Caesar Cipher

```
-------Caesar Cipher-------
Enter your plain-text: Symmetric Cipher
Enter encryption key: 5
Pain text: Symmetric Cipher
Encrypted msg: XDRRJYWNH HNUMJW
Decrypted msg: SYMMETRIC CIPHER
```

Playfair Cipher

```
-------Play-fair Cipher-------
Plain text:  the imitation game
Plain Diagram:  ['pd', 'fk', 'ae', 'sr', 'sk', 'na', 'in', 'c
Encrypted msg:  pdfkaesrsknaincl
Enc Diagram:  ['pd', 'fk', 'ae', 'sr', 'sk', 'na', 'in', 'cl'
Decrypted msg:  theimitationgame
```

Rail Fence Cipher

```
--------Rail Fence-------
Enter plain text: Democracy a joke
Enter rail depth: 4
Message: Democracyajoke
Cipher: Dakercoemcyjoa
Plain: Democracyajoke
```

Modular Arithmetic Operation

```
***** Modular Arithmetic Operation *****
Enter modulo(+ve): 47
Enter (+ve, -ve) dividend: -1397
------a mod m ------
-1397 mod 47 = 13
```

Vegenere and Vernam

```
*******Vegenere Cipher*******
-----Encryption-----
Message:  we are discovered save yourself
keyword:  deceptive
Message:  wearediscoveredsaveyourself
keyword:  deceptivedeceptivedeceptive
Cipher text: ZICVTWQNGRZGVTWAVZHCQYGLMGJ
-----Decryption-----
Decrypted msg:  WEAREDISCOVEREDSAVEYOURSELF

*******Vernam Cipher*******
-----Encryption-----
Msg: Randomkeygeneration
Random key: BSDIYIICVGKINGJXCRD
Cipher: SSQLMUSGTMOVRXJQKFQ
-----Decryption-----
Plain:  RANDOMKEYGENERATION
```

Hill cipher

```
-------Hill Cipher-------
keyword: GYBNQKURP
key matrix: [[6, 24, 1], [13, 16, 10], [20, 17, 15]]
plain text: ACT
plain matrix: [0, 2, 19]
Cipher matrix: [15, 14, 7]
Cipher text:['P', 'O', 'H']
Message matrix [ 0.  2. 19.]
Original msg:  ['A', 'C', 'T']
```

```
-----Lucas Lehmar Test (Mersenne Prime Number)----
Enter any positive integer: 2
Not a Mersenne prime number.
Enter any positive integer: 3
Given number is Mersenne Prime.
Enter any positive integer: 31
Given number is Mersenne prime number.
Enter any positive integer:
```

```
----------RSA Algorithm----------
private key:
p=11    q=61
Encryption: public key: e=7, n=671
    Msg: 592
    Cipher: -1096
Decryption: d=343
    Msg: 592
    Cipher: -1096
```

```
-----GCD using euclidean algorithm-----
Enter first number: 768
Enter second number: 1248
GCD(768,1248) = 96
```

```
-----Deffie Hellman Algorithm-----
q: 41    primitive root(alpha): 3
For User A: X_a= 34, Y_a= 9 K_a= 9
For User B: X_b= 29, Y_b= 38 K_b= 9
```

```
------Coprime check-------
Enter first number: 34
Enter second number: 13
34 and 13 are coprime numbers.
```

```
-----Multiplicative inverse using Extended Euclidean Algorithm-----
Enter dividend: 23
Enter Modulo: 35
Multiplicative inverse of 23 mod 35 is 32

Process finished with exit code 0
```

```
Enter a number: 457
Euler's totient:  456
Enter a number: 223
Euler's totient:  222
Enter a number: 645
Euler's totient:  336
Enter a number: 090
Euler's totient:  24
```

elGamal Algorithm

```
------Elgamal CryptoSystem------
Encryption:
    Msg: 55
    K:26
    (C1,C2): (6, 8)
Decryption: K=26
    Msg: 55
    C2: 8
```

```
------Primitive root check------
Remainders:  [32, 19, 5, 26, 28, 25, 63, 6, 58, 47, 30, 22, 34, 16, 43, 36, 13, 14,
Yes 32 is primitive root of 67 (modulo)
```