CODEBREAKERS

INTRODUCTION

For centuries, some people, organisations and governments have wanted to send information secretly. Different ways of sending secret messages have been developed over time but the most common practice has been to hide information by using a code or a cipher (see box below).

Just as some people want to keep their messages to certain people secret, others want to know what that secret is! This has meant that just as some people will develop codes and ciphers for sending messages secretly, other people will spend their time trying to discover or break them. Sometimes the messages were sent on bits of paper and sometimes people had to remember them. Messages sent in secret could be anything from love letters to new discoveries in technology but, in war time and amongst the military, they are usually things that can actually change lives.

For governments during a war, keeping their communication secret is highly important, and these messages may include information between friendly governments, messages to army leaders giving out orders for an attack, or requests for more supplies. Trying to capture or intercept a message being sent in secret can reveal important information to another side. It could be something big, such as when a battle is planned, or it could be something that seems small, such as a shortage of bread – but it all reveals an important aspect of how a side is managing or planning.

Governments have established special organisations – intelligence agencies or ‘spies’ – to intercept messages, but if the message is encrypted, they then need people who can break that cipher. Once a cipher or code is broken, the meaning of the message can be revealed – however, the real significance of that message can only be fully understood if lots of bits of information are gathered together to create a full picture. This means that an intelligence group and a codebreaking group have to intercept, break and analyse hundreds of messages to make proper use of the information during a war.

Secret code	A method of keeping the meaning of a message hidden by changing whole words, and replacing them with other words or using a different symbol, such as images. At sea flags might be used to replace words and sentences
encoded	A message that has been put into code
cipher	Relies on hiding a message by jumbling up individual letters of the message
encryption	Sending a whole message with the letters jumbled up using a cipher
decryption	Knowing what the cipher is to unravel an encrypted message, e.g. knowing that each letter has been replaced by the one next to it in the alphabet
Caesar cipher	A method of hiding a message by mixing the letters up by simply moving each one along the alphabet, e.g. a = c, b=d, c=e, etc.
keyphrase/ keyword/crib	The way to find out how a substitution cipher has mixed up the letters; the keyword gives you the first few letters of the alphabet and then the rest can be worked out
Decipher	Unravel an encrypted message
Cryptanalyst	Someone who studies secret messages in order to gain access to encrypted information.
Intelligence analyst	Someone who has to read through all the information gathered from secret messages and from open sources to try to identify what is true and whether there are any patterns in the information, and who then has to recommend a course of action

CODEBREAKERS

Enigma machine	A machine used by the German military in the Second World War to encrypt all their messages that were sent by radio or electric telegraph
Bombe machine	A machine invented to work out how to decrypt a message that was encrypted by an Enigma machine
Y station	A place in the UK with a large aerial that listened into and wrote down the secret encrypted messages being sent by the Germans and their allies, and which then sent them to the UK intelligence sites for decryption
Lorenz machine	A machine for sending encrypted messages that was even more sophisticated than the Enigma machine

CODES & CIPHERS

In the field of secret communications (cryptography), a code refers to a way of keeping the meaning of a message hidden by changing whole words. For example, during the Second World War, the word 'DYNAMO' was used by the Allies when referring to the operation to rescue troops from Dunkirk beach. In contrast, a cipher relies on hiding a message by jumbling up individual letters of the message. For example, the word 'DUNKIRK' can be hidden by replacing each letter with the next one in the alphabet, so that once it has been encrypted it will read 'EVOLJSL'.

In both World Wars, all sides relied mostly on the use of ciphers rather than codes, as ciphers only required the sender and receiver to share a set of short instructions that could be changed easily (e.g. I've encrypted this message by shifting each letter to one up in the alphabet), rather than a large codebook that included alternatives for all the words that they may need to keep secret.

SECRET COMMUNICATIONS IN THE FIRST WORLD WAR

In the First World War, or Great War, as well as more traditional methods, such as carrier pigeon, millions of messages were sent using the modern technology of radio broadcasts and electric telegraph. Radio waves and electric circuits were used because messages could be sent over long distances in a matter of seconds, unlike someone sending a paper message. However, anyone could quite easily listen in to radio messages or intercept telegraph communications and understand what the message was. This is why governments started to encrypt their messages. The encryption technique (cipher) had to be agreed in advance so that the person receiving the message could decipher it and understand what they were being sent.

