

# DEPARTMENT OF COMPUTER ENGINEERING & APPLICATIONS

**Institute of Engineering & Technology**

**Cryptography & Network Security Lab (BCSE-0071)**

Name:

Gautam Rathore

Krishankant Sharma

Section:

J (20)

J (31)

University roll no.: Course: B.Tech CS

201500256

201500349

Submitted to: Dr. Rakesh Kumar Galav

INDEX

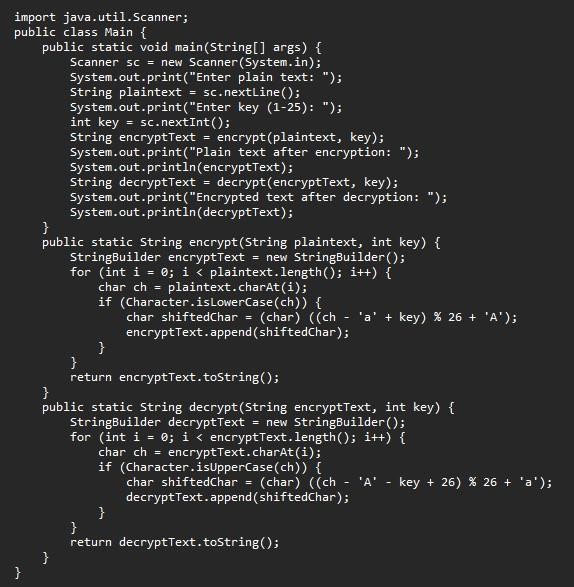
|  |  |
| --- | --- |
| **Serial No.** | **Title** |
| 1. | Write a program to implement Additive Cipher (Z26) with the following  conditions: Plaintext should be in lowercase, Ciphertext should be uppercase, Brute force attack. |
| 2. | Write a program to implement Multiplicative Cipher: Plaintext should be in lowercase, Ciphertext should be uppercase, Brute force attack. |
| 3. | Write a program to implement Affine Cipher: Plaintext should be in lowercase, Ciphertext should be uppercase, Brute force attack. |
| 4. | Write a program in to implement Autokey Cipher: Plaintext should be in lowercase, Ciphertext should be uppercase, Brute force attack. |
| 5. | Write a program to implement Playfair Cipher to encrypt & decrypt the given message where the key matrix can be formed by using a given keyword. |
| 6. | Write a program to implement Hill Cipher to encrypt & decrypt the given message by using a given key matrix. Show the values for key and its  corresponding key inverse values. |
| 7. | Write a program to implement Elgamal Cryptosystem to generate the pair of keys and then show the encryption & decryption of a given message. |
| 8. | Write a program to implement Rabin Miller Primality Test to check whether given number is prime or composite. |
| 9. | Write a program to implement Diffie-Hellman key exchange Algorithm to exchange the symmetric key and show the encryption & decryption. |
| 10. | Write a program to implement RSA Algorithm to generate a pair of keys and show the encryption and decryption by using a given key pair. |
| 11. | Write a program to implement Elgamal algorithm for implementing digital signature. |

# Experiment 1

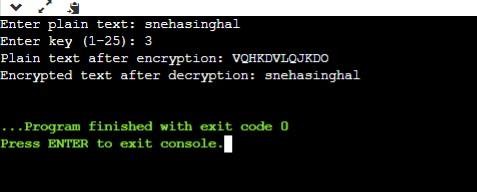
Write a program to implement Additive Cipher (Z26) with the following conditions:

* Plaintext should be in lowercase.
* Ciphertext should be uppercase.
* Brute force attack.

