

Affine Cipher – An Introduction to Algebra and Modular Arithmetic

RLOIN RLOPZ HPHOI NHZPN YZNJI PZIGA LJHYN
ZNHHL AXZFY ZKVHP FYHSN YWLRP YMNPA ZN

The Affine Cipher

The affine cipher works by converting the letters in the message to numbers, doing some math on the numbers and converting the numbers back to letters.

The correspondence between the alphabet and numbers is normal alphabetic order:

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
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	26

The secret key used to encode the message consists of two numbers m and a . The plaintext letter's number is p and the ciphertext's number is c . The formula for computing the ciphertext letter is $c = m(p + a) \bmod 26$.

The **mod** in this formula is an abbreviation for modulo, and it means we need to use modular arithmetic. You may have worked with modular arithmetic in earlier math classes under the name "Clock Arithmetic."

Addition, Subtraction and Multiplication in modulo N

The basic idea of "modulo N" arithmetic is that suddenly our world only has N numbers in it! The numbers we use are 0 through N-1. Whenever arithmetic gives us a number greater than N we need to divide the number by N and only keep the *remainder*. Whenever we get a number that is less than 0 we need to add multiples of N until the result is in the range 0 through N-1.

Examples:

$4 + 11 = 15 \bmod 26$	(no surprise here!)
$17 + 13 = 4 \bmod 26$	($17 + 13 = 30$; $30 / 26 = 1$ R 4; keep the remainder.)
$5 - 12 = 19 \bmod 26$	($5 - 12 = -7$; $-7 + 26 = 19$)
$8 \times 9 = 20 \bmod 26$	($8 \times 9 = 72$; $72 / 26 = 2$ R 20)

Encrypting a Message

Let's encrypt the message "Meet me after school" using key $m = 3$, $a = 7$.

M	e	e	t		m	e		a	f	t	e	r		s	c	h	o	o	l
13	5	5	20		13	5		1	6	20	5	18		19	3	8	15	15	12
$c = 3(p + 7) \bmod 26$																			
8	10	10	3		8	10		24	13	3	10	23		0	4	19	14	14	5
H	J	J	C		H	J		X	M	C	J	W		Z	D	S	N	N	E

The second row of numbers is the result of the formula $c = 3(p + 7) \bmod 26$. Use the letter correspondence to translate these numbers to the ciphertext. Note that $Z = 26 = 0 \bmod 26$ so the 0 translates to Z. Here's the encrypted message.

Affine Cipher – An Introduction to Algebra and Modular Arithmetic

HJJCH JXMCJ WZDSN NE

(It's conventional when doing ciphers by hand to write the ciphertext in same-sized groups of letters, usually 5. This helps make sure you don't skip any letters when copying the message.)

Doing all those mod 26 multiplications by hand was a lot of work. You should make a mod 26 multiplication table.

Decryption and Modular Division

How does our friend decode the message when he gets it? He knows the key is $m = 3$, $a = 7$ so all he has to compute is the inverse of the enciphering function: $p = \frac{c}{m} - a \pmod{26}$. This shouldn't be too hard: H is 8, so $8 / 3$ is ... um ... ???

To do modular division we need to remember what the definition of division is. Division is the answer to the question "What times this equals that?" So $8 / 3 \pmod{26}$ answers "What times 3 equals 8 mod 26?"

The easiest way to do this is to look on the 3 row of your multiplication table for the answer 8 and note that it's in the 20 column, so that's the answer to $8 / 3$. Now subtract a from 20 to get 13, so the first plaintext letter is M. Keep doing this for every letter in the ciphertext.

Decryption can be done a bit faster by rearranging the deciphering function to:

$p = \frac{1}{m}c - a \pmod{26}$. Now we only need to do one division to find the inverse of m . The inverse of 3 is 9 so the deciphering function for this message is: $p = 9c - 7 \pmod{26}$. (Note that the order of multiplication and addition are reversed in the deciphering function compared to the enciphering function.)

