COMPUTER CRYPTOGRAPHY AND NETWORK SECURITY (SAMPLE IMPLEMENTATIONS and/or INPUTS)

1] CAESAR CIPHER

```
Enter the String: Cryptography subject is not an elective

After Encryption - Cipher Text: Fubswrjudskb vxemhfw lv qrw dq hohfwlyh
After Decryption - Plain Text: Cryptography subject is not an elective
```

2] RAIL FENCE CIPHER

```
Depth(k): 2
Plain Text: MEETMEAFTERCLASS

Encrypted Cipher Text: MEMATRLSETEFECAS
Decrypted Cipher Text: MEETMEAFTERCLASS
```

3] COLUMNAR TRANSPOSITION

```
Key: WORD
Filler: X
Input: COMPUTERPROGRAMMING


ENCRYPTION:
 Plain Text: COMPUTERPROGRAMMING

 Matrix:
        COMP
        UTER
        PROG
        RAMM
        INGX

 Cipher Text: PRGMXOTRANMEOMGCUPRI


DECRYPTION:
 Cipher Text: PRGMXOTRANMEOMGCUPRI

 Matrix:
        COMP
        UTER
        PROG
        RAMM
        INGX

 Plain Text: COMPUTERPROGRAMMING
```

4] PLAYFAIR CIPHER

Key: HELLO
Filler: X
Plain Text: TOMORROW

Matrix:
H E L O A
B C D F G
I K M N P
Q R S T U
V W X Y Z

ENCRYPTION PROCESS:
Plain Text:TOMORROW
Plain Text With Filler:TOMORXROWX
Resulting Cipher Text: YFNLSWTEXY

DECRYPTION PROCESS:
Cipher Text:YFNLSWTEXY
Plain Text With Filler:TOMORXROWX
Resulting Plain Text: TOMORROW

5] HILL CIPHER:

Key Size: 3 3

Key:

5	7	6
12	13	20
8	3	7

Filler: X

Input: SECRET

ENCRYPTION:

Adding Filler (if required): PT = SECRET

CT = (K * PT) (mod 26)

=

130	227
308	636
170	281

(mod 26)

=

0	19
22	12
14	21

Cipher Text: AWOTMV

DECRYPTION:

Det(k) = 279

Multiplicative Inverse of 279 in Z_279

q	r1	r2	r	s1	s2	s	t1	t2	t
0	26	279	26	1	0	1	0	1	0
10	279	26	19	0	1	-10	1	0	1
1	26	19	7	1	-10	11	0	1	-1
2	19	7	5	-10	11	-32	1	-1	3
1	7	5	2	11	-32	43	-1	3	-4
2	5	2	1	-32	43	-118	3	-4	11
2	2	1	0	43	-118	279	-4	11	-26
	1	0		-118	279		11	-26	

gcd(26,279) = 1

Multiplicative Inverse of 279 in Z_26: 11

Adj(k) =

31	-31	62

```
          76        -13       -28
          -68       41        -19
         =
          31        21        62
          76        13        24
          10        41        7

K^-1 = (1 / 279) * Adj(k)
         = (11) * Adj(k)
         =
          341       231       682
          836       143       264
          110       451       77
          (mod 26)
         =
          3         23        6
          4         13        4
          6         9         25

PT       = (K^-1 * CT) (mod 26)
         =
          590       459
          342       316
          548       747
          (mod 26)
         =
          18        17
          4         4
          2         19

PT with Filler (if any): PT = SECRET

Plain Text: SECRET
```

6] ONE TIME PAD:

```
Enter the String: UDITYALAAD
Random Key: ROSUFTNBAX

After Encryption - Cipher Text: LRANDTYBAA
After Decryption - Plain Text: UDITYALAAD
```

7] EXTENDED EUCLIDIAN ALGORITHM:

n: 26
a: 11

q	r1	r2	r	s1	s2	s	t1	t2	t
2	26	11	4	1	0	1	0	1	-2
2	11	4	3	0	1	-2	1	-2	5
1	4	3	1	1	-2	3	-2	5	-7
3	3	1	0	-2	3	-11	5	-7	26
	1	0		3	-11		-7	26	

gcd(26,11) = 1

Multiplicative Inverse of 11: 19

8] DES:

PT: 1 1 1 1 0 0 1 1
Key: 1 0 1 0 0 0 0 0 1 0

Genrated Keys:
K1: 10100100
K2: 01000011

Encryption:
IP(PT) = 10111101
EP_IP_2 = 11101011

EP_Part_2 XOR K1 = 01001111
Temp = 1111
P4(Temp) = 1111
SW = 0100

EP(SW) = 00101000
EP_Part_2 XOR K2 = 01101011
Temp = 1001
P4(Temp) = 0101
SW = 1000

Temp = 10000100
IP_Inverse(Temp) = 01000001

CT = 01000001

Decryption:
IP(PT) = 10000100
EP_IP_2 = 00101000
EP_Part_2 XOR K2 = 01101011
Temp = 1001
P4(Temp) = 0101
SW = 1101

EP(SW) = 11101011
EP_Part_2 XOR K1 = 01001111
Temp = 1111
P4(Temp) = 1111
SW = 1011

Temp = 10111101
IP_Inverse(Temp) = 11110011

PT = 11110011

9] RSA:

M: 12345

Key Generation

Step 1:

p = 35797
q = 95311

Step 2:

n = 3411847867
phi(p) = 35796
phi(q) = 95310
phi(n) = 3411716760

Step 3:

gcd(e, 35796) = 1
gcd(e, 95310) = 1
gcd(e, 3411716760) = 1

e = 153191

Step 4:

e.d = 1 mod phi(n)
153191.d = 1 mod 3411716760
=> d = 22271

Encryption:

C = 12345^153191 mod 3411847867 = 125549024
Cipher Text: 125549024

Decryption:

M = 125549024^22271 mod 3411847867 = 12345
Plain Text: 12345

10] DIFFIE-HELLMAN KEY EXCHANGE

q: 353

Private Key of:
  User A (XA): 97

  User B (XB): 233

alpha = 3

Public Key of:
  User A:
    YA = (Alpha ^ XA) mod q
      = (3 ^ 97) mod 353
      = 40

  User A:
    YB = (Alpha ^ XB) mod q
      = (3 ^ 233) mod 353
      = 248

Secret Key for:
  User A:
    K = (YB ^ XA) mod q
      = (248 ^ 97) mod 353
      = 160

  User B:
    K = (YA ^ XB) mod q
      = (40 ^ 233) mod 353
      = 160