# Source Code:



**Input & Output:**

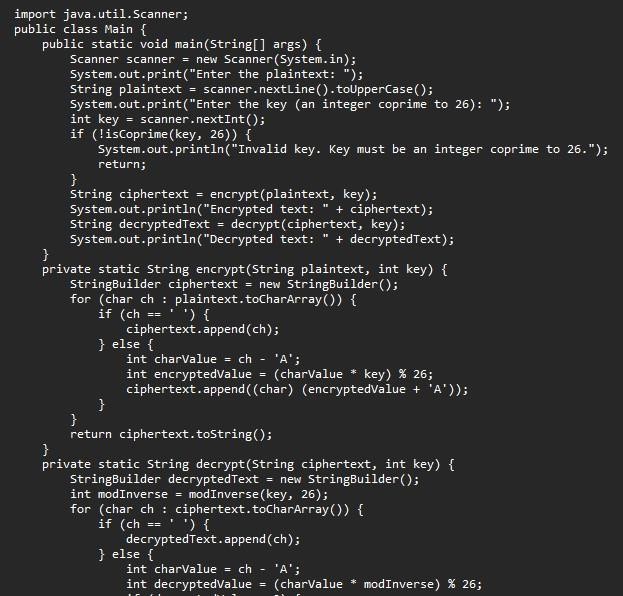


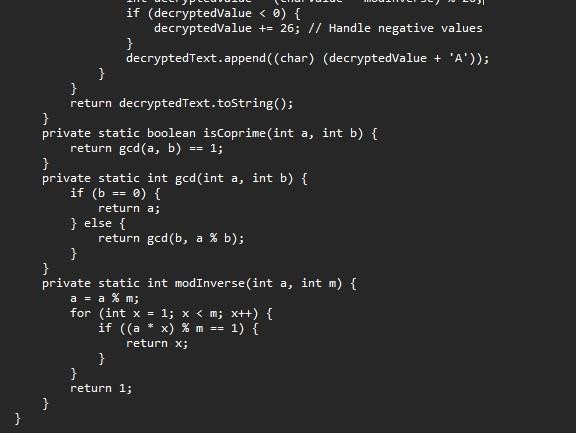
**Experiment 2**

Write a program to implement Multiplicative Cipher.

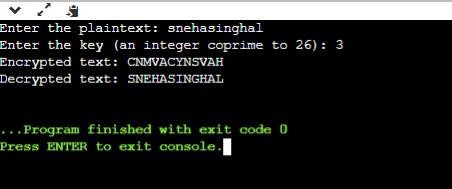
* Plaintext should be in lowercase.
* Ciphertext should be uppercase.
* Brute force attack.

**Source Code:**





**Input & Output:**

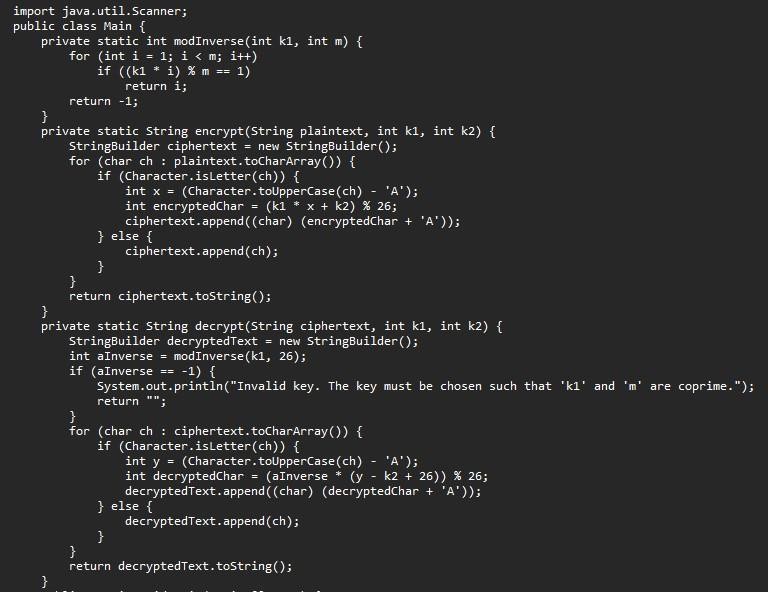


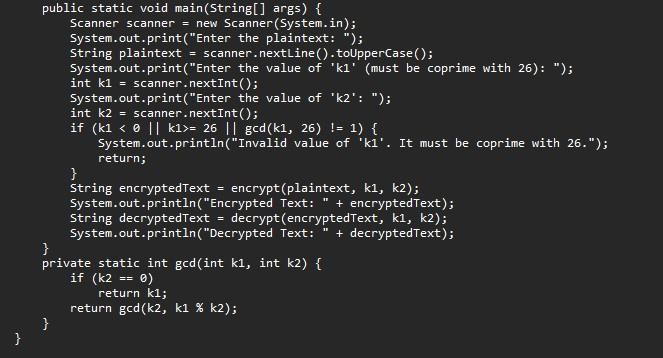
**Experiment 3**

Write a program to implement Affine Cipher.