Picking m

To be able to decrypt the message, we need to be able to divide by m . There is an interesting feature of modular division – you cannot divide by all values of m . Some division problems have no answer; some have multiple answers.

Look at your multiplication table. How many answers are there for "What times 4 equals 20?" $20 / 4$ has two answers: 5 and 18! $0 / x$ can have multiple answers and so can x / x .

To pick an m that works, m and 26 must be relatively prime (their GCD must be 1).

Try it Yourself

Decrypt this message that was enciphered using key $m = 19$, $a = 2$:

GHSGE IBHCB CEQHC PPKI ICSCJ HCQKU FJRBQ KRBPK FHAID UDAFI

Cryptanalysis of the Affine Cipher

The ciphertext at the top of the paper was encoded using the affine cipher. How can we decipher it when we don't know the values of m and a ?

English Letter Probability

To be able to make good guesses about what the ciphertext might mean it is very useful to know about the probability of letters and combinations of letters in English (or whatever language you think the plaintext is). Here are some tables for English:

Single letter		Double letter		Digram		Trigram	
E	12.64%	TT	21.87%	TH	4.83%	THE	2.64%
T	10.00%	LL	16.46%	HE	4.58%	AND	0.89%
A	8.59%	EE	14.64%	ER	2.67%	ING	0.74%
O	7.64%	SS	12.88%	IN	2.36%	HER	0.60%
N	6.74%	OO	11.59%	AN	2.23%	ERE	0.51%
H	6.59%	PP	3.65%	RE	1.72%	NTH	0.42%
S	6.29%	FF	3.31%	ND	1.63%	THA	0.41%
I	6.13%	RR	3.28%	ES	1.60%	DTH	0.38%
R	5.62%	DD	3.22%	ED	1.59%	WAS	0.37%
D	4.37%	NN	2.44%	NT	1.58%	TTH	0.36%
L	3.95%	MM	1.68%	TO	1.56%	HES	0.36%
U	2.74%	GG	1.21%	OU	1.44%	ETH	0.36%
W	2.51%	HH	1.13%	AT	1.41%	OTH	0.35%
G	2.24%	WW	0.73%	EA	1.38%	SAI	0.34%
C	2.21%	CC	0.53%	HA	1.37%	HAT	0.34%
M	2.21%	YY	0.48%	ST	1.36%		
P	1.94%	BB	0.41%	AS	1.32%		
F	1.90%	AA	0.30%	ET	1.31%		
Y	1.84%	UU	0.08%	EN	1.30%		
B	1.57%	II	0.05%	ON	1.29%		
K	1.02%	ZZ	0.04%	IT	1.26%		
V	0.76%	KK	0.02%	NG	1.21%		
J	0.27%			SA	1.17%		
X	0.12%			TE	1.16%		
Q	0.07%			RO	1.05%		
Z	0.05%			TT	1.05%		
				AR	1.02%		
				HI	1.01%		
				WA	0.98%		
				OR	0.96%		
				NE	0.94%		
				TI	0.92%		
				LE	0.90%		

Affine Cipher – An Introduction to Algebra and Modular Arithmetic

RLOIN RLOPZ HPHOI NHZPN YZJNI PZIGA LJHYN
ZNHHL AXZFY ZKVHP FYHSN YWLRP YMNPA ZN

Look at the ciphertext and search for repeated digrams and trigrams. The repeated trigrams are RLO and OIN. The repeated digram are ZN (3 times) and FY, HP, IN, LO, NH, NY, OI, PZ, RL, YZ.

