STEM ACTIVITY 3
TEACHER NOTES

COMMUNICATION

RAF 100
raf100schools.org.uk

EQUIPMENT REQUIRED PER PAIR OF STUDENTS:

- Power supply eg 2xD cells
- Four connecting leads
- Two long connecting leads (a series of shorter leads can be attached to make long leads)
- Two bulbs and holders
- Switch
- Split pin (or a drawing pin and cork)
- Two copies of the Scrambler Template
- Writing paper
- Two copies of STEM extension sheet (optional)

PHYSICS CURRICULUM LINKS: SERIES AND PARALLEL CIRCUITS; DIGITAL SIGNALS

STEM ACTIVITY: COMMUNICATION CIRCUITS

In this activity students design an electric circuit and investigate how it can be used to send encoded and encrypted messages.

Introduce the activity by playing the accompanying video: *Codebreakers*. Explain that during the Second World War, both sides laid hundreds of miles of electrical cables for ground-based communications. Messages could be sent quickly between the sender and receiver by using a switch to tap the message out in Morse code (dots and dashes) and kept secret by using scramblers to jumble the letters before sending the message so that only someone else who knew the scrambler settings could decrypt the message.

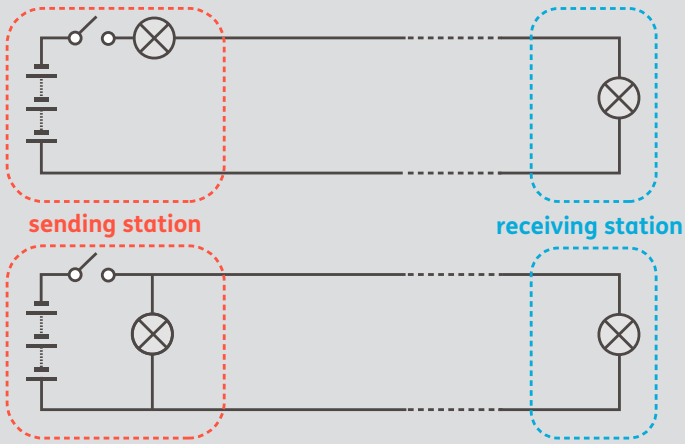
Students should follow the STEM activity instructions to design a one-way communication link (a simple electric telegraph). They should work in pairs to sketch a circuit diagram that contains two bulbs, one next to a switch at the "sender station" and one further away on long leads in another part of the room or behind a partition (eg a pile of books) at the "receiver station". Once they have set up their circuits, they should ensure that when they are sitting at their stations, they cannot see the other station's bulb (see figure 1).

Accept any series or parallel combination that works, as long as there is a sufficient number of leads available to build it.

FIGURE 1:
ONE-WAY COMMUNICATION

Circuits diagrams for one way communication

Top: A series circuit **Bottom:** A parallel circuit



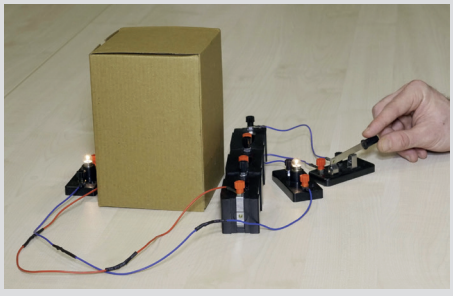


Photo: A one-way communication circuit in use

STEM ACTIVITY 3
TEACHER NOTES
COMMUNICATION

raf100schools.org.uk

Once they have completed their one-way communication link, students can test it by encoding messages using the Morse code wheel (on their Scrambler Template) and sending them to their partner by switching the circuit on and off. Explain that that they are not expected to become Morse code experts; they are simply testing their circuit and should concentrate on sending single words rather than whole messages (sending long messages can become very time consuming).