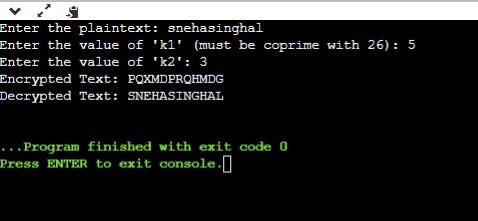
* Plaintext should be in lowercase.
* Ciphertext should be uppercase.
* Brute force attack.

# Source Code:





**Input & Output:**

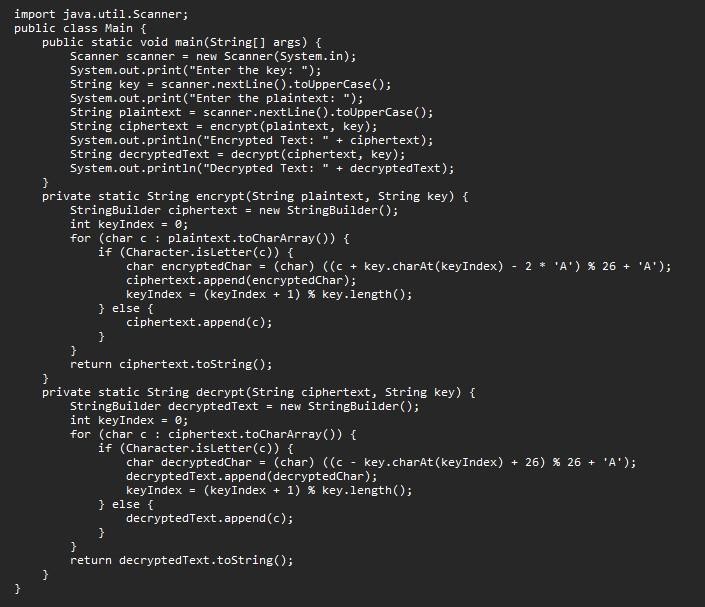


**Experiment 4**

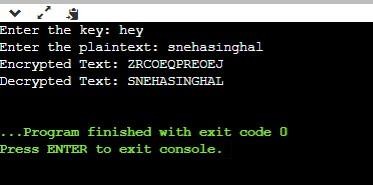
Write a program in to implement Autokey Cipher.

* Plaintext should be in lowercase.
* Ciphertext should be uppercase.
* Brute force attack.

