❑ 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 .....(7)

Decryption:

p=D(k_1, k_2, C)= k_1^{-1} (C - k_2) mod n = k_1^{-1} (C - k_2) mod 26 .....(8)

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

Example: Suppose that an Affine cipher E(x) = (ax + b) mod 26 enciphers h as **X** and q as **Y**. Find the cipher (that is, determine a and b).

Ans. : C=E(p)=(k_1 x p + k_2) mod 26, suppose that k_1=a, p=x, k_2=b.

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

We see that h → X means E(7) = 23 and q → Y means E(16) = 24.

That is, a · 7 + b ≡ 23 (mod 26) and a · 16 + b ≡ 24 (mod 26).

Subtracting gives 16a − 7a ≡ 1 (mod 26)

(mod 26) = 3. So that 9a ≡ 1 (mod 26). Therefore, a = 9^{-1}

Finally, we substitute a = 3 into either of the earlier equations and solve for b,

i.e., 3 · 7 + b ≡ 23 (mod 26) implies b = 2.

In summary, E(x) = (3x + 2) mod 26.

❑ Mixed Alphabet

If we permit the cipher alphabet to be any rearrangement of the plain alphabet, then we can generate an enormous number of distinct modes of encryption. There are 26! such rearrangements, which is greater than 4×10^{26} which gives rise to an equivalent number of distinct cipher alphabets. Each cipher alphabet is known as a key. If our message is intercepted by the enemy, who correctly assumes that we have used a monoalphabetic substitution cipher, they are still faced with the impossible challenge of checking all possible keys. If an enemy agent could check one of these possible keys every second, it would take roughly one billion times the lifetime of the universe to check all of them and find the correct one. The disadvantage of this method is that the arrangement is difficult to be remembered. It would involve both sender and recipient to remember a random string of 26 letters. In the table below is one such random ciphertext alphabet.

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

A Mixed Ciphertext alphabet, where the order of the ciphertext letters has been selected randomly.

❑ Keyword Mixed or Alphabet Mixing via a Keyword

A keyword or key phrase can be used to mix the letters to generate the cipher alphabet.

In this method we need a **keyword** like **MATHEMATICS**, and a **keyletter** like **S**, then:

- Remove the repeated letters from the keyword, and you will get MATHEICS.
- Put the first letter of the modified keyword under the keyletter followed by the remaining letters of the keyword.
- Complete the ciphertext alphabet by the remaining letters without repetitions.

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

Example: Encrypt the message “meet at ten in the park”, using a keyword Mixed cipher for a given keyword (**MATH**) and key latter a.

Ans. :

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

Ciphertext: “KBBS MS SBL FL SEB OMQI”.

Example: Decrypt the message **"ANA, F WMR WQNLD. KY TNVBQ FR CFLB.** MJFTB", using a keyword Mixed cipher for a given keyword (**MATH**) and key letter a.

Ans. :

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

The Plaintext: "bob, i was wrong. my cover is fine. alice".

❑ Transposed Keyword Mixed or Alphabet Mixing via a Columnar Transposition

In this method we need a **keyword** like **MATHEMATICS**. After removing the repeated letters, we put it in a matrix with number of columns equal to the number of the letters in the modified keyword. The letters of the keyword form the headings of the columns and the remaining letters of the alphabet fill in order in the rows below. Then, Mixing is achieved by transcribing columns and taking the matrix letters column by column and we will get:

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

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

Example: Encrypt the message “far above cayuga’s waters”, using Transposed Keyword Mixed for a given keyword (**CORNELL**).

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

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

Ans. : Ciphertext: “OCV CANWY ICQPBC’E LCGYVE”.