# Addition Ciphers ~ 1

Nowadays, most ciphers are based on numbers rather than letters. There are different reasons for this, but mainly it is done so that various arithmetic operations can be carried out on the numbers to produce a final cipher message that is 'impossible' to read without knowing the key. The word 'impossible' has to be treated with some caution because the long history of cryptology has shown that every cipher method ever devised (for practical use) has been broken eventually. But, as long as it keeps its contents secret for long enough, whether that be for weeks or years, then it will have served its purpose.

The first thing to do is to change the plain text into numbers. This is not difficult. Make **A** = 1, **B** = 2, **C** = 3, **D** = 4 and so on, up to **X** = 24, **Y** = 25 but **Z** = 0. (The reasons for this last one need not matter here.)

Since this changing from letters to numbers and back again will need to be done quite a lot, it is worth writing out the alphabet and numbering the letters. If the Cipher Wheels are available, write the numbers under the letters on the inner wheel.

Start with the plain text message

GIVE ME HELP

Put it into numbers

| G | I | V | E | M | | E | H | E | L | P |
|---|---|---|---|---|---|---|---|---|---|---|
| ↓ | ↓ | ↓ | ↓ | ↓ | | ↓ | ↓ | ↓ | ↓ | ↓ |
| 7 | 9 | 22 | 5 | 13 | | 5 | 8 | 5 | 12 | 16 |

It may look different, but the security (or lack of it) has not changed one bit. So we do some simple arithmetic on the numbers. Like add 3 to each of them to produce

10 12 25 8 16 8 11 8 15 19

A first simple test to apply to any cipher method is to look at what has happened to any letter that is repeated in the original plain text message. In this case the letter E makes three appearances. And so does the number 8 in the cipher message. That is just about useless.

So now, instead of adding the same number every time we will use different numbers. We will use a number key. Let it be the set

(3, 5, 7, 11, 2, 6)

Our working then looks like this

| Plain text | G | I | V | E | M | | E | H | E | L | P |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | ↓ | ↓ | ↓ | ↓ | ↓ | | ↓ | ↓ | ↓ | ↓ | ↓ |
| In numbers | 7 | 9 | 22 | 5 | 13 | | 5 | 8 | 5 | 12 | 16 |
| ADD key | 3 | 5 | 7 | 11 | 2 | | 6 | 3 | 5 | 7 | 11 |
| Cipher is | 10 | 14 | 29 | 16 | 15 | | 11 | 11 | 10 | 19 | 27 |

Now in the number scale we are using there are no numbers above 25 (Z = 0), and this leads to the need for this rule *'If any number is greater than 25 then we subtract 26 from it'*. (This is known as 'modulo' or 'clock' arithmetic.) Applying that rule to the last (cipher) line above leaves us with

10 14 3 16 15 11 11 10 19 1

which can be sent as numbers (1 and 3 would have to be expressed as 01 and 03 to avoid confusion) or else changed back into letters like this

J N C P O K K J S A

Notice how the three E's are now all shown differently (P, K, J). A vast improvement.

**Exercise 13**

Encipher these messages using the method outlined above.

First change the message into numbers, then ADD on the (cipher key) given. After subtracting 26, where necessary, change the numbers back into letters. Lastly write out the cipher message in groups of five.

1. SEND ME HELP (2, 8, 5, 12)
2. LOOK FOR GUN (7, 4, 8, 2, 11)
3. ATTACK FORT (13, 9, 7, 2, 10, 8)
4. WATCH FOR ME (8, 13, 15, 6, 12)
5. FLY HOME NOW (13, 10, 11, 12)
6. USE NEW CODE (10, 12, 14, 16, 18, 20)
7. SPY IS KNOWN (7, 14, 21, 2, 9, 16, 23, 4, 11, 18)
8. YOU MUST RUN (3, 7, 11, 15, 19, 23, 1, 5, 9, 13)

**Deciphering**

Having put the message into cipher by adding on a set of numbers it would be reasonable to suppose that we would recover it by subtracting those same numbers. Well we could but, when working with modulo arithmetic, subtraction is not properly defined and would create problems. Instead we still use addition, but with a different set of numbers.

