# Cryptography Worksheet — The Affine Cipher 1

The Affine Cipher is a cipher that uses Maths to encode the message. It works by converting every letter in the alphabet into a number, performing a function on that number, and turning the result back into a letter. When converting letters into numbers, we use the following:

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

Example 1 (KEY: Add 3)

Plaintext: Julius Caesar used codes

Numerical translation: 9,20,11,8,20,18,2,0,4,18,0,17,20,18,4,3,2,14,3,18

Transform (add 3): 12,23,14,11,23,21,5,3,7,21,3,20,23,21,7,6,5,17,6,21

Ciphertext: MXOLXVFDHVDUXVHGFRGV

This is an Affine Cipher with Key Function "ADD 3". *How else could we describe this enciphering?*

*Does the Affine Cipher work if we use the Key Function* "MULTIPLY BY 3" *instead?* Look at Example 2.

Example 2 (KEY: Multiply by 3)

Plaintext: Look Carefully

Numerical translation: 11,14,14,10,2,0,17,4,5,20,11,11,24

Transform: 7,16,16,…

Ciphertext: HQQ…

*How does 11 × 3 = 7? Or 14 × 3 = 16?*

HINT: When telling the time, what is 10am + 4hours? How does this relate to our situation?

*Complete the enciphering for Example 2.*

We have used a key to add and a key to multiply. *Can you use a key to do both?*

*Encipher the plaintext* "Cryptography" *using the Key Function* "MULTIPLY BY 3 then ADD 4".

# Cryptography Worksheet — The Affine Cipher 2

We have seen the use of a key when using the Affine Cipher, and we know that we can either add, multiply or do both in our function. Here is how we write the Key Function for "MULTIPLY BY 9 then ADD 7".

$$C = (9P + 7) \bmod 26$$ where $P$ = plaintext number and $C$ = ciphertext number

This tells us to take the number of the plaintext (uncoded) letter and multiply it by 9, and then add 7 to it. The "mod 26" stands for "modulo arithmetic", and simply means divide by 26 and take the remainder.

For example, to encipher G using this key:

1) G is given by the number 6.
2) $(9 \times 6) + 7 = 61$.
3) $61 \div 26 = 2$r. 9
   so $61 = 9 \bmod 26$.
4) 9 represents the ciphertext letter J.

We can do this for the whole alphabet, and show it in a table, from which we can more easily convert plaintext to ciphertext:

| **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** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 7 | 16 | 25 | 8 | 17 | 0 | 9 | 18 | 1 | 10 | 19 | 2 | 11 | 20 | 3 | 12 | 21 | 4 | 13 | 22 | 5 | 14 | 23 | 6 | 15 | 24 |
| **H** | **Q** | **Z** | **I** | **R** | **A** | **J** | **S** | **B** | **K** | **T** | **C** | **L** | **U** | **D** | **M** | **V** | **E** | **N** | **W** | **F** | **O** | **X** | **G** | **P** | **Y** |

*Using the Key* $C = (7P + 3) \bmod 26$, *encipher the plaintext:*

"Success is a journey, not a destination"

*Using the Key* $C = 4P \bmod 26$, *encipher the plaintext:*

*"Never say never"*

*What is the problem with this key? Can you explain why?*

*Find all possible keys. What are the requirements for a key to work?*

# Cryptography Worksheet — The Affine Cipher 3

We now know how to encrypt a message using an Affine Cipher. However, it is just as important that we can decrypt the message at the other end, otherwise the person we are sending the message to will not be able to read it. We have received the ciphertext "E" from a friend, and we know that the key used was ***C* = (3*P* + 1) mod 26**. *What do we need to work out?*

*If the ciphertext is* "E"*, what is C equal to?*

*How do we solve this equation (remember that we are working* mod 26*)*?

Example 1. Ciphertext= E, so C=5

| | |
|---|---|
| 5 = (3P+1) mod26 | (1) subtract the 1 |
| 4 = (3P) mod26 | (2) multiply by 9 |
| 36=27P mod26 | (3) REMEMBER!!!! Because it is mod26 we divide by 26 and take the remainder!!! |
| 10=P mod26 | |

Hence the plaintext letter was K.

