Affine Cipher Method

Affine method is used to encrypt and decrypt the message. Tow operation can be applied to get the encryption processes which are addition and multiplication. So the 'key' for the affine cipher consists of 2 numbers, that mean two key need in this algorithm k_1 and k_2. The k_1 must be odd number in the range (0- 25) except 13 while the k_2 may be any number in the same range.

The encryption low is:

$$C = (k_1 * p + k_2) \bmod 26$$

The decryption low is:

$$P = [k_1^{-1} * (c - k_2)] \bmod 26$$

k_1 only used in the encryption process and must be the range as shown in the table below. Whereas $\mathbf{k_1^{-1}}$ is used only in the decryption process.

If k_1 is equal to 3 in the encryption process, then the $\mathbf{k_1^{-1}}$ is equal to 9 in the decryption process and so on.

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

Example 1

Use the affine algorithm to encrypt the message **"COMPUTER",** if the first key is 5 and the second key is 4

Solution

Encryption process

The encryption function is $C = (k_1 * p + k_2) \bmod 26$

C(c)	=	(5	*	2	+ 4)	= 14	Mod 26	= 14	o
C(o)	=	(5	*	14	+ 4)	= 74	Mod 26	= 22	w
C(m)	=	(5	*	12	+ 4)	= 64	Mod 26	= 12	m
C(p)	=	(5	*	15	+ 4)	= 79	Mod 26	= 1	b
C(u)	=	(5	*	20	+ 4)	= 104	Mod 26	= 0	a
C(t)	=	(5	*	19	+ 4)	= 99	Mod 26	= 21	v
C(e)	=	(5	*	4	+ 4)	= 24	Mod 26	= 24	y
C(r)	=	(5	*	17	+ 4)	= 89	Mod 26	= 11	l

The ciphertext is "**owmbavyl**"

Example 2

Use the affine algorithm to decrypt the ciphertext is "**dwmbavyl**", $\mathbf{K_2}$ is the same equal to **4 and** the $\mathbf{k_1} = \mathbf{5}$

Answer

In the solution we take the value of $\mathbf{k_1^{-1} = 21}$ because $k_1 = 5$ in encryption process

$$P = [\, k_1^{-1} * (c - k_2) \,] \bmod 26$$

P (o)	=	[21*	(14 - 4)]	= 210	Mod 26	=	2	c
P (w)	=	[21*	(22 - 4)]	= 378	Mod 26	=	14	o
P (m)	=	[21*	(12 - 4)]	= 168	Mod 26	=	12	m
P (b)	=	[21*	(1- 4)]	= - 63	Mod 26	=	-11 + 26 = 15	p
P (a)	=	[21*	(0- 4)]	= -84	Mod 26	=	- 6 + 26 = 20	u
P (v)	=	[21*	(21 - 4)]	= 357	Mod 26	=	19	t
P (y)	=	[21*	(24 - 4)]	= 420	Mod 26	=	4	e
P (l)	=	[21*	(11 - 4)]	= 147	Mod 26	=	17	r

NOTE if the result of $(i - k_2)$ is minus, then take its mode and the final result subtract it from the 26 as shown above in p (b) and p (a) .