Name: Muhammad Rafiq

Seat No: B17101061

Course: Network Security & Cryptography (NS'21 Lab)

Assignment : Assignment # 4

Section: A

Modulus Algorithm

In [43]:
```
def modulo(a, m)->int:
    R = abs(a) % m
    if a>= 0:
        R =R
    elif a < 0 and R != 0:
        R = m - R
    elif a < 0 and R == 0:
        R = 0
    return R
```

AUTOKEY CIPHER

1- Decrypt the text "dlcjm hw tusklmj tuwgn me vygczwttrnwr hnrt xuaklalmf vyi cgqhelbkhk dq xem lwgyxt. Key="Key size" using Autokey Cipher

In [44]:

```
def auto_key_decrypt(message, key):
    message = message.replace(" ", "").upper()
    key = key.replace(" ", "").upper()
    i =0
    dec_string = ""
    for character in message:
        '''print(ord(character)-65 , "\t" ,key[i] ,"\t",ord(key[i])-65,"\t",
              modulo((ord(character) - 65 - (ord(key[i])-65)), 26), "\t",
              chr(modulo((ord(character) - 65 - (ord(key[i])-65)), 26)+65))'
        dec_character = modulo((ord(character) - 65 - (ord(key[i])-65)), 26)
        i += 1
        dec_string += chr(dec_character + 65)
        key += chr(dec_character + 65)
    return dec_string



def main():
    message = "dlcjm hw tusklmj tuwgn me vygczwttrnwr hnrt xuaklalmf vyi cgq
    key_new = "Key size"
    cipher_text = auto_key_decrypt(message, key_new)
    print(cipher_text)


if __name__ == '__main__':
    print("Text after decrypting thorugh Autokey cipher would be:\n ")
    main()
```

```
Text after decrypting thorugh Autokey cipher would be:

THEREISANOTHERTHINGINCRYPTOGRAPHYTHATINCREASESTHECOMPLEXITYOFTHESYSTEM
```

PORTA CIPHER

2- Decrypt the text "goiindugafybxjqofbnuynxjwhrcbinzolnsnjpjvgysety", Key="Bonus Marks", using porta cipher.

In [47]:

```
alphabet = {
    "A": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "NOPQRSTUVWXYZABCDEFGHIJKLM"),
    "B": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "NOPQRSTUVWXYZABCDEFGHIJKLM"),
    "C": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "OPQRSTUVWXYZNMABCDEFGHIJKL"),
    "D": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "OPQRSTUVWXYZNMABCDEFGHIJKL"),
    "E": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "PQRSTUVWXYZNMLMABCDEFGHIJK"),
    "F": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "PQRSTUVWXYZNMLMABCDEFGHIJK"),
    "G": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "QRSTUVWXYZNOPKLMABCDEFGHIJ"),
    "H": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "QRSTUVWXYZNOPKLMABCDEFGHIJ"),
    "I": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "RSTUVWXYZNOPQJKLMABCDEFGHI"),
    "J": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "RSTUVWXYZNOPQJKLMABCDEFGHI"),
    "K": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "STUVWXYZNOPQRIJKLMABCDEFGH"),
    "L": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "STUVWXYZNOPQRIJKLMABCDEFGH"),
    "M": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "TUVWXYZNOPQRSHIJKLMABCDEFG"),
    "N": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "TUVWXYZNOPQRSHIJKLMABCDEFG"),
    "O": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "UVWXYZNOPQRSTGHIJKLMABCDEF"),
    "P": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "UVWXYZNOPQRSTGHIJKLMABCDEF"),
    "Q": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "VWXYZNOPQRSTUFGHIJKLMABCDE"),
    "R": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "VWXYZNOPQRSTUFGHIJKLMABCDE"),
    "S": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "WXYZNOPQRSTUVEFGHIJKLMABCD"),
    "T": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "WXYZNOPQRSTUVEFGHIJKLMABCD"),
    "U": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "XYZNOPQRSTUVWDEFGHIJKLMABC"),
    "V": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "XYZNOPQRSTUVWDEFGHIJKLMABC"),
    "W": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "YZNOPQRSTUVWXCDEFGHIJKLMAB"),
    "X": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "YZNOPQRSTUVWXCDEFGHIJKLMAB"),
    "Y": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "ZNOPQRSTUVWXYBCDEFGHIJKLMA"),
    "Z": ("ABCDEFGHIJKLMNOPQRSTUVWXYZ", "ZNOPQRSTUVWXYBCDEFGHIJKLMA"),
}

def convert(cipher_text, key):
    '''
    It can encrypt and decrypt in both ways
    '''
    cipher_text = cipher_text.replace(" ", "").upper()
    key = key.replace(" ","").upper()
    string = ""
    i = 0
    for i in range(len(cipher_text)):
        string += alphabet[key[i % len(key)]][1][ord(cipher_text[i])-65]
    return string

print("Plain Text Would be: \n")
print(convert("goiindugafybxjqofbnuynxjwhrcbinzolnsnjpjvgysety","Bonus Marks
```

```
Plain Text Would be:

THOSEWHOSOLVETHISWILLGETANEXTRAFIVEMARKSINFINAL
```