*Why did we multiply by 9 instead of dividing by 3?*

*What would we need to multiply by if the key was 5P instead of 3P?*

The following message was encoded using the key ***C* = (3*P* + 4) mod 26**. *Decode it.*

(NOTE: it has been split into blocks of 5 letters to make it easier to read)

URQDC RWJUD MLQJZ QOURQ DCRWJ UDMLQ JZQOU RQDCR WJUTC RNDML QURQD
CRWJU HDCRW DMLQE LLERN CRNCR JZQNE DIRQG GHCRN JZQO

*Write a message of your own, and give the ciphertext and the key to a friend to decipher.*

# Teacher's Notes — The Affine Cipher

**Worksheet 1**

The Affine Cipher is a more complex cipher that uses the Mathematics of functions to encipher the plaintext. First explain that the letters of the alphabet must be converted into numbers, and ask the pupils for any ideas of how to do this. Note that we start at 0 (not 1), and explain that this is just convention as it makes the Maths slightly easier to do (we will be working modulo 26). Show the table on the board, and go through Example 1 on the board, first converting the letters to their respective numbers, then performing the function on these numbers, and finally converting the numbers back to letters. Ask if anyone recognises this enciphering (it is a Caesar Shift of 3).

Ask them in pairs to look at Example 2, and to work out how $11 \times 3 = 7$ ($11 \times 3 = 33 \bmod 26 = 7$, it is the remainder when 33 is divided by 26). For those that are struggling, use Clock Arithmetic to help.

The solution to Example 2 is 7,16,16,4,6,0,25,12,15,8,7,7,20, with a ciphertext HQQEGAZMPIHHY.

(KEY: Multiply by 3 then Add 4)

Plaintext: Cryptography

Numerical translation: 2,17,24,15,19,14,6,17,0,15,7,24

Transform: 10,3,24,23,9,20,22,3,4,23,25,24

Ciphertext: KDYXJUWDEXZY

**Worksheet 2**

It is recommended that you spend a little bit of time going through some modulo arithmetic before starting this sheet.

Ask the pupils how you could write a formula for $C$ in terms of $P$ given that you need to multiply $P$ by 9 then add 7. Go through the example of how to convert a plaintext letter to its ciphertext letter, and emphasise that for longer messages, it is usually quicker to first calculate the whole alphabet in table form, and then perform the substitutions. To work out the values for the table, ask them if they can spot any patterns in the way they increase (it is adding 9 each time, but working modulo 26, so 25 + 9 = 8). For higher ability sets, this could be linked to arithmetic sequences.

The table for the key $\boldsymbol{C = (7P + 3) \bmod 26}$ is shown below, along with the ciphertext.

| **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** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 3 | 10 | 17 | 24 | 5 | 12 | 19 | 0 | 7 | 14 | 21 | 2 | 9 | 16 | 23 | 4 | 11 | 18 | 25 | 6 | 13 | 20 | 1 | 8 | 15 | 22 |
| **D** | **K** | **R** | **Y** | **F** | **M** | **T** | **A** | **H** | **O** | **V** | **C** | **J** | **Q** | **X** | **E** | **L** | **S** | **Z** | **G** | **N** | **U** | **B** | **I** | **P** | **W** |

ZNRRFZZHZDOXNSQFPQXGDYFZGHQDGHXQ.

# Teacher's Notes — The Affine Cipher

**Worksheet 2 (cont)**

The table for the second encryption is below.

| **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** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | 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 |
| **A** | **E** | **I** | **M** | **Q** | **U** | **Y** | **C** | **G** | **K** | **O** | **S** | **W** | **A** | **E** | **I** | **M** | **Q** | **U** | **Y** | **C** | **G** | **K** | **O** | **S** | **W** |

This causes problems because more than one plaintext letter are enciphered to the same ciphertext letter. This is not a problem in encrypting, but when it comes to decrypting this message, we won't know whether an "A" is meant to be and "a" or an "n", for example. This is because the greatest common divisor of 4 and 26 is not 1 (i.e. they have a common factor, namely 2). If you wish to explain in more detail to a top set then you can briefly mention Group Theory, and it is because 4 has no multiplicative inverse in the group of integers mod 26 under multiplication.