# Source Code:



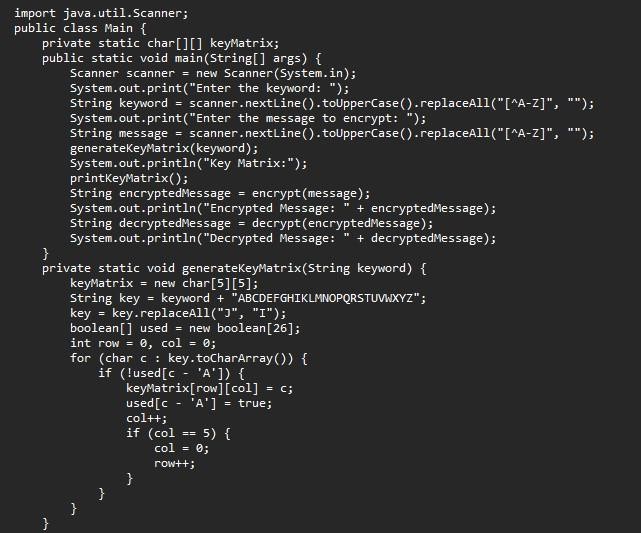
**Input & Output:**

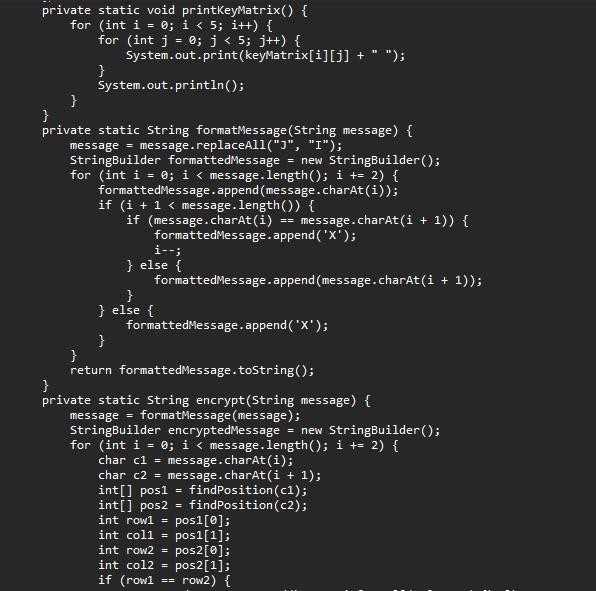


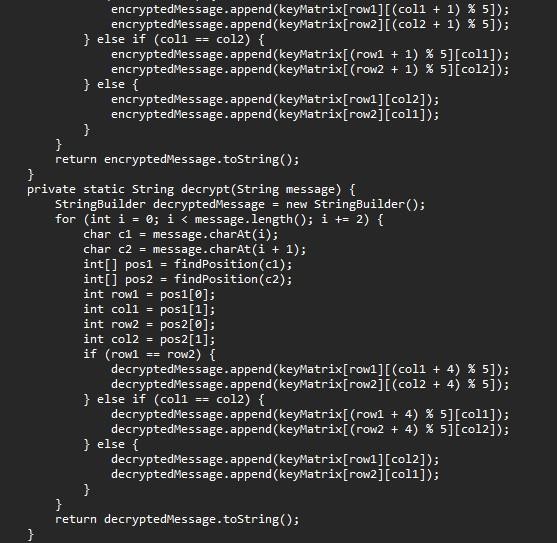
**Experiment 5**

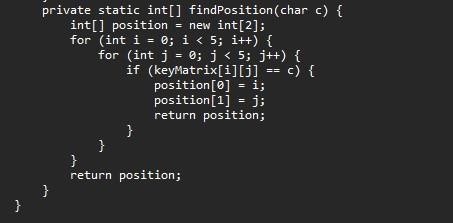
Write a program to implement Playfair Cipher to encrypt & decrypt the given message where the key matrix can be formed by using a given keyword.