The most common trigram in English is THE, and THE is a great first word in a message, so let's assume that TH (20, 8) enciphers to RL (18, 12) and see if we can solve for m and a using simultaneous equations.

$$\left. \begin{array}{l} m(20 + a) = 18 \\ m(8 + a) = 12 \\ 20m + ma = 18 \\ 8m + ma = 12 \\ 12m = 6 \\ m = \frac{6}{12} \\ m = 7 \text{ or } 20 \end{array} \right\} \text{mod } 26$$

20 is not a legal value for m so assume m is 7 and solve for one of the above equations for a .

$$\left. \begin{array}{l} 8 \cdot 7 + 7a = 12 \\ 4 + 7a = 12 \\ 7a = 8 \\ a = \frac{8}{7} \\ a = 16 \end{array} \right\} \text{mod } 26$$

Start decrypting with the assumed key $m = 7, a = 16$: thaol thapj zpza

This doesn't look good so let's try the other trigram for THE. Assume that TH (20, 8) enciphers to OI (15, 9).

$$\left. \begin{array}{l} m(20 + a) = 15 \\ m(8 + a) = 9 \\ 20m + ma = 15 \\ 8m + ma = 9 \\ 12m = 6 \\ m = \frac{6}{12} \\ m = 7 \text{ or } 20 \end{array} \right\} \text{mod } 26$$

It's just a coincidence that m has the same value as last time. So let's substitute 7 into one of the equations and see what we get for a this time.

$$\left. \begin{array}{l} 8 \cdot 7 + 7a = 9 \\ 4 + 7a = 9 \\ 7a = 5 \\ a = \frac{5}{7} \\ a = 23 \end{array} \right\} \text{mod } 26$$

Start decrypting with the assumed key $m = 7, a = 23$: mathe matic sith

This looks like English! Decipher the rest of the message: escie ncewh ichdr awsne cessa rycon clusi onsbe njami npeir ce

Break it into words and we get:

"Mathematics is the science which draws necessary conclusions."
– Benjamin Peirce

If the trigrams don't let you break the cipher you need to start trying the most common digrams to set up the equations. It may take a while, but you should be able to crack any affine cipher this way if the message isn't too short.

Decrypting by Encrypting

Consider this:

$$c = m(p + a)$$

$$p = \frac{1}{m}c - a$$

$$p = \frac{1}{m}(c - ma)$$

$$\text{Let } n = \frac{1}{m}, \quad b = -ma$$

$$p = n(c + b)$$

So, if you encipher a message with key m, a and then **encipher** the ciphertext with key n, b you get right back to the starting message. Here's the "Meet me after school" message again. It was enciphered using key $m = 3, a = 7$.

M	e	e	t		m	e		a	f	t	e	r		s	c	h	o	o	l
13	5	5	20		13	5		1	6	20	5	18		19	3	8	15	15	12
$c = 3(p + 7) \text{ mod } 26$																			
8	10	10	3		8	10		24	13	3	10	23		0	4	19	14	14	5
H	J	J	C		H	J		X	M	C	J	W		Z	D	S	N	N	E

Affine Cipher – An Introduction to Algebra and Modular Arithmetic

$$\text{Let } n = \frac{1}{m}, \quad b = -ma$$

$$n = \frac{1}{3} = 9 \pmod{26}, \quad b = -3 \cdot 7 = -21 = 5 \pmod{26}$$

and encipher using key $m = 9, a = 5$.

H	J	J	C		H	J		X	M	C	J	W		Z	D	S	N	N	E
8	10	10	3		8	10		24	13	3	10	23		26	4	19	14	14	5
$c = 9(p + 5) \pmod{26}$																			
13	5	5	20		13	5		1	6	20	5	18		19	3	8	15	15	12
M	e	e	t		m	e		a	f	t	e	r		s	c	h	o	o	l

Modulo 26 Multiplication Table

\times_{26}	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
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	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
2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
8	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
9	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
10	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
11	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
12	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
14	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
15	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
16	0	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
17	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
18	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
19	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
20	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
21	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
22	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
23	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
24	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
25	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Modulo 26 Division Table

