Affine

Affine

The ‘key’ for the Affine cipher consists of 2 numbers, we’ll call them a and b. We assumes the use of a 26 character alphabet (m = 26). a should be chosen to be relatively prime to m (i.e. a should have no factors in common with m).

E (x) = (a x + b) mod m

modulus m: size of the alphabet

a and b: key of the cipher.

a must be chosen such that a and m are coprime.

D (x) = a^-1 (x - b) mod m

a^-1 : modular multiplicative inverse of a modulo m. i.e., it satisfies the equation

1 = a a^-1 mod m .

AFFINE CIPHER

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

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

ciphertext

$$c = E(p) = ap + b \bmod 26$$

plain text

$$p = D(c) = a^{-1}(c-b) \bmod 26$$

Example:

$$keys = (a = 7, b = 2)$$

$$c = E(\text{“G”}) = 7(6) + 2 \bmod 26 = 44 \bmod 26 = 18 = \text{“S”}$$

$$p = D(\text{“S”}) = 7^{-1}(18-2) \bmod 26 = 15(16) \bmod 26 = 6 = \text{“G”}$$

Example

- Encrypt the message CRYPTO using the key pair (5,3)
- E(x) = (5x + 3) mod 26

Plaintext	C	R	Y	P	T	O
x	2	17	24	15	19	14
5x + 3	13	88	123	78	98	73
(5x + 3) mod 26	13	10	19	0	20	21
Ciphertext	N	K	T	A	U	V

- Hence the message *'CRYPTO' is encrypted to 'NKTAUV'*

DECRYPTION

- $E(x) = (ax+b) \bmod 26 = y$
- We need to find $D(y)$ or $E^{-1}(y)$
- $y = (ax + b) \bmod 26$
- $y - b = ax \pmod{26}$
- $ax = y - b \pmod{26}$
- $aa^{-1}x = a^{-1}(y-b) \bmod 26$
- $x = a^{-1}(y-b) \bmod 26$
- $D(y) = a^{-1}(y-b) \bmod 26$

Decryption cont...

- Hence D(y)= 21 (y – 3) mod 26

Ciphertext	N	K	T	A	U	V
y	13	10	19	0	20	21
y – 3	10	7	16	23	17	18
21 (y-3)	210	147	336	483	357	378
21(y-3) mod 26	2	17	24	15	19	14
Plaintext	C	R	Y	P	T	O

Example: Encrypt the plaintext: "affine cipher", using the key: k_1=5, k_2=8, using Affine cipher.

Ans. : $C=E(k_1, k_2, p)=(5\,p+8) \bmod 26$

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext	a	f	f	i	n	e		c	i	p	h	e	r
p	0	5	5	8	13	4		2	8	15	7	4	17
5p+8	8	33	33	48	73	28		18	48	83	43	28	93
(5p+8) mod26	8	7	7	22	21	2		18	22	5	17	2	15
Ciphertext (C)	I	H	H	W	V	C		S	W	F	R	C	P

Example: Decrypt the ciphertext: **"IHHWVC SWFRCP"**, using the key: k_1=5, k_2=8, using Affine cipher.

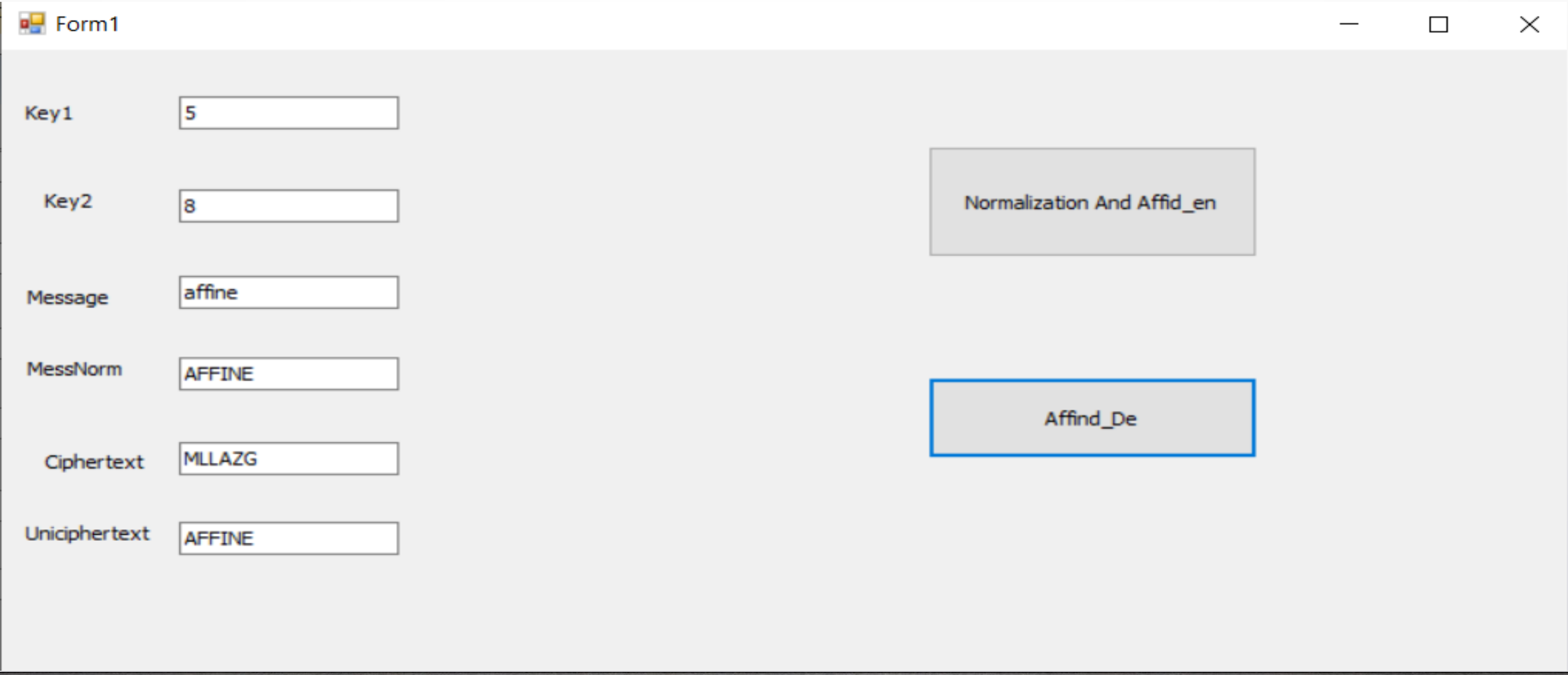
Ans. :

p=D(k_1, k_2, C)= k_1^{-1} (C - k_2) mod 26, where k_1^{-1} = 21

k_1	1	3	5	7	9	11	15	17	19	21	23	25
k_1^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext (C)	I	H	H	W	V	C		S	W	F	R	C	P
C	8	7	7	22	21	2		18	22	5	17	2	15
C-8	0	-1	-1	14	13	-6		10	14	-3	9	-6	7
21(C-8)	0	-21	-21	294	273	-126		210	294	-63	189	-126	147
21(C-8) mod26	0	5	5	8	13	4		2	8	15	7	4	17
Plaintext	a	f	f	i	n	e		c	i	p	h	e	r


Form1
Key1
5
Key2
8
Message
affine
MessNorm
AFFINE
Ciphertext
MLLAZG
Uniciphertext
AFFINE
Normalization And Affid_en
Affind_De