# Source Code:









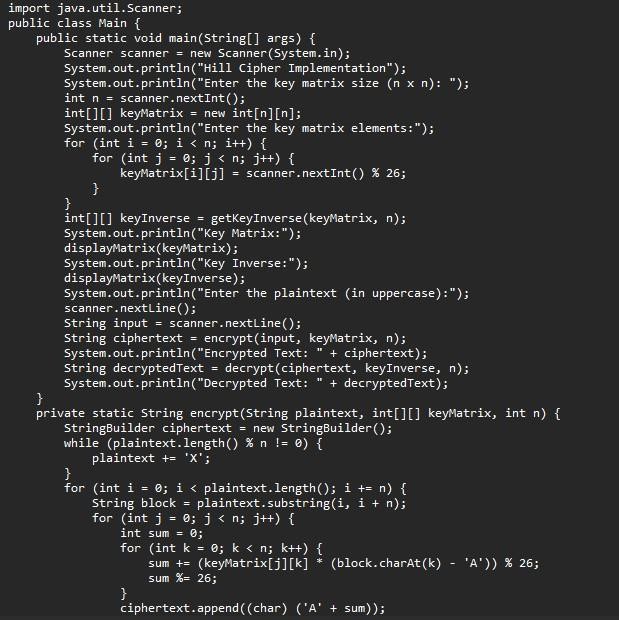
**Input & Output:**

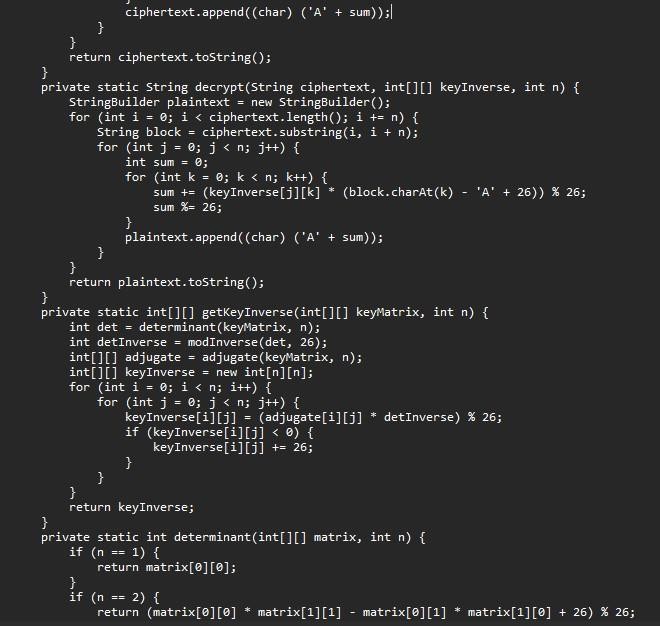


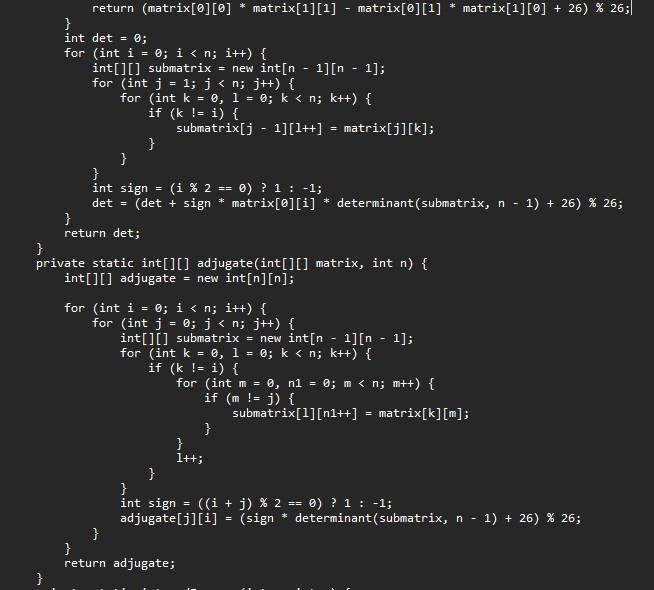
**Experiment 6**

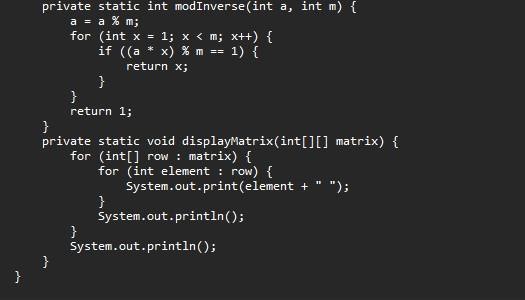
Write a program to implement Hill Cipher to encrypt & decrypt the given message by using a given key matrix. Show the values for key and its corresponding key inverse values.