On their first attempt they are likely to encode words as a continuous stream of dots and dashes with no gaps between the letters. Let them discover the pitfalls themselves and encourage them to develop their own encoding "protocols" (eg they could simply wait for a few seconds between each letter, or transmit a very long dash to separate the letters). After sending, they should swap seats with their partner and practise receiving and decoding.

Emphasise that although converting a message into Morse Code makes it easier to send it doesn't make it secure. Both sides in the Second World War had experts in coding and decoding Morse. Secret communication requires encryption. Ask them to construct a scrambler (see figure 2) and use this to encrypt their messages before encoding and sending them.

Finally, the students are challenged to modify their circuit design so that they can send and receive secret messages without swapping seats (see figure 3).

FIGURE 2:
THE SCRAMBLER

Students can make a scrambler by cutting out the two wheels on their Scrambler Template.

They should start by setting the scrambler to **+2** and use this to finish encrypting the letters "RAF" before trying their own words and settings.

Message	R	A	F
Encrypted message	T	C	H
Encoded encrypted message	-	-•-•	••••

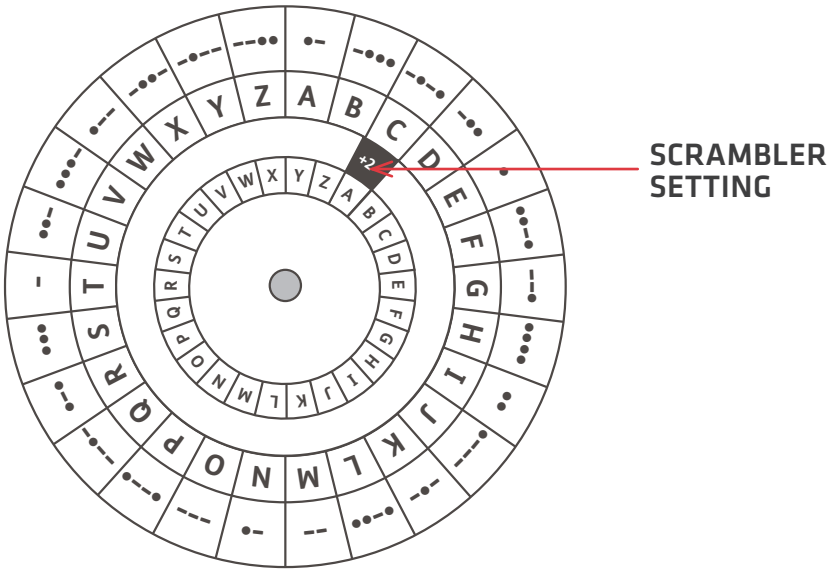
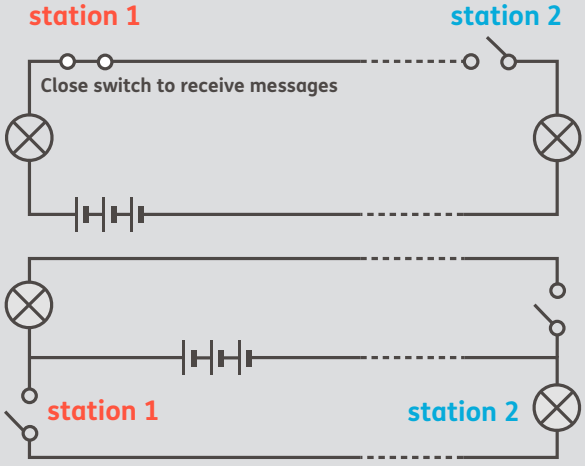


FIGURE 3:
TWO-WAY COMMUNICATION

Circuits designs for two way communication.

Top: A series circuit.

Bottom: A parallel circuit



STEM ACTIVITY 3
TEACHER NOTES
COMMUNICATION

RAF 100
raf100schools.org.uk

ABOUT ELECTRICAL SIGNALS AND CIPHERS

Depending on the students' age and aptitude, you may want to include more discussion about the advantages of using the Morse code for long distance communications and different ways of encrypting messages.