\div_{26}	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
0	—	0	0,13	0	0,13	0	0,13	0	0,13	0	0,13	0	0,13	0,2,4, 6,8, 10,12, 14,16, 18,20, 22,24	0,13	0	0,13	0	0,13	0	0,13	0	0,13	0	0,13	0
1	—	1	—	9	—	21	—	15	—	3	—	19	—	—	—	7	—	23	—	11	—	5	—	17	—	25
2	—	2	1,14	18	7,20	16	9,22	4	10,23	6	8,21	12	11,24	—	2,15	14	5,18	20	3,16	22	4,17	10	6,19	8	12,25	24
3	—	3	—	1	—	11	—	19	—	9	—	5	—	—	—	21	—	17	—	7	—	15	—	25	—	23
4	—	4	2,15	10	1,14	6	5,18	8	7,20	12	3,16	24	9,22	—	4,17	2	10,23	14	6,19	18	8,21	20	12,25	16	11,24	22
5	—	5	—	19	—	1	—	23	—	15	—	17	—	—	—	9	—	11	—	3	—	25	—	7	—	21
6	—	6	3,16	2	8,21	22	1,14	12	4,17	18	11,24	10	7,20	—	6,19	16	2,15	8	9,22	14	12,25	4	5,18	24	10,23	20
7	—	7	—	11	—	17	—	1	—	21	—	3	—	—	—	23	—	5	—	25	—	9	—	15	—	19
8	—	8	4,17	20	2,15	12	10,23	16	1,14	24	6,19	22	5,18	—	8,21	4	7,20	2	12,25	10	3,16	14	11,24	6	9,22	18
9	—	9	—	3	—	7	—	5	—	1	—	15	—	—	—	11	—	25	—	21	—	19	—	23	—	17
10	—	10	5,18	12	9,22	2	6,19	20	11,24	4	1,14	8	3,16	—	10,23	18	12,25	22	2,15	6	7,20	24	4,17	14	8,21	16
11	—	11	—	21	—	23	—	9	—	7	—	1	—	—	—	25	—	19	—	17	—	3	—	5	—	15
12	—	12	6,19	4	3,16	18	2,15	24	8,21	10	9,22	20	1,14	—	12,25	6	4,17	16	5,18	2	11,24	8	10,23	22	7,20	14
13	—	13	—	13	—	13	—	13	—	13	—	13	—	0,2,4, 6,8, 10,12, 14,16, 18,20, 22,24	—	13	—	13	—	13	—	13	—	13	—	13
14	—	14	7,20	22	10,23	8	11,24	2	5,18	16	4,17	6	12,25	—	1,14	20	9,22	10	8,21	24	2,15	18	3,16	4	6,19	12
15	—	15	—	5	—	3	—	17	—	19	—	25	—	—	—	1	—	7	—	9	—	23	—	21	—	11
16	—	16	8,21	14	4,17	24	7,20	6	2,15	22	12,25	18	10,23	—	3,16	8	1,14	4	11,24	20	6,19	2	9,22	12	5,18	10
17	—	17	—	23	—	19	—	21	—	25	—	11	—	—	—	15	—	1	—	5	—	7	—	3	—	9
18	—	18	9,22	6	11,24	14	3,16	10	12,25	2	7,20	4	8,21	—	5,18	22	6,19	24	1,14	16	10,23	12	2,15	20	4,17	8
19	—	19	—	15	—	9	—	25	—	5	—	23	—	—	—	3	—	21	—	1	—	17	—	11	—	7
20	—	20	10,23	24	5,18	4	12,25	14	9,22	8	2,15	16	6,19	—	7,20	10	11,24	18	4,17	12	1,14	22	8,21	2	3,16	6
21	—	21	—	7	—	25	—	3	—	11	—	9	—	—	—	17	—	15	—	23	—	1	—	19	—	5
22	—	22	11,24	16	12,25	20	8,21	18	6,19	14	10,23	2	4,17	—	9,22	24	3,16	12	7,20	8	5,18	6	1,14	10	2,15	4
23	—	23	—	25	—	15	—	7	—	17	—	21	—	—	—	5	—	9	—	19	—	11	—	1	—	3
24	—	24	12,25	8	6,19	10	4,17	22	3,16	20	5,18	14	2,15	—	11,24	12	8,21	6	10,23	4	9,22	16	7,20	18	1,14	2
25	—	25	—	17	—	5	—	11	—	23	—	7	—	—	—	19	—	3	—	15	—	21	—	9	—	1