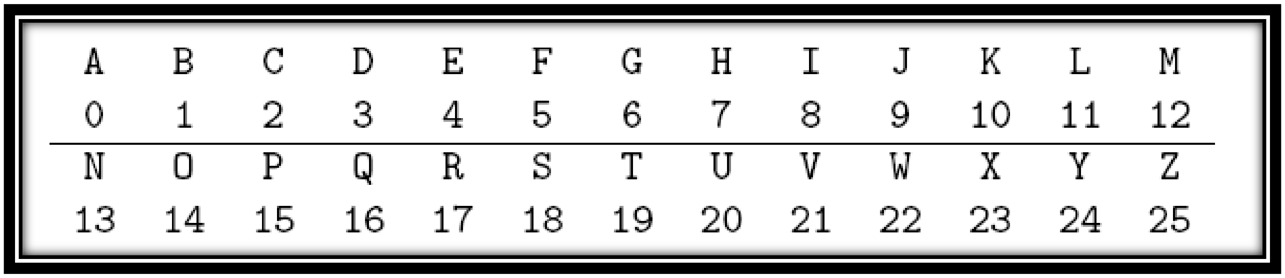
Affine Cipher Example

Encryption

$$E(x) = (ax + b) \,\mathrm{MOD}\, 26$$

is called an affine cipher. Here **x** is the numerical equivalent of the given plaintext letter, **a** and **b** are (appropriately chosen) integers. 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

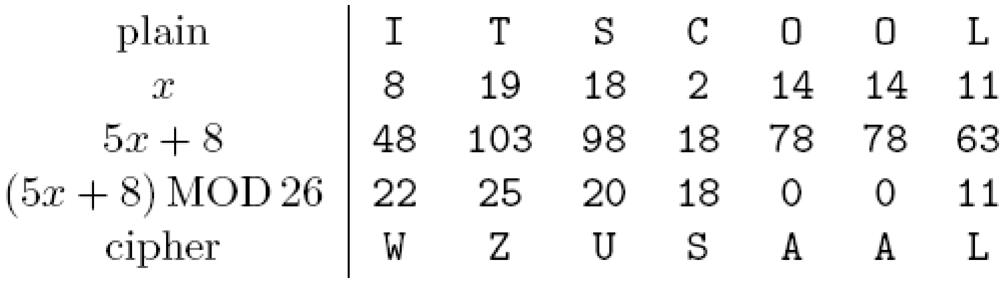
Example:

Plain Text: Its cool

A=5
B=8

$$E(x) = (5x + 8) \,\mathrm{MOD}\, 26.$$

Solution: Filling in the following table gives



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
$(5x + 8) \,\mathrm{MOD}\, 26$	22	25	20	18	0	0	11
cipher	W	Z	U	S	A	A	L

Decryption

$$E^{-1}(y) = a^{-1}(y - b)\,\mathrm{MOD}\,26.$$

Example:

Cipher Text: HPCCXAQ

Encryption Function:

$$E(x) = (5x + 8)\,\mathrm{MOD}\,26.$$

So Decryption Function is:

$$E^{-1}(y) = a^{-1}(y - b)\,\mathrm{MOD}\,26.$$

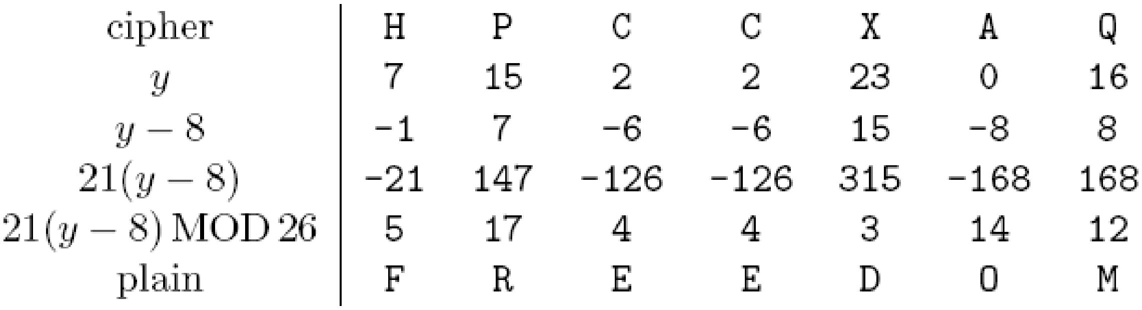
Multiplication Inverse of a is 21

a^{-1} =21

So

$$E^{-1}(y) = 21(y - 8)\,\mathrm{MOD}\,26$$

and so filling in our table gives



cipher	H	P	C	C	X	A	Q
y	7	15	2	2	23	0	16
$y - 8$	-1	7	-6	-6	15	-8	8
$21(y - 8)$	-21	147	-126	-126	315	-168	168
$21(y - 8)\,\mathrm{MOD}\,26$	5	17	4	4	3	14	12
plain	F	R	E	E	D	O	M