As well as being easy to encode (using a simple switch), and encrypt (one letter at a time), Morse code had the advantage that it can be sent as a digital signal (see figure 4). All signals get weaker as they travel; in ground based systems due to the electrical resistance of the cables, in wireless systems it's because radio waves diffract as they travel. On their journey from sender to receiver, they are likely to also pick up random extra signals called noise (eg crackles and hiss on analogue radio stations).

Digital encoding methods such Morse have the advantage that the noise is usually lower in amplitude than the 'on' states (the dot or dash). The signal can be more easily identified and separated than it can in an analogue signal. (Students can investigate this for themselves by putting their hand firmly over their mouth and then, at normal volume, saying a word to their partner. Then, again with their hand covering their mouth, using "bleeps" of different durations to spell out the word in Morse code; they should conclude that when the signal is weak, communicating digitally allows the message to be conveyed most clearly).

During the Second World War it was relatively easy to intercept enemy messages. Wireless communications could be picked up using a radio receiver and messages sent down electrical cables could be intercepted by monitoring the magnetic field around the cable.
The security of the message depended on the encryption technique, or cipher, used.

One of the simplest encryption techniques is a shift or Caesar cipher in which the original letters are replaced with a letter corresponding to a certain number of letters up or down in the alphabet.
There are only 25 distinct shift cipher possibilities (corresponding to setting +1 to +25 on their scrambler). This means that they are easy to break by simply trying each possibility in turn.

A more secure encryption method is to use a system in which any each letter can be represented by any other, in no particular order. These substitution ciphers can be generated by using a keyphrase.

For example to use ROYAL AIR FORCE as a keyphrase, begin by removing any spaces and repeated letters (ROYALIFCE) and then use this at the beginning of the cipher alphabet. The remainder of the cipher alphabet is the remaining letters, in the correct order, starting where the keyphrase ends (see figure 5).

FIGURE 4:
TELEPHONE VS TELEGRAPH

Messages can be sent along electrical cables by telephone or telegraph.

Left: Speaking into the telephone microphone converts the message into an analogue signal.

Right: Tapping the message out in Morse code using a telegraph switch creates a digital signal.

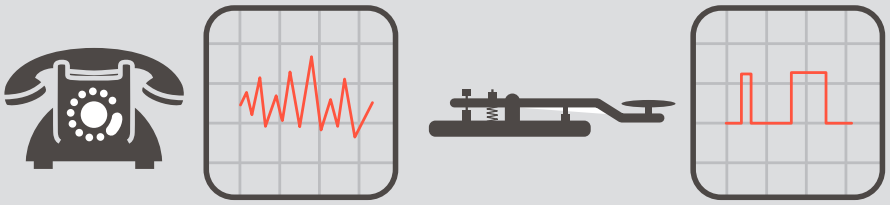


FIGURE 5: CIPHER SYSTEMS

A SHIFT CIPHER (SCRAMBLER SETTING +3)

Plain alphabet	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
Cipher alphabet	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

A SUBSTITUTION CIPHER (KEYPHRASE **ROYAL AIR FORCE)**

Plain alphabet	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
Cipher alphabet	R	O	Y	A	L	I	F	C	E	G	H	J	K	M	P	Q	S	T	U	V	W	X	Y	Z	B	D

Top: An example of a shift cipher. The letters are in an alphabetical sequence.

Bottom: An example of a more general substitution cipher. The letters are no longer in any alphabetical order.

STEM ACTIVITY 3
TEACHER NOTES
COMMUNICATION

raf100schools.org.uk

The number of possible substitution ciphers is very large (of the order of 10^{26}) making it effectively impossible for the enemy to check all possibilities. Substitution ciphers can however be broken by a technique known as frequency analysis which relies on the fact that some letters appear more often in words than others. For example, in English, E is the most common letter, followed by T and then A (see figure 6). By comparing the frequency of letters that appear in the encrypted message to those in a long piece of plaintext most of the letters can be identified.