**Source Code:**

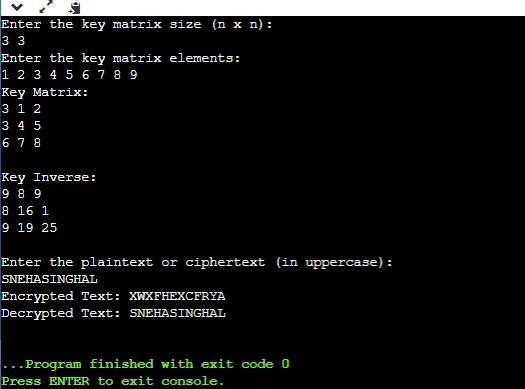






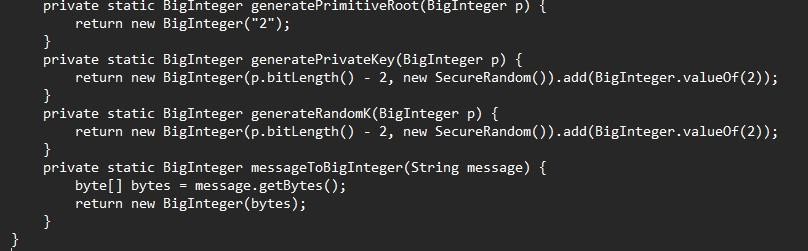
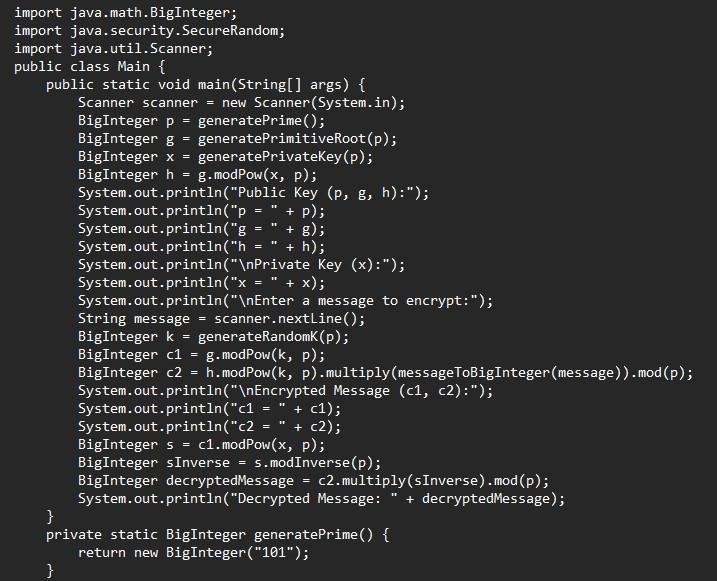


**Input & Output:**

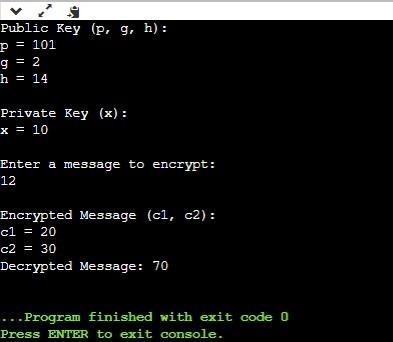


**Experiment 7**

Write a program to implement Elgamal Cryptosystem to generate the pair of keys and then show the encryption & decryption of a given message.

**Source Code:**

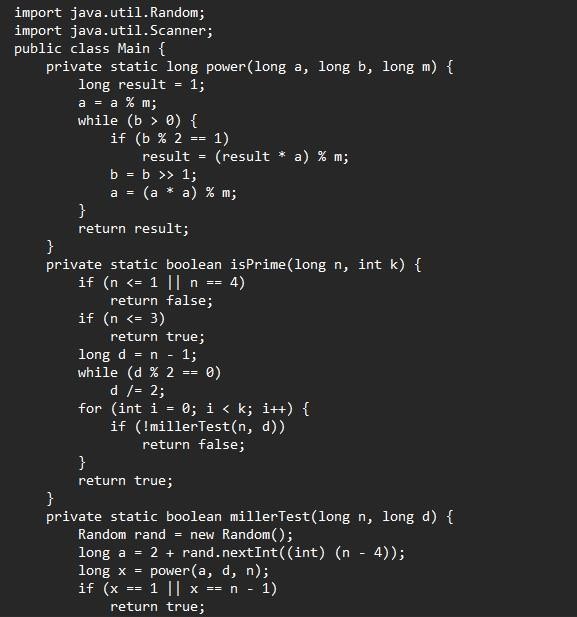
**Input & Ouput:**

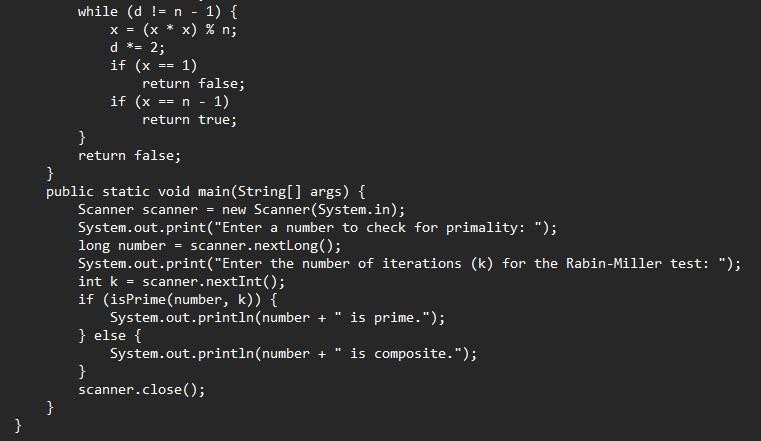


**Experiment 8**

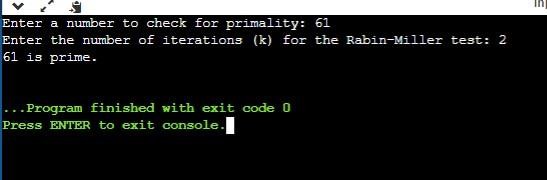
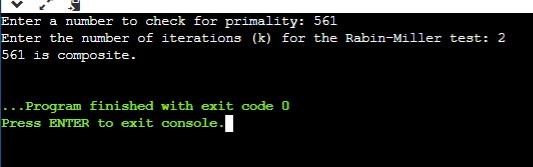
Write a program to implement Rabin Miller Primality Test to check whether given number is prime or composite.

