❑ Affine Cipher

Addition (shifting) and multiplication can be combined to give an Affine transformation.

Encryption:

C=E(k_1, k_2, p)=(k_1 x p + k_2) mod n = (k_1 x p + k_2) mod 26

Decryption:

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

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) mod 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: $\mathbf{k_1}$=5, $\mathbf{k_2}$=8, using Affine cipher.

Ans. :

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

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

Example: Encrypt the plaintext: "its cool", using the key: $\mathbf{k_1}$=5, $\mathbf{k_2}$=8, using Affine cipher.

Ans. : $\mathbf{C=E(k_1, k_2, p)=(k_1 \times p + k_2) \bmod 26}$

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	i	t	s		c	o	o	l
p	8	19	18		2	14	14	11
5p+8	48	103	98		18	78	78	63
(5p+8) mod26	22	25	20		18	0	0	11
Ciphertext (C)	W	Z	U		S	A	A	L

Example: Decipher **"HPCCXAQ"** if the encipherment function is E(x) = (5x + 8) MOD 26, using Affine cipher.

Ans. : $\mathbf{p=D(k_1, k_2, C)= k_1^{-1} (C - k_2) \bmod 26}$

where $k_1^{-1} = 21$

Ciphertext (C)	H	P	C	C	X	A	Q
C	7	15	2	2	23	0	16
C-8	-1	7	-6	-6	15	-8	8
21(C-8)	-21	147	-126	-126	315	-168	168
21(C-8) mod26	5	17	4	4	3	14	12
Plaintext	f	r	e	e	d	o	m