Any number between 0 and 25 that does not share any factors with 26 will make a good multiplicative element to the key (NOTE that multiplying by 30 is the same as multiplying by 30 - 26 = 4). Then we can add on any number between 0 and 25, since they do not affect whether the key works or not (once again note that adding on 30 is the same as adding on 4). Also, note that subtracting 2 is the same as adding 24. So, in total there are 12 numbers in the range that work as keys (the prime factors of 26 are 2 and 13, so the multiples of these in the range will not work as keys), and for each of these there are 26 options for the additive element. So there are 12 × 26 = 312 possible keys, of which 26 are the trivial Caesar Shifts.

This activity has great potential for the pupils to use a Spreadsheet to work out the ciphertext numbers using the formula. For the Key ***C* = (7*P* + 3) mod 26**, type in what is shown on the right (note—to show formulae in Excel press CTRL + `).

| Plaintext Letter | Plaintext Number | Function | Ciphertext Number | Ciphertext Letter |
|---|---|---|---|---|
| A | =CODE(A2)-65 | =(9*B2)+7 | =MOD(C2,26) | =CHAR(D2+65) |
| B | =CODE(A3)-65 | =(9*B3)+7 | =MOD(C3,26) | =CHAR(D3+65) |
| C | =CODE(A4)-65 | =(9*B4)+7 | =MOD(C4,26) | =CHAR(D4+65) |
| D | =CODE(A5)-65 | =(9*B5)+7 | =MOD(C5,26) | =CHAR(D5+65) |
| E | =CODE(A6)-65 | =(9*B6)+7 | =MOD(C6,26) | =CHAR(D6+65) |

| Plaintext Letter | Plaintext Number | Function | Ciphertext Number | Ciphertext Letter |
|---|---|---|---|---|
| A | 0 | 7 | 7 | H |
| B | 1 | 16 | 16 | Q |
| C | 2 | 25 | 25 | Z |
| D | 3 | 34 | 8 | I |
| E | 4 | 43 | 17 | R |

And get as an output what is on the left.

# Teacher's Notes — The Affine Cipher

**Worksheet 3**

Emphasise that for a cipher to be of any use, then it needs to be easy to encrypt a message, but also easy to decrypt the message, if you know the key. It should also be hard to decrypt the message for people who do not have the key used. What we need to do, is solve the equation for $P$, since we know that $C = 5$. Once the pupils have come up with

$$5 = (3P + 1) \bmod 26$$

Ask them what you need to do to get $P$ by itself, to which they should respond with "subtract 1" (NOTE— the brackets do not serve their usual purpose here, but indicate we are working modulo 26, which applies to both sides of the equation):

$$4 = (3P) \bmod 26$$

Ask them what the next step is, to which the response will come "divide by 3". Ask if we can get $1P$ by multiplying by a whole number (remind them we are working modulo 26). If none of the class can see it, assert that we want to "multiply by 9", and ask them why we would want to do this. This is because $9 \times 3 = 27 = 1 \bmod 26$ (or in Group Theoretic terms, 9 is the multiplicative inverse of 3 in the integers modulo 26).

$$36 = 27P \bmod 26$$

Once again, note that we are working modulo 26, and so we must divide each number by 26, and take the remainder, to get:

$$10 = P \bmod 26$$

So the plaintext letter is "k".

For the higher ability, it is probably better to talk about this in terms of rearranging the formula, so that when it comes to using the decryption process for many letters, they can use the formula instead of having to do this each time. In that case, you should get $9 \times (C - 1) = P \bmod 26$.

In the case when it is $5P$, you would need to multiply by 21 to get 105, which is one more than 104, a multiple of 26.

Make a note of the fact that the long message has been split into blocks of 5 letters of ciphertext, something used regularly in cryptography. It is partly to do with transmitting messages, and partly to do with making the ciphertext more easily digestible for the receiver. Importantly, the spaces are not where the spaces are in the original message.

The message decodes as:

"One ring to rule them all, One ring to find them, One ring to bring them all
and in the darkness bind them"