Lab Assignment: 5

Write a menu driven program with appropriate functions to implement the affine cipher i.e. E(x) = (a x + b) mod 26. Let the values of a and b be entered by the user. Your program must check for the feasibility of these values before encrypting the plaintext. The program must also output the decrypted values. Let the plaintext be input as a character array of defined size.

Encryption:

An encipherment scheme of the form,

E(x) = (ax + b) MOD m or

E(x) = (ax + b) MOD 26

x is the numerical value of the letter in the plaintext,

m is the number of letters in the plaintext alphabet,

a and b are the secret numbers, (appropriately chosen) integers. It are chosen with some restrictions from 0 to m-1.

a must be one of the: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21 23 and 25. In other word we must have gcd(a,26)=1

E(x) is the result of transformation.

Recall that the numerical equivalents of the letters are as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Example: Encipher **ITS COOL** with

E(x) = (5x + 8) MOD 26.

Example: Encipher ITS COOL with E(x) = (5x + 8) MOD 26.

plain	I	T	S	C	O	O	L
x	8	19	18	2	14	14	11
$5x + 8$	48	103	98	18	78	78	63
$(5x + 8)$ MOD 26	22	25	20	18	0	0	11
cipher	W	Z	U	S	A	A	L

Decryption:

y = E(x) = (ax+b) MOD 26

if $y \equiv (ax + b) \pmod{26}$, then

$y - b \equiv ax \pmod{26}$,

Multiply both sides by $a^{-1} \pmod{26}$, then $x \equiv a^{-1}(y - b) \pmod{26}$

So decipherment function is $E^{-1}(y) = a^{-1}(y - b)$ MOD 26.

$D(y) = a^{-1}(y - b)$ MOD 26.

Cipher text: WZUSAAL

$D(y)= 5^{-1}$ (y-8) mod 26

Modular Multiplicative Inverse:

[(i * N) + 1]/ A where i=1,2,3,.. , N=26 and A=5

=[(4 * 26) +1]/5

=21

W=D(22)= 21 (22-8) mod 26

= (21 * 14) mod 26

= 294 mod 26

= 8

= I