The simplest form of encryption is to use 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 the alphabet. There are, however, only 25 distinct shift cipher possibilities, which makes them easy to break by simply trying each possibility in turn. A better encryption method is to use a system in which any letter can be represented by any other, in no particular order. These substitution ciphers can be generated by using a keyphrase. For example, if using 'Royal Air Force' as a keyphrase, begin by removing any spaces and repeated letters (ROYALIFCE) and then use this at the beginning of the alphabet. The remainder of the cipher alphabet is the remaining letters, in the correct order, starting where the keyphrase ends.

If someone does not have the keyphrase then trying to work out the cipher can be extremely time-consuming, as there are many billions of possibilities. How people set about breaking a cipher like this is to use frequency analysis. All languages use some letters more than others; in English, for example, the letter E is the most common letter, followed by T and then A. By comparing the frequency of letters that appear in the encrypted message to those in a long piece of plain text, most of the letters can be identified. A keyword/keyphrase is also called a 'crib'.

CODEBREAKERS

THE GOVERNMENT CODE AND CIPHER SCHOOL

**In 1909, the British government created the Secret Intelligence Service (or Bureau as it was known for a while). SIS was engaged in all areas of intelligence-gathering, codebreaking and analysis of information.
In addition, during the First World War, the Army and the Navy both had their own intelligence units that intercepted and decrypted messages. After the war, Hugh Sinclair, the Director of Naval Intelligence, was given the task of merging the Army and Navy units and creating the Government Code and Cipher School. Sinclair also became the head of SIS. All these intelligence units were based in London.**

During the 1920s and 1930s, the staff at GC&CS grew, and they became aware that new methods of encrypting messages were emerging. Recruitment of codebreakers had usually focused on linguists: those who were good at languages (especially as many intercepted messages, once decrypted, would still be written in a foreign language).

However, technological changes in that period meant that messages that were being sent seemed to have far more complex ciphers than the ones people were used to – it was obvious that some type of machine was also involved to create a cipher. Sinclair decided to start recruiting mathematicians as well as linguists to his team.

In 1938, events across Europe made war look likely again. Sinclair decided that having all his important people in London might be dangerous, as London was likely to be attacked from the air in any war, just as it had been during the First World War. So the government secretly bought or took over (requisitioned) a number of country houses in the Home Counties around London. One of the key purchases was Bletchley Park in the village of Bletchley, Buckinghamshire, just outside London. The site was ideal as it had plenty of space and was very close to a train station from which trains travelled straight into London. The whole of GC&CS was transferred to Bletchley in 1938 under the leadership of Alastair Denniston.

