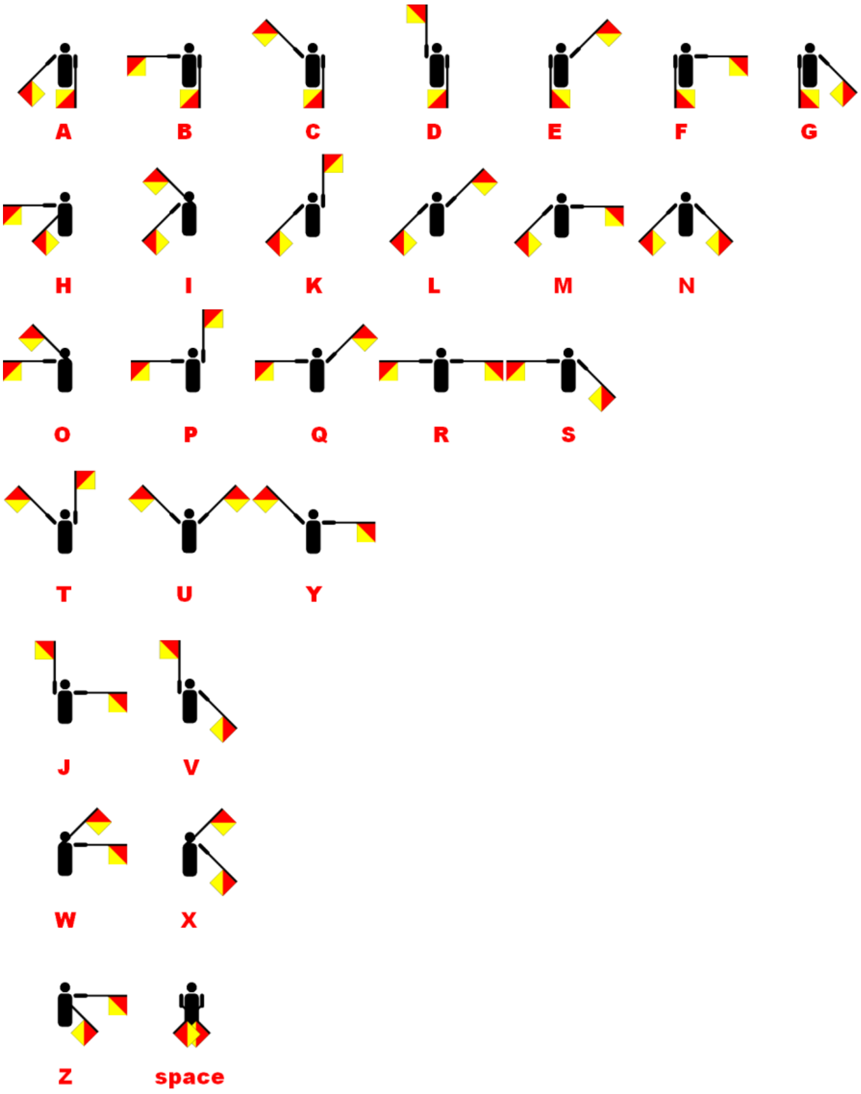
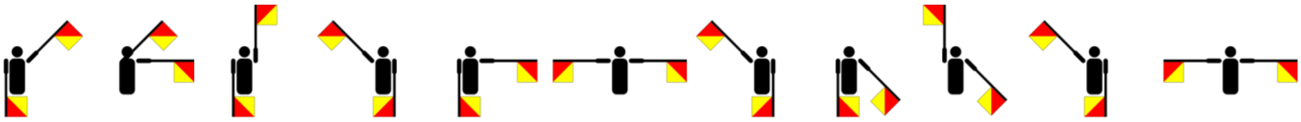
Semaphore

How the code works: This code is a way to send messages over large distances using flags:



Break this code: I was stood behind the flag waver and this is what I saw. What is the message?



Historical Footnote: Semaphore flags are used by the navy to send messages between ships. It has proved to be useful during battle, most famously at the Battle of Trafalgar during the Napoleonic Wars. The downside is there is no secrecy because everyone within visual distance can see the message.

Atbash Cipher

Below are three clues to a secret animal. Decode the messages and find the secret animal.

How the code works: Reverse the alphabet so **a** becomes **Z**, **b** becomes **Y**, **c** becomes **X**, and so on. Decode this message:

R SZEV XLOLFIUFO DRMTH

Reverse and shift: For this message, I reversed alphabet and then shifted that alphabet across so **a** becomes **M**, **b** becomes **L**, **c** becomes **K**, and so on. Decode this message:

E BECI HBYQIVU

Reverse with an unknown shift: For this message, I used a reverse alphabet with a different shift. Decode this message:

W KMAB LQ DA E CELANPWTTEN

Historical Footnote: Atbash was originally used in Hebrew. The name comes from the first and last letters in Hebrew, *aleph* and *tav*, and the second and second to last letters, *beth* and *shin*. Some Hebrew religious texts use atbash to turn words into other words. For example, in English the word '*hold*' becomes '*slow*', and '*grog*' becomes '*tilt*'.

The Atbash Cipher in Hebrew

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת

ת ש ר ק צ פ ע ס נ מ ל כ י ט ח ז ו ה ד ג ב א

Subtraction Cipher

How the code works: First, turn all the letters of your message into two-digit numbers like this:

a		b		c		d		e		f		g		h		i		j		k		l		m	
0	1	0	2	0	3	0	4	0	5	0	6	0	7	0	8	0	9	1	0	1	1	1	2	1	3

n		o		p		q		r		s		t		u		v		w		x		y		z	
1	4	1	5	1	6	1	7	1	8	1	9	2	0	2	1	2	2	2	3	2	4	2	5	2	6

For example, the word **monster** becomes

plaintext:	m		o		n		s		t		e		r	
plaintext digits:	1	3	1	5	1	4	1	9	2	0	0	5	1	8

To make a code: A random sequence of 1-digit numbers is written above the message. This is called the *key.* To make a cipher digit, *subtract* each plaintext digit from key digit above it.

cipher digit = key digit – plaintext digit

If we get any negative numbers, add 10 so all the numbers are all positive 1-digit numbers.

Example: We have written a key sequence above the digit form of the word **monster**:

key digits:	4	8	1	1	6	7	3	2	5	6	8	3	3	8
plaintext digits:	1	3	1	5	1	4	1	9	2	0	0	5	1	8
subtraction:	3	5	0	- 4	5	3	2	- 7	3	6	8	- 2	2	0
cipher digits:	3	5	0	6	5	3	2	3	3	6	8	8	2	0

So the final code is **35065323368820**.

Break this code: We have intercepted two coded messages. We don't know what either of the key sequences were, but we suspect the same key sequence was used for both messages.

We already think the first message is the word **mission.** What is the second message?

cipher one:	8	0	3	0	4	0	5	1	8	5	8	3	1	9
cipher two:	8	8	3	6	3	9	5	5	7	8	7	7	1	4

Historical Footnote: This code was used by the British Navy during World War II. Each ship would carry a book full of random digits, called a subtraction table, which they used in the method above. This code is good for hiding the frequency of letters. Eventually, the German Navy broke the British code. However, the British knew the Germans had broken their code because they had broken the German code saying that they had broken the British code!