorun...
Generating random keys...
Alice's public key is: ( m = 98988676981577 , e = 64452285131999 )
and private key is: ( m = 98988676981577 , d = 83023784237819 )

Bob wants to send message 1443905 to her.
Bob encrypts the message 1443905 using Alice's public key.
The cipher text is 48297620046296

Alice receives the ciphertext from Bob and decrypts it with her private key.
She gets the plaintext 1443905

Eve also knows the ciphertext Bob sends to Alice;
however, she does not have the private key to decrypt the message.
She tries to crack it without the private key.
By calculating the factor of the modulus, Eve finds 8431811 and 11739907
which are the prime factors of the modulus 98988676981577
Eve now can have Alice's private key ( 98988676981577 83023784237819 )
and thus able to decrypt the message.
Eve gets the result: 1443905

Autorun is finished.
```

Sample Two

```
Starting autorun...
Generating random keys...
Alice's public key is: ( m = 82408833307 , e = 54503728831 )
and private key is: ( m = 82408833307 , d = 73621767295 )

Bob wants to send message 14145146 to her.
Bob encrypts the message 14145146 using Alice's public key.
The cipher text is 58435934068

Alice receives the ciphertext from Bob and decrypts it with her private key.
She gets the plaintext 14145146

Eve also knows the ciphertext Bob sends to Alice;
however, she does not have the private key to decrypt the message.
She tries to crack it without the private key.
By calculating the factor of the modulus, Eve finds 7333 and 11238079
which are the prime factors of the modulus 82408833307
Eve now can have Alice's private key ( 82408833307 73621767295 )
and thus able to decrypt the message.
Eve gets the result: 14145146

Autorun is finished.
```

Sample Three

```
Starting autorun...
Generating random keys...
Alice's public key is: ( m = 85996747875671 , e = 74593181200261 )
and private key is: ( m = 85996747875671 , d = 978401005741 )

Bob wants to send message 13540158 to her.
Bob encrypts the message 13540158 using Alice's public key.
The cipher text is 35119501084645

Alice receives the ciphertext from Bob and decrypts it with her private key.
She gets the plaintext 13540158

Eve also knows the ciphertext Bob sends to Alice;
however, she does not have the private key to decrypt the message.
She tries to crack it without the private key.
By calculating the factor of the modulus, Eve finds 11132941 and 7724531
which are the prime factors of the modulus 85996747875671
Eve now can have Alice's private key ( 85996747875671 978401005741 )
and thus able to decrypt the message.
Eve gets the result: 13540158
Autorun is finished.
```

El Gamal Algorithm

Sample One

```
Starting autorun...
Generating random prime number...

Alice and Bob both agreed on prime number 13732717 and the generator 797543
Alice chooses her secret number 7739452 and calculates 1740830
Bob chooses his secret number 3911428 and calculates 4986869

The public knowledge are
Prime number: 13732717
The generator: 797543
Alice's public number: 1740830
Bob's public number: 4986869

The private knowledge are
Alice's secret number: 7739452
Bob's secret number: 3911428
Alice and Bob both share the key: 3233815
And the multi-inverse of the key: 6416323

Now Alice and Bob can share messages between them.


Alice wants to send a message: 7398853 to Bob.
She does the calculation: 7398853 * 3233815 mod 13732717 = 8985095
Bob receives the cipher and does the calculation: 8985095 * 6416323 mod 13732717 =
7398853
They successfully exchange information.

Eve also knows the public information and the ciphertext.
She will try to crack it without knowing the secret numbers.
She is trying...(usually under 10 sec)
By using Baby-Step&Giant-Step, Eve tries to solve the problem.
She now has the secret numbers: 873094 and 3911428
With that, she can get the plaintext: 7398853

Autorun is finished.
```

Sample Two

```
Starting autorun...
Generating random prime number...
Alice and Bob both agreed on prime number 10062281 and the generator 3125573
Alice chooses her secret number 2134355 and calculates 9343362
Bob chooses his secret number 6066580 and calculates 9811572

The public knowledge are
Prime number: 10062281
The generator: 3125573
Alice's public number: 9343362
Bob's public number: 9811572

The private knowledge are
Alice's secret number: 2134355
Bob's secret number: 6066580
Alice and Bob both share the key: 8240758
And the multi-inverse of the key: 7383903

Now Alice and Bob can share messages between them.


Alice wants to send a message: 2419865 to Bob.
She does the calculation: 2419865 * 8240758 mod 10062281 = 2811341
Bob receives the cipher and does the calculation: 2811341 * 7383903 mod 10062281 =
2419865
They successfully exchanged information.

Eve also knows the public information and the ciphertext.
She will try to crack it without knowing the secret numbers.
She is trying...(usually under 10 sec)
By using Baby-Step&Giant-Step, Eve tries to solve the problem.
She now has the secret numbers: 2134355 and 6066580
With that, she can get the plaintext: 2419865

Autorun is finished.
```