

Code-breakers

A code replaces words with letters or symbols. A cipher is a form of code that adds or substitutes letters to disguise it. Both sides used codes and ciphers for messages during the war. Some Allied cryptographers (code-breakers) cracked the Axis codes, revealing valuable information that gave the Allies considerable advantage over their enemies.

Rotor cylinder carries three (later four) alphabetical rotors

Alphabetical keyboard shows clear encoded letter

Plugboard settings are changed daily

Alan Turing

Mathematician Alan Turing was one of the brilliant people working for British intelligence during the war. He played a key role in deciphering the German Enigma.

Early computers

Scientists and cryptographers at Bletchley Park (the British code-breaking centre) developed the "bombe" to decipher German Enigma messages. As Enigma grew more complex, they built Colossus, a forerunner of modern electronic computers.

The German Enigma cipher

The Enigma was the main cipher machine in use during World War II. It enciphered each letter with alphabetical rotors, placed on a cylinder in a predetermined order, and a set of plugs in a plugboard. The settings varied each day, giving millions of possible combinations.

An inside ring

Everyday objects were used to hide microdots – tiny photographs of a coded message that can be read only with a magnifying viewer.

Secret chamber

Screw top

Boris Hagelin

The converted

In the 1930s Swedish cryptographer Boris Hagelin invented the Converter M-209. It was the main cipher machine used by the US Army during the war.

Fact to fiction

Some code-breakers and spies turned their experiences into fiction, such as Ian Fleming, who worked for British Naval Intelligence.

Ian Fleming, creator of the fictional spy James Bond

Reading aperture

Top cover in open position

Switching unit

Compartment for stepping switches

Stepping switch

Purple cipher

The Japanese Purple machine used a plugboard and telephone switches to create a complex cipher device. US intelligence cracked Purple's code in September 1940 and built a replica.

Pearl Harbor following the Japanese attack

Cryptonic discs

Spring motor

Indicating discs

Kryha cipher

The Kryha, invented in 1924, used a spring-driven alphabetic rotor to substitute each letter with a different one every time the letter was used in a word. The Germans used the Kryha in the war, not realizing that the US had already broken its code.

Ignored information

Communications from the Japanese Purple machine, detailing an attack on the US in late 1941, were decoded by the US, but the Pearl Harbor target was not clear until it was too late. Code-breaking in 1942 enabled the US to defeat the Japanese navy at Midway.

30

31

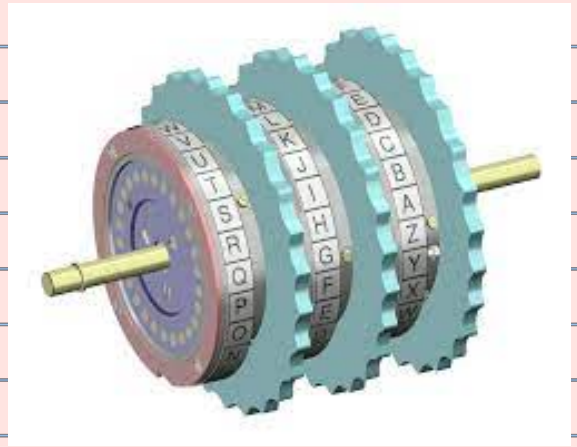
Reading

Strategy

- Look at each part of the word.
- Look at the pre-fix/suffix of the word. Does this tell us anything?
- Read the full sentence again. Is the word used as a noun, verb or an adjective?
- Is the word similar to another word you are familiar with?

Glossary

code-breakers
symbols
substitute
Allied
Axis
deciphering
forerunner
predetermined
combination
rotor
plugboard





Glossary

code-breaker - a person who solves a code or codes.

symbols - a drawing, shape, or object that represents an idea, object, or amount of something

substitute - to put in the place of another

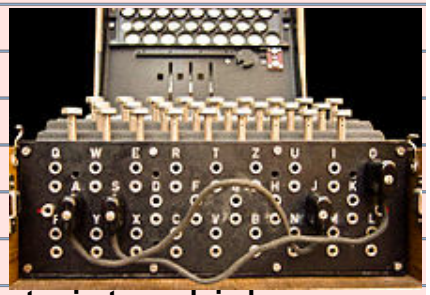
Allied- In WW2, Great Britain, France, and the United States.

Axis - In WW2, Germany, Italy, and Japan

deciphering - translate from code, or more generally, figure out

forerunner - a person or thing that came before another

combinations - various ways in which a group of letters, numbers and/or symbols can be ordered.



rotor- the part of an electrical machine that turns

predetermined - to decide in advance

plugboard- a device with a large number of sockets into which electrical plugs can be inserted to form many different temporary circuits

LO: To find information in the text to answer questions.

you do

1. What is a code?
2. What is a cipher?
3. Who used codes and ciphers in the war? What were they used for?
4. What is a cryptographer?
5. What was the Enigma?
6. Who played a key role in deciphering the German Enigma?
7. What was developed to decipher the German Enigma messages?
8. What were hidden in everyday objects?
9. What was the Converter M-209? Who invented it?
10. How did the Japanese Purple machine work?
11. In 1942, what did code-breaking enable the US to do?
12. Why was it a mistake for the Germans to use the Kryha in the war?

LO: To find information in the text to answer questions.

you do

1st read: Read the text

we do

Read the text with your partner - take it in turns to read a sentence/ section each.

Find the information in the text to answer the questions.

LO: To find information in the text to answer questions.

we do

1. What is a code? **replaces words with letters or symbols**
2. What is a cipher? **a form of code that adds or substitutes letters to disguise it**
3. Who used codes and ciphers in the war? What were they used for? **Both sides (Allied and Axis) for messages**
4. What is a cryptographer? **a code-breaker**
5. What was the Enigma? **the main cipher machine in use during WW2**
6. Who played a key role in deciphering the German Enigma? **Alan Turing**
7. What was developed to decipher the German Enigma messages? **the 'bombe' and Colossus**
8. What were hidden in everyday objects? **microdots**
9. What was the Converter M-209? Who invented it? **main cipher machine used by the US Army, Boris Hagelin**
10. How did the Japanese Purple machine work? **used a plugboard and telephone switches to create a complex cipher device**
11. In 1942, what did code-breaking enable the US to do? **defeat the Japanese navy at Midway**
12. Why was it a mistake for the Germans to use the Kryha in the war? **the US had already broken its code**