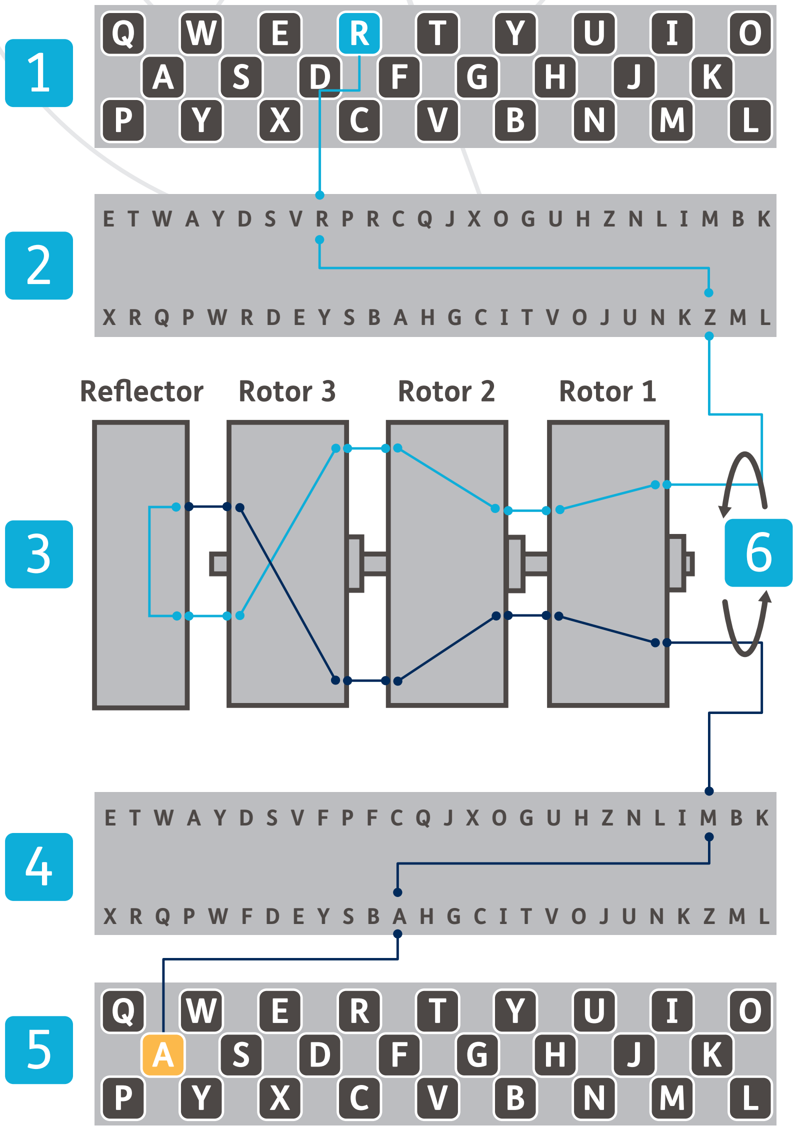
THE ENIGMA MACHINE AND BREAKING ENIGMA

The Enigma machine was invented by a German engineer, Arthur Scherbius, shortly after the First World War.

The machine (of which a number of varying types were produced) resembled a typewriter. It had a lamp board above the keys, with a lamp for each letter. The operator pressed the key for the plaintext letter of the message and the enciphered letter lit up on the lamp board. It was adopted by the German armed forces between 1926 and 1935. The machine contained a series of interchangeable rotors, which rotated every time a key was pressed to keep the cipher changing continuously. This was combined with a plug board on the front of the machine, where pairs of letters were transposed. These two systems combined offered 159 million million million possible settings to choose from, which the Germans believed made Enigma unbreakable.

The Poles had broken Enigma as early as 1932, but in 1939, with the prospect of war, the Poles decided to inform the British of their successes. Dilly Knox, one of the former British First World War codebreakers, was convinced he could break the system, and set up an Enigma Research Section, comprising himself and Tony Kendrick, and later joined by Peter Twinn, Alan Turing and Gordon Welchman. They worked in the stable yard at Bletchley Park, and this is where the first wartime Enigma messages were broken in January 1940. Enigma traffic continued to be broken routinely at Bletchley Park for the remainder of the war.

Extract Taken from the Bletchley Park Trust


1
Q W E R T Y U I O
A S D F G H J K
P Y X C V B N M L
2
E T W A Y D S V R P R C Q J X O G U H Z N L I M B K
X R Q P W R D E Y S B A H G C I T V O J U N K Z M L
Reflector
Rotor 3
Rotor 2
Rotor 1
3
6
4
E T W A Y D S V F P F C Q J X O G U H Z N L I M B K
X R Q P W F D E Y S B A H G C I T V O J U N K Z M L
5
Q W E R T Y U I O
A S D F G H J K
P Y X C V B N M L

THE ENIGMA MACHINE

The encryption process and signal path through an Enigma machine.

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 use for encryption lights up on lamp-board.
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).