**Source Code:**





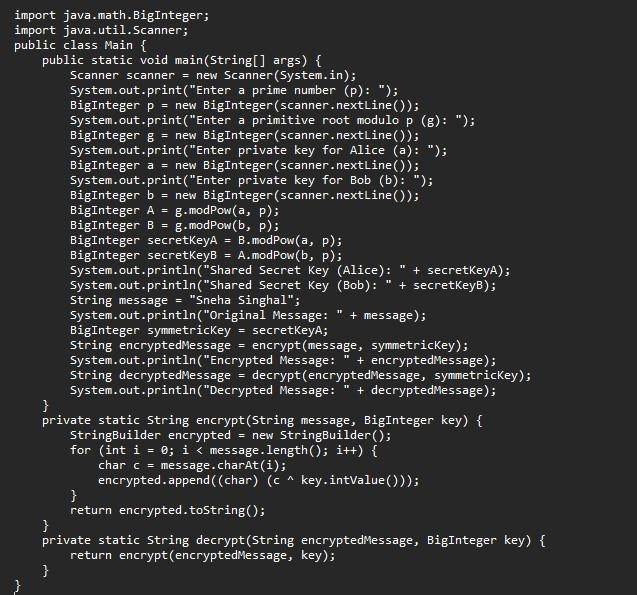
**Input & Output:**



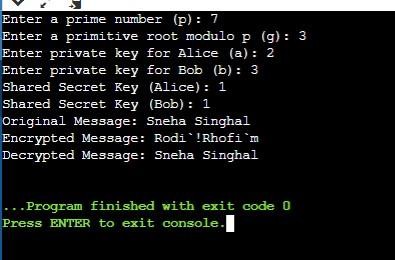
**Experiment 9**

Write a program to implement Diffie-Hellman key exchange Algorithm to exchange the symmetric key and show the encryption & decryption.

