Cryptography Worksheet — Polybius Square

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I / J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Using the grid shown, can you encipher the message:

"We escape tonight"

Explain how you did it.

Now decipher the message:

32 15 44 23 34 14 24 33 44 23 15 32 11 14 33 15 43 43

Why do you think "I" *and* "J" *are in the same square?*

Could you use a larger grid?

This is called the *Polybius Square*, since it was first described by Polybius in his "Histories" in around 150BC. It has been used by many cultures throughout history in different sizes depending on the length of the alphabet (for example the Japanese used a 7 × 7 grid). Although useful as a form of enciphering, it is not particularly strong. *Why is it not a strong cipher?*

This was not a problem for the uses that Polybius intended it for, however. He believed it to be a useful aid in *telegraphy* (which is the long-distance transmission of messages via a signalling method).
Can you think of some examples of telegraphy?

Polybius suggested that the cipher could be used by signalling the numbers using two sets of torches.
Can you think of any other ways in which the message could be sent once it has been encrypted using the Polybius Square?

What is different about this substitution cipher compared to the Mono-alphabetic Substitution Cipher?

How could we make the cipher better? That is harder to break, but still easy to use.

Using a keyword of "TOMATO"*, encipher the plaintext*: "The only way is up".

Using the same keyword, decipher: 11 31 23 25 43 23 23 35 23 54 23 22 13 12 35 44 11 23 43.

Chooses a keyword and encrypt a short message. Pass the message and the keyword to a friend, and get them to decipher it.

Teacher's Notes — Polybius Square

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I / J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

The Polybius Cipher is fairly easy to implement, and I expect that the vast majority of pupils should be able to encrypt the first message without any aid, maybe set as a starter.
The encrypted message should read:

52 15 15 43 13 11 35 15 44 34 33 24 22 23 44

The way it is written will vary, with some pupils using brackets like co-ordinates or other similar layouts. When discussing, ask why do we lay it out like this (actually the spaces would also be removed). It is because, if the ciphertext is presented in pairs then it is much easier to deduce what cipher has been used. Some pupils may have written the "coordinates" of the letters the other way round as well. Specify that it is convention that we go down first, then across (unlike actual coordinates), but that as long as the encipherer and decipherer do it the same way, either is fine.

The plaintext of the enciphered message reads: "Method in the Madness".

"I" and "J" are in the same square because we only have 25 squares, but 26 letters. You can pair up other letter (such as "X" and "Z") as long as one of them is a very uncommon letter. The convention is to use "I" and "J" for this.

A common variation of the Polybius Square is to use different sized squares. A 6 × 6 square can be used by adding the digits 0-9.

It has a long history, as outlined in the worksheet. It is not particularly strong since it has no key (that we have seen so far), and more importantly it is still a method of mono-alphabetic substitution, so is susceptible to frequency analysis. Some forms of telegraphy that the pupils might come up with are semaphore (waving different colour flags to send messages to ships in a fleet), smoke signals, etc.

There are many different ways to transmit the encrypted message: flashing lamps; blasts of sound; smoke signals; tapping. Probably the most famous example of the use of the Polybius Square was by American Prisoners of War in the Vietnam War. They tapped the enciphered message on walls and pipes to communicate with each other when they were generally kept with no human contact. In this way some just had conversations, whilst others planned escapes. It was a similar, but much simpler, way of encrypting messages to Morse Code (which could also provide a nice activity). It has also been used to aid steganography (physically hiding messages), by tying knots in rope, or stiches in a quilt.

Although this is a substitution cipher, it is different to other ones we have looked at since each letter is replaced by <u>two</u> numbers. In this way, we can represent 25 letters by only 5 symbols. This process is called *Fractionation*. This is a very powerful tool in cryptography, and although the Polybius Square itself is not that strong, using it in other ciphers increases their security.

Teacher's Notes pg 2 — Polybius Square

An easy way to make the cipher harder to break, but still easy to implement, is to add a key (after all this is always what makes a cipher more secure). Ask the pupils if they can think of any way to implement a key, and if they have no ideas, get them to think about when looking at the Mono-alphabetic Substitution Cipher. To implement a key, we simply jumble up the order of the letters in the grid. Like with the Mono-alphabetic Substitution Cipher, you can just choose the order randomly, but as we discussed then, it is hard to remember an ordered list of 26 objects. For this reason we use the same method here to create the order. We choose a keyword, and put the letters in order from the keyword first, ignoring any repeated letters. Then we add the remaining letters in alphabetical order. For example, for the keyword "SCHOOL" we get the Square shown on the right.

	1	**2**	**3**	**4**	**5**
1	S	C	H	O	L
2	A	B	D	E	F
3	G	I / J	K	M	N
4	P	Q	R	T	U
5	V	W	X	Y	Z

The square created for the keyword "TOMATO" is shown below, and the ciphertext generated is:

11 31 23 12 35 34 54 52 14 54 32 44 45 41

The plaintext for the second message is "the green eyed monster"

	1	**2**	**3**	**4**	**5**
1	T	O	M	A	B
2	C	D	E	F	G
3	H	I / J	K	L	N
4	P	Q	R	S	U
5	V	W	X	Y	Z

Cryptography Worksheet — Polybius Square Long Encryption

Choose a keyword.

Choose a paragraph to encrypt from a book.

Encrypt the passage using a Polybius Square with you chosen keyword.

Pass the encrypted passage to someone else in the class for them to decrypt.

DO NOT give them the keyword.

Teacher's Notes — Polybius Square Long Encryption

If you have done Frequency Analysis and the Polybius Square this is a nice lesson activity. You will need to get them to bring books in for the lesson.

Make sure that they are choosing passages which are long enough to perform frequency analysis on.