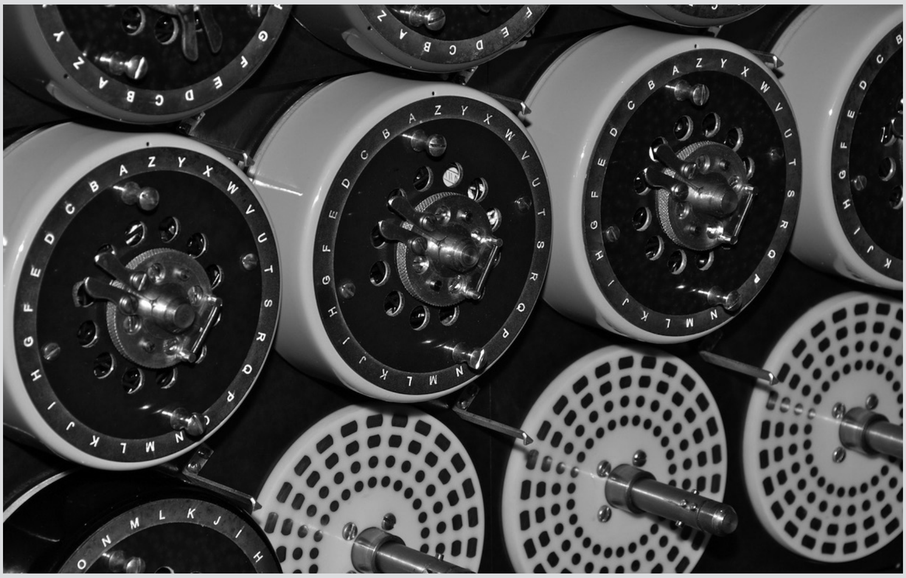
The problem for the team at Bletchley was that they needed to break the hundreds of Enigma messages that were coming in each say quickly. That led to the building of the Bombe machine.

TURING-WELCHMAN BOMBE

Based on the information presented by the Poles, British mathematician Alan Turing developed a machine that was capable of recovering the key settings. The machine was called Bombe (later Turing-Welchman Bombe) and was built by the British Tabulating Machine Company (BTM) in Letchworth, Hertfordshire (UK) under the supervision of Harold (Doc) Keen.

The name was derived from Bomba, a similar machine developed by the Poles shortly before the outbreak of the Second World War.

Turing designed the British Bombe in 1939. Compared to the Polish Bomba, it used a completely different approach. It was based on the assumption that a known a crib was present at a certain position in the message. The first machine, called 'Victory', was delivered at Bletchley Park on 18 March 1940.



The Bombe was further enhanced with the so-called diagonal board, an invention by fellow codebreaker Gordon Welchman, which greatly reduced the number of steps needed for the codebreaking effort. A second Bombe, with Welchman's diagonal board present, was installed on 8 August 1940. It was named 'Agnus Dei', later shortened to 'Agnes' or 'Aggie'. The first machine (Victory) was later modified with a diagonal board as well.

During the course of the war, over 200 Turing-Welchman Bombes were built. To avoid the risk of losing them in case of a bomb attack, they were spread between Bletchley Park and its so-called outstations in Wavendon, Adstock, Gayhurst, Eastcote and Stanmore, where they were operated by WRNS, RAF-technicians and civilian personnel.

Extract taken from the Crypto Museum www.cryptomuseum.com/crypto/bombe/

Therefore, the Bombe's job was to try to find the crib in the message. Once the crib was discovered, it was possible to limit how many settings it could possibly be on the Enigma machine, to try to decrypt the whole message.

The crib was usually at the start of a message and it helped to indicate to the receiver that they were using the correct settings on their machine.

Cipher books: The German military were issued with cipher books, which told them what setting to use on their machine on a certain day. The books were changed weekly, except for those parts of the military that could not receive new cipher books easily. Submarines would use their cipher books for weeks, as they were often underwater for long periods of time. Capturing cipher books was extremely useful, as they provided the crib for a certain day and for a certain set of communications – e.g. all Luftwaffe communiqués on 2 November 1943. If the codebreakers had the crib, they could set their Enigma machine at the correct settings and they would not need the Bombe team to do its job – which could take hours.

CODEBREAKERS

FROM Y STATION TO ACTION

All across the UK were bases called 'Y' stations. The 'Y' name came from the shape of the aerial, and this was what made it significant. A Y station would be listening in to the many radio messages that were sent out across the airways. Some listened to actual voice messages but the majority were there to pick up the encrypted messages being sent between armies and commanders, government departments, etc. Y station staff (military) would collect hundreds of messages a day, which would then be passed on to places such as Bletchley Park, either on paper and delivered by a motorcycle rider or by using a teleprinter machine – a type of electronic printer that printed out a message that had been sent electronically or down a telephone cable.