# Source Code:



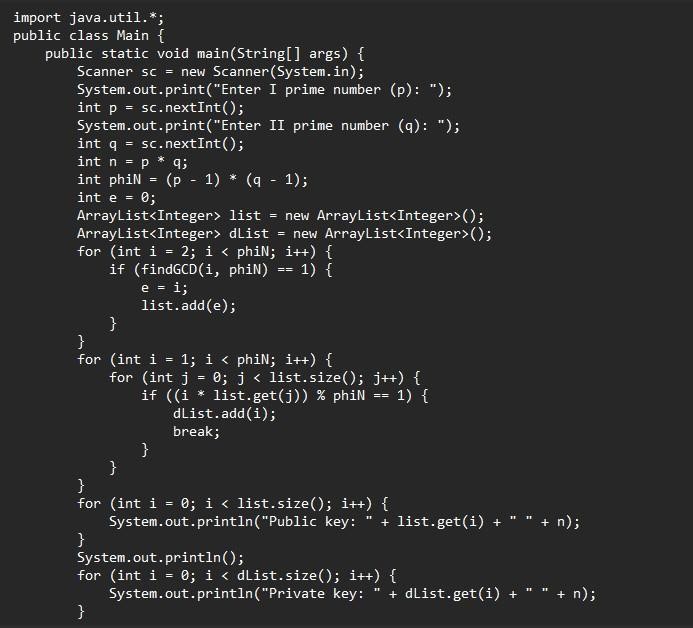
**Input & Output:**

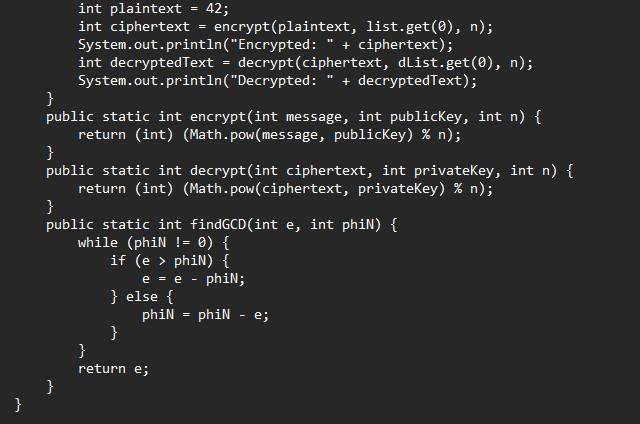


**Experiment 10**

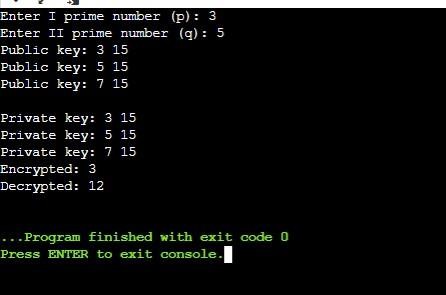
Write a program to implement RSA Algorithm to generate a pair of keys and show the encryption and decryption by using a given key pair.

# Source Code:



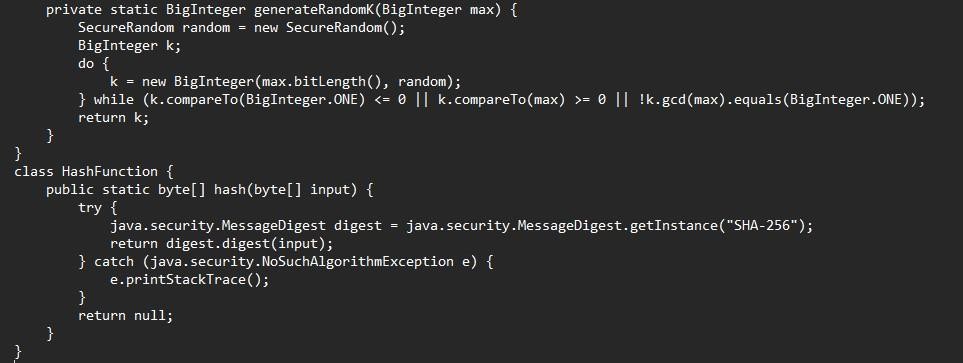
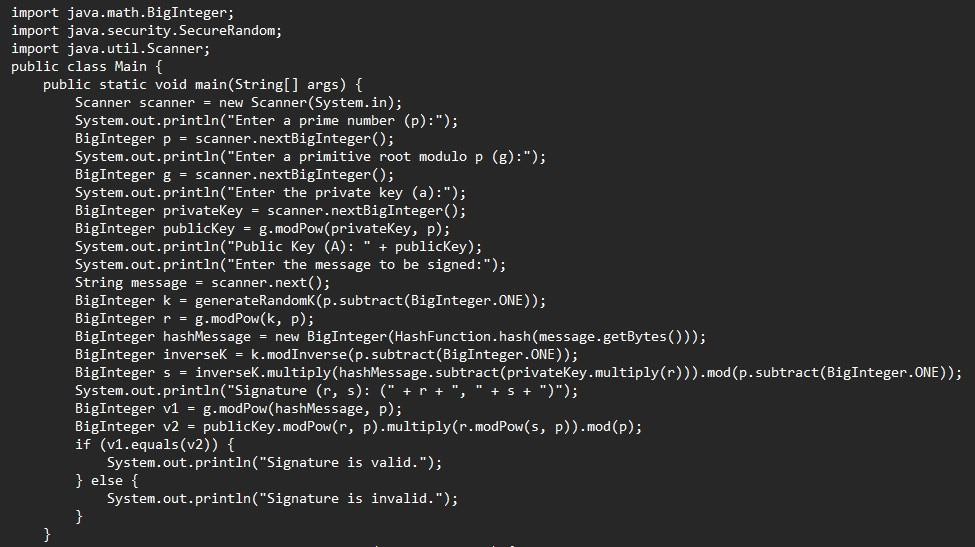


**Input & Output:**



**Experiment 11**

Write a program to implement Elgamal algorithm for implementing digital signature.

**Source Code:**

**Input & Output:**