To protect against frequency analysis both sides used machines to encrypt messages. The British used the Typex machine. The Germans used the Enigma. The core part of these cipher machines was the electromechanical rotor, which is an electronic equivalent of the students' scrambler. Each rotor was a moveable disc with jumbled wiring connected via a plugboard to a keyboard and a lampboard. If a letter was pressed on the keyboard the circuit containing the rotors caused a different letter to light up on the lampboard to indicate which cipher text to use. After each letter was encrypted the rotor moved forward one place, so that if the same letter was pressed again it was encrypted to a different one.

The obvious weakness of using a single rotor is that after 26 encryptions the encryption pattern repeats (students can see this for themselves using their scrambler). The cipher machines used during the Second World War employed multiple scramblers for extra security (see figure 7).

The starting rotor and plugboard settings were changed periodically, which meant that deciphering even the most simple message became a near impossible task for codebreakers when using pen and paper. The Germans never broke the British Typex encrytion and breaking the German Enigma required the use of the first computer.

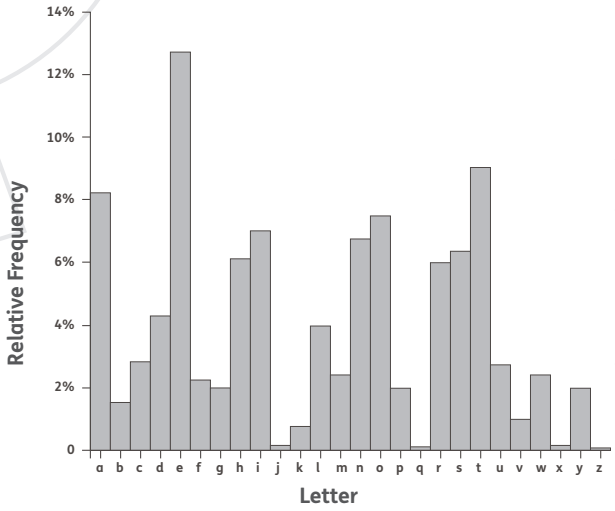


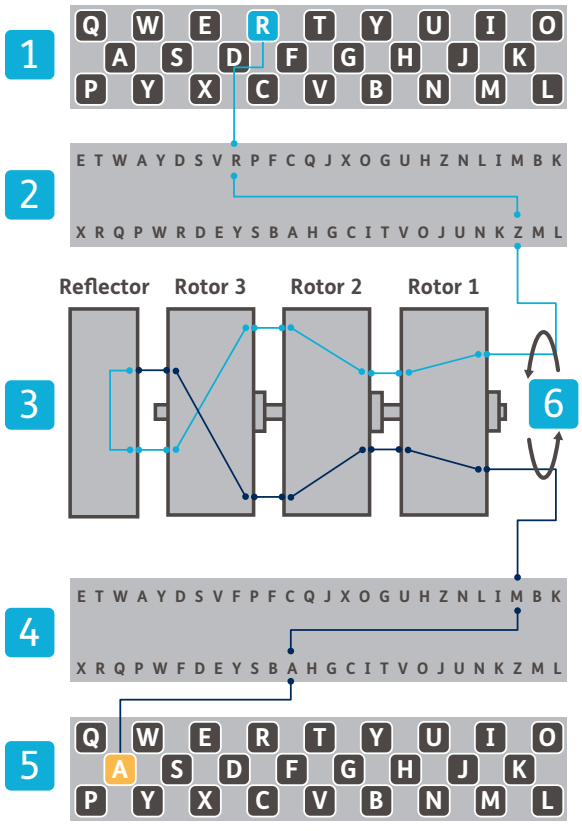
FIGURE 6:
LETTER FREQUENCY

A typical distribution of letters in English language text. Weak ciphers do not sufficiently mask the distribution, and this might be exploited by a codebreaker to decipher the message.

FIGURE 7:
ENIGMA MACHINE

The encryption process and signal path through the three rotor German Enigma machine (the British five-rotor Typex machine worked in a similar way).