Think of the 26 numbers, 0 to 25, arranged clockwise around a circle. If we add (say) 7 to any number then we can find the answer by counting forward (clockwise) from where we started. So, 5 + 7 means start at 5, count on 7 places and finish at 12. More simply 5 + 7 = 12 which works as well in ordinary arithmetic.

In reverse, 12 - 7 means start at 12 and count back 7 places to finish at 5, or 12 – 7 = 5 but, in modulo arithmetic we can get the same result by adding. Re-writing 12 – 7 as 12 + 19 we get the answer 5, remembering that we have to take off 26 when the answer goes above 25.

Do we really need this? Well consider 4 – 7. Ordinarily we would be considering the use of negative numbers, but they do not exist on our 0 to 25 circle. However, we can do 4 + 19 and get the answer 23 which is correct

What is the connection between 7 and 19? It is that 7 + 19 = 26. Or put another way, that going back 7 places is the same as going forward 19. So we have another rule

*'Instead subtracting a number we add on the value of its difference from 26'*

For example, instead of subtracting 6 we would add 20

instead of subtracting 22 we would add 4

which means that if the enciphering key was

6, 22, 7, 11, 2, 19

the deciphering key would be

20, 4, 19, 15, 24, 7

Note the totals of the two keys are

26, 26, 26, 26, 26, 26

# Addition Ciphers ~ 3

We will decipher this message

GOBET XEHNQ DEOFI

which was put into cipher with the key

(10, 14, 8, 2, 12, 9)

all of which we subtract from 26 to get the deciphering key

(16, 12, 18, 24, 14, 17)

*(Check they all add up to 26)*

No matter how it is actually done, the steps to be followed are these

| Cipher | G | O | B | E | T | X | E | H | N | Q | D | E | O | F | I |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| In numbers | 7 | 15 | 2 | 5 | 20 | 24 | 5 | 8 | 14 | 17 | 4 | 5 | 15 | 6 | 9 |
| ADD key | 16 | 12 | 18 | 24 | 14 | 17 | 16 | 12 | 18 | 24 | 14 | 17 | 16 | 12 | 18 |
| Totals | 23 | 27 | 20 | 29 | 34 | 41 | 21 | 20 | 32 | 41 | 18 | 22 | 31 | 18 | 27 |
| Take 26 ? | | 26 | | 26 | 26 | 26 | | | 26 | 26 | | | 26 | | 26 |
| Plain nos. | 23 | 1 | 20 | 3 | 8 | 15 | 21 | 20 | 6 | 15 | 18 | 22 | 5 | 18 | 1 |
| | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| In letters | W | A | T | C | H | O | U | T | F | O | R | V | E | R | A |

which is

Watch out for Vera

Notice the system for deciphering is exactly the same as for enciphering, only the key is different. Also, the key could be given in letter form. After all, WILHELMINA is a lot easier to remember than (23, 9, 12, 8, 5, 12, 13, 9, 14, 1).

## Exercise 14

Decipher these messages with the (deciphering key) given

1. IXXGC XVREM (10, 7, 16, 23)
2. FGCMA GYIXF (12, 20, 6, 17, 8)
3. UFZZW IAEUH (12, 9, 20, 15, 23, 6)
4. ZZEEE EMVNA EJZTR (13, 5, 0, 15, 4, 9, 20)

In the next four, the key given was the one used to encipher the message

5. EQUIF VUDQH (12, 9, 20, 6)
6. QMAUH WXABN (14, 5, 18, 16, 2)
7. BSLNQ BAUBC (22, 7, 13, 6, 2, 15)
8. BDFPJ HWQJP (10, 15, 5, 12, 8, 19)

Put these message into cipher using the key given

9. ATTACK FORT (8, 11, 3, 14, 2)
10. WATCH FOR ME (7, 14, 6, 20, 8, 12)