At Bletchley: the encrypted message would be given to one of the codebreaking team. They would work with the Bombe machine operators to try to find a breakthrough to the cipher – the crib that would help provide the settings for an Enigma machine. If the Bombe hit upon a match and the cipher could be converted into a message, it was then handed to the translators. The translators would be attached to a military or intelligence unit. The Bombe machines were usually operated by the WRNS (Women's Royal Naval Service). The RAF team were largely based in Huts 3 and 6, which also contained some of the analysis teams.

Analysis: The decrypted, translated messages would be analysed and compared to other intelligence information. Some of this information came from encrypted messages at Bletchley Park, but other material came from further afield and from other intelligence sources. The RAF had a site at Medmenham, which was its centre for a photographic interpretation unit. All of the reconnaissance and aerial photography that was taken by the RAF on operations was examined there. Information revealed at Bletchley could be passed to Medmenham, who might compare discussions of troop movement to the photographs that they had taken.

Alternatively, the analysis might be taken into central London to be compared with other information being gathered by the SIS and its international network of spies.

Action: The analysis of the information provided by decrypted messages could affect military decision-making or planning. Sometimes this effect might be immediate, e.g. extra aircraft moved to a certain part of the UK in anticipation of an attack. Sometimes the result of the information might be to affect British military planning over a long period of time, e.g. how an attack for months ahead should be planned and for what date, according to what the German were planning. Sometimes the information gathered resulted in no immediate action, e.g. during the run-up to D-Day, the Allied invasion of Normandy, the decrypted messages and wider intelligence-gathering helped to support the British belief that the Germans did not know that the attack was being planned for Normandy. On other occasions, decisions to not do anything after messages were decrypted were taken so that the Germans did not suspect that the Enigma messages could be decrypted – this could often be a controversial decision, as it might mean that British lives would be lost rather than acting on intelligence.

Timeframes: Trying to break the German messages sent by Enigma machines was always a race against time. There was no point in finally being able to understand a message if what it was talking about had happened days or weeks before. Therefore, trying to decrypt a message and reveal its meaning was always done with a sense of urgency, ideally within a few hours of the message arriving at Bletchley.

CODEBREAKERS

WHO WORKED AT BLETCHLEY PARK?

When Bletchley was first established in 1938, only a few hundred people were based there, but this number grew as time went on. By January 1945, 10,000 people worked at Bletchley, three quarters of whom were women. The whole place operated on a shift pattern so that it was able to operate 24 hours a day. The people there, including the women, worked as mathematicians, codebreakers, language translators (to translate the message once it was broken), analysis, administration and machine operators.

THE ROLE OF INTELLIGENCE DURING THE WAR

https://bletchleypark.org.uk/cms/2017/01/0110_colossus-10-with-attending-Wren

When people think of conflicts and war, they usually think of armies going off to fight, and although gaining information (intelligence) has always been important, it wasn't always perceived as being as important as the actual fighting. However, the Second World War changed that. The Nazis' dominance in Europe, coupled with the rise in technology, meant that wars could also be waged through other means – propaganda, strategic planning, deception and by knowing what your enemy was doing so that you could manipulate them or counter them. The RAF flew thousands of reconnaissance missions in addition to its role in combat. Hundreds of men and women acted as intelligence agents across Europe, collecting information and sending it back to the UK. At home in Britain, thousands of men and women served the military as codebreakers, analysts and strategists for deception.

During the planning for D-Day and the invasion of Western Europe, the Allies used their intelligence-gathering to understand where German troops were, how defences were organised and how quickly they could be reinforced. In addition to preparations for the invasion, the Allies spent months sending out false information to convince the Germans that an attack would start at other sites along the French coast or even in Norway. From the intercepted messages that the British decrypted, they were also able to ascertain that the Germans did not expect Normandy to be the invasion zone and that they were convinced it would be in Calais. Knowing that the Germans were not prepared provided the Allies with a massive advantage when they did successfully attack on 6 June 1944. It is said that the use of intelligence to deceive, as well as to listen in, helped to end the war more quickly than just through fighting.