M. Rafa B171C1061

Autokey Cipher

$Pi = (Ci - Ki) \bmod m.$

C	C value	K	K value	C-K	Pi	Answer
d	3	K	10	-7	19	T
l	11	E	4	7	7	H
c	2	Y	24	-22	4	E
j	9	S	18	-9	17	R
m	12	I	8	4	4	E
H	7	Z	25	-18	8	I
w	22	E	4	18	18	S
T	19	T	19	0	0	A
u	20	H	7	13	13	N
s	18	E	4	14	14	O
K	10	R	17	-7	19	T
L	11	E	4	7	7	H
m	12	I	8	4	4	E
j	9	S	18	-9	17	R
T	19	A	0	19	19	T
y	20	N	13	7	7	H
w	22	O	14	8	8	I
G	6	T	19	-13	13	N
N	13	H	7	6	6	G
M	12	E	4	8	8	I
R	4	R	17	-13	13	N
V	21	T	19	2	2	C

Muhammad Rafiq
B171010G1

C	C value	K	K value	C-K	Pi	Answer
Y	24	H	7	17	17	R
G	6	I	8	-2	24	Y
C	2	N	13	-11	15	P
Z	25	G	6	19	19	T
W	22	I	8	14	14	O
T	-19	N	13	6	6	G
T	19	C	2	17	17	R
R	17	R	17	0	0	A
N	22	Y	24	-11	15	P
W	22	P	15	7	7	H
R	17	T	19	-2	24	Y
H	7	O	14	-7	19	T
N	13	G	6	7	7	H
R	17	R	17	0	0	A
T	19	A	0	19	19	T
X	23	P	15	8	8	I
U	20	H	7	13	13	N
A	0	Y	24	-24	2	C
K	10	T	19	-9	17	R
L	11	H	7	4	4	E
A	0	A	0	0	0	A
L	11	T	19	-8	18	S
M	12	I	8	4	4	E
F	5	N	13	-8	18	S
V	21	C	2	19	19	T

M. Rafiq
B17101061

C	C value	K	K value	C-K	Pi	ANSWER
Y	24	R	17	7	7	H
T	8	E	4	4	4	E
C	2	A	0	2	2	C
S	6	S	18	-12	14	O
Q	16	E	4	12	12	M
H	7	S	18	-11	15	P
E	4	T	19	-15	11	L
L	11	H	7	4	4	E
B	1	E	4	-3	23	X
K	10	C	2	8	8	I
H	7	O	14	-7	19	T
K	10	M	12	-2	24	Y
D	3	P	15	-12	14	G
Q	16	L	11	5	5	F
X	23	E	4	19	19	T
E	4	X	23	-19	7	H
M	12	I	8	4	4	E
L	11	T	19	-8	18	S
W	22	Y	24	-2	24	Y
S	6	G	14	-8	18	S
Y	24	F	5	19	19	T
X	23	T	19	4	4	E
T	19	H	7	12	12	M

Porta Cipher

Cipher Text:

qoiyndugafybnjqofbny
ynxjuhrcbinzolnsnjpjvgy
sefy

Key:

Bonus marks

Solving Using the table provided
in the class, I got

Plain text:

THOSE WHO SOLVE THIS WILL GET
AN EXTRA FIVE MARS IN FINAL.