1. Sender keys in letter to a standard keyboard.
2. Signal passed through plugboard which changes letters around
3. Three rotors, each wired like spaghetti, change the output letter before a reflector send the signal through the rotors again.
4. Signal makes second pass through plugboard
5. Letter to be used for encryption lights up on lampboard.
6. Rotor moves forward one setting (first rotor setting changes after each key press, second every 26 key presses and third after every 676 key presses).



STEM ACTIVITY 3
TEACHER NOTES
COMMUNICATION

raf100schools.org.uk

EXTENSION: CODE-BREAKING

As an extension activity students can investigate different ways of breaking an encrypted message.

Each student will need a copy of the STEM extension sheet and the additional writing paper. They should start by breaking the encryption for the intercepted message provided (see figure 8).

Explain that weather reports were a rich source of information for code-breakers as it allowed them to make an educated guess at some of the words. They should then choose their own scrambler setting and weather-related word and encrypt it, before swapping words with their partner and racing each other to break each other's encryption.

Students should then move onto trying frequency analysis of a shift cipher. A short encrypted message is provided; they should try breaking the encryption by identifying which letter represents E (see figure 9).

Finally they should choose a phrase and use the scramblers to encrypt it, increasing the scrambler setting by one after encrypting each letter. They should conclude that using rotating scramblers means that each letter does not map to the same letter each time and so the encryption cannot be broken by frequency analysis alone.

FIGURE 8: DECRYPTING WEATHER MESSAGES

Intercepted message	**U**	**D**	**L**	**Q**
Decrypted Message	**R**	**A**	**I**	**N**
Scrambler setting	**+3**			

Scrambler setting	**+6**			
Message	S	N	O	W
Encrypted Message	**A**	**T**	**U**	**C**

Left: The last letter (N) of the intercepted message has been worked out for them. This corresponds to a scrambler setting of +3, which they can use to decrypt the rest of the message to RAIN.

Right: Students should choose their own weather related word (eg SNOW) and encrypt it using their own secret setting (eg **+6**) before handing the message to their partner to see if they can break the encryption.

FIGURE 9: FREQUENCY ANALYSIS AND ROTATING SCRAMBLERS

Intercepted message	O	**A**	J	Z		I	**A**	Z	E	Y	W	H		O	Q	L	L	H	E	**A**	O
Decrypted Message	S	**E**	N	D		M	**E**	D	I	C	A	L		S	U	P	P	L	I	**E**	S

Message	**S**	E	N	D	-	A	I	R	-	**S**	U	P	P	O	R	T
Scrambler setting	**+2**	+3	+4	+5	-	+6	+7	+8	-	+9	+10	+11	+12	+13	+14	+15
Encrypted Message	**U**	H	R	I	-	G	P	Z	-	**B**	E	A	B	B	F	I

Top: The most frequent letters in the provided encrypted message are A and O. After some trial and error, or thought, they should realise that it is the letter A that is most likely to represent an E, corresponding to a setting of **+4** on the scrambler. So A becomes E, B becomes F, etc.

Bottom: The students should choose their own three or four letter phrase (eg SEND AIR SUPPORT) and their own starting setting (eg +2) and encrypt the message by increasing the scrambler setting by one after each letter. Unlike a normal substitution cipher, they should find that this means that each letter does not map directly to another one (in the example shown S is represented by both U and B).

MAKING THE HISTORY CONNECTION

The linked history activity is designed to show how technology was used in the past. The history activity here is about the codebreakers at Bletchley Park. For information about how to use this STEM extension activity as part of a history session see the History information, guidance notes & workshop ideas.

FURTHER INFORMATION

For more information about how scientists are now harnessing quantum mechanics for communication and encryption, see **bit.ly/RAF-Qubit.**
For more information about teaching electric circuits see Supporting Physics Teaching (11-14): **bit.ly/RAF-Circuits**.