CODEBREAKERS

USING THIS INFORMATION

This historical information can be combined with the introductory film and resources from the resource section for exploring some creative ideas in a school club/informal club, or for a more curriculum-based lesson.

Also attached here is the PDF for teachers on communication technology – this will help you to understand the technology that underpins the following history and STEM exercises.

Below are the ideas and questions that these materials could support.

In addition to the historical information above, case studies and extra information are available in the resource section. These include biographies and technology case studies.

QUESTIONS FOR EXPLORATION IN ANY SETTING:

Why do secret messages and codebreaking play an important role during a war?

Why was being able to understand the encrypted messages of the Nazis and their allies important during the Second World War?

HOW TO USE THIS MATERIAL IN A HISTORY CLUB OR LUNCHTIME/ AFTER-SCHOOL/INFORMAL CLUB

These ideas are suitable for a mixture of age groups and abilities. They can also be used with the interactive map to begin a local history investigation.

START BY SHOWING THE ACCOMPANYING FILM: *CODEBREAKERS*

Provide the historical information or read it to students, and select one or both of the questions from the list above that you think the group might find interesting. (You may want to use the additional questions in the box to stimulate ideas.)

Ask the group to create or devise their own substitution or shift cipher and then use it to encrypt messages. You could also use the activity explored in the lesson below (c) for ages 11–13 years.

Select some of the case studies/biographies from the resource section. Ask the young people to answer the question(s) and present their discoveries as:

- An information poster about Bletchley Park – written in code.
- A newspaper story for their school/group newsletter on the role of Bletchley Park during the war.
- A display for the school/class/group noticeboard about the different people and groups that contributed to codebreaking.
- A comic script or graphic showing all the stages of intercepting, decrypting and analysing a message – and then how that information can be used.
- An assembly presentation or talk for other members of your group on the importance of using technology in a war situation.

Extension: Try to carry out the STEM activity 3 extension – link

Now use this information to start investigating the local history of an airbase near you – this can begin by using the interactive map. Over the course of the last century, there have been over 1,500 air bases or places used by the RAF; even if you don't live near to one now, there will have been one at some time.

Find out about the base. Identify what other information or understanding of an historical period is needed to tell the story of that base.

CODEBREAKERS

LESSONS IN SUPPORT OF THE CURRICULUM AND/OR EXAMINATIONS

RAF 100

raf100schools.org.uk

GUIDANCE ON HOW THIS MATERIAL *COULD* BE USED IN A LESSON ABOUT:

1. The Second World War
2. The Technology of Warfare

The questions in the box can also be used to explore this theme and the materials.

1. THE SECOND WORLD WAR

Ages 11–14

Example question:

Why did the codebreakers need to develop new technology to break German military codes during the Second World War?

a) Show the students the accompanying film: *Codebreakers*

b) Allow them access to the historical information and to the biographies and case studies in the resources section.

c) Explain to students working in groups that they will be trying to send each other secret messages and that you will be trying to break them. Introduce substitution ciphers and provide an example generated using a keyphrase (e.g. the ROYAL AIR FORCE example on page X). Split each group into two and ask them to create their own substitution cipher and to write down a short message and then use the cipher to encrypt their message. Tell them they have 15 minutes to complete both parts of the activity.

Ask the groups to swap examples of the encrypted messages (but not ciphers). Ask them to keep the message secret from you, but only pass on one piece of information – the letter that appears most often in the message (there may be more than one).

Ask groups to now swap ciphers. They all have ten minutes to decrypt the message.

Explain that you are going to try to break their cipher. Predict that the letter they have identified is (most likely to be) E. How did you do? Explain frequency analysis, and why you maximised your chances of being correct by choosing the letter E.

There will be a raid at midday London time on the dockyards of Southampton.
The keyword is Wintersun.

Show them the diagram of how Enigma worked.

d) From their own experience of creating and breaking codes, ask the students how the Enigma machines helped the Germans and how they caused a problem for the British and their Allies.

Ask the pupils to create a diagram of the process of creating a cipher and encrypting a message, and then the process of it being intercepted, decrypted and its contents used. Ask them to describe each stage and what the challenges are at that stage.

Ask the students to discuss how technology affected communication during the Second World War, using examples and experiences that they have just tested.

Now ask the students to answer the question: Why did the codebreakers need to develop new technology to break German military codes during the Second World War?

2. THE TECHNOLOGY OF WARFARE

Ages 11–16

Example question:

What do the activities carried out at Bletchley Park demonstrate about the role of the mathematics team and the codebreakers in the fighting during the Second World War?

a) Show the film.

b) Provide each student with a copy of the STEM extension worksheet and scrambler template (see below).

If you are running RAF100 activities with a science teacher and the students have already completed the STEM activity, or you do not feel confident doing the STEM activity, then use the activity in c) in the above lesson model.

c) Following on from the activity, and using the historical information and content from the film, ask the students to create a mind map/spider diagram of the role of secret communication during war, distinguishing between codes and ciphers.

d) Ask the students to present an argument supporting or dismissing the importance of those working at Bletchley Park during the Second World War.

Conclude: How important was technology to decision-making during the War?

Extension: Find out about how ciphers are sent today.

CODEBREAKERS

THE STEM ACTIVITY

Each student will need a copy of the STEM 3 Extension sheet and scrambler template and a split pin (or drawing pin with a cork). To build the scrambler, students should cut out the **two wheels on the Scrambler Template and connect them by putting the pin through their centres see diagram below…**

They should start by breaking the encryption for the intercepted message provided (see figure below).

Explain that weather reports were a rich source of information for codebreakers, as they allowed them to make an educated guess at some of the words. Students 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 the other's encryption.

Students should then move on to 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 below).

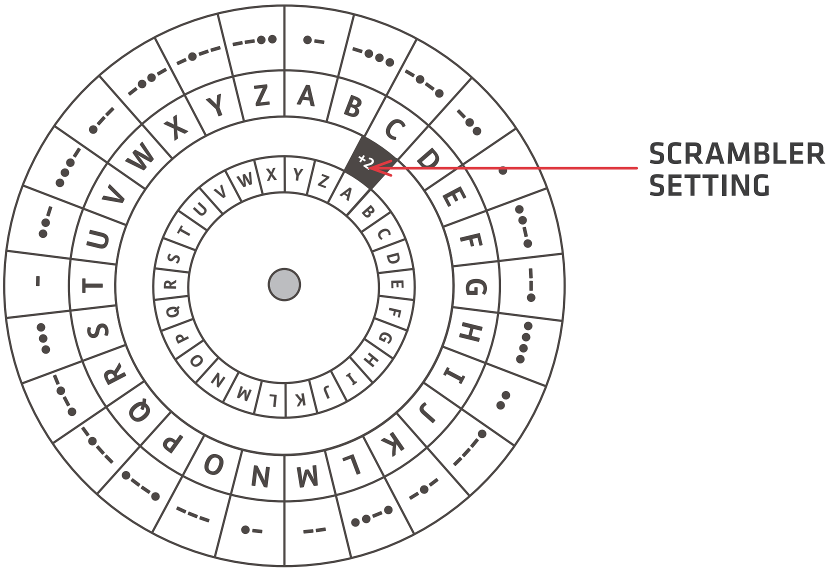
Finally, they should choose a phrase and use the scramblers to encrypt it; increasing the scrambler setting by one after encrypting each letter. They should conclude that using rotating scramblers means that each letter does not map to the same letter each time (and so the encryption cannot be broken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

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	-	-•-•	••••



CODEBREAKERS

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.

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).

ADDITIONAL QUESTIONS TO SUPPORT LEARNING FOR ALL GROUPS

- Why were so many women employed at Bletchley Park?
- Why does some information need better protection than others?
- Who are the key scientists/ mathematicians who worked at Bletchley Park?
- Why is the analysis of many pieces of information needed before a decision is made for action?
- What roles did the RAF and the WRAF carry out at Bletchley Park and in intelligence-gathering elsewhere?

MAKING THE STEM CONNECTION

The associated STEM activity is designed to show an aspect of technology that demonstrates some of the thinking in the past. The STEM activity here involves designing and building a communication circuit. Team up with a science teacher to help students explore how secret messages can be sent as electrical signals.