Communicating in Code: Technology in World War I

At the beginning of the 20th century, a new invention - wireless telegraphy, the transmission of *telegraph* signals by *radio* - made communication easier than ever before. It allowed governments to communicate with warships at sea and with armies in the field. But intercepting wireless communication was very easy, so new codes and ciphers were used to disguise messages.

This resource explores the use of cryptology and coding in World War I and in today's society. It encourages pupils to use some simple substitution ciphers to break and create messages.

The resource is designed to develop communication, numeracy and critical thinking skills through STEM-based and creative learning.

Set the Scene

During WWI, both ciphers and codes were used extensively. On the Western Front, field armies used trench codes to communicate between lines. Codebooks were distributed to military personnel, but this proved to be a security liability since they could be stolen by enemy forces. Trench raiding parties would try to sneak into enemy lines and snatch codebooks, which meant codes had to be changed frequently.

The British Navy also used codes, as it was much easier to distribute and protect code books for naval vessels than for armies on the move.

At the outbreak of the war, Britain had no formal code-breaking operation. In October 1914, the Dundee-born Sir James Alfred Ewing, the Admiralty's Director of Naval Education, formed a group of code-breakers called Room 40. It existed mainly to decrypt intercepted German naval messages. Room 40 was legendary for its successes, particularly intercepting the Zimmermann Telegram that triggered the United States' entry to the war. German efforts at code-making and -breaking during World War I are somewhat obscure, mostly because many official records were destroyed during World War II. They did have a signals intercept system in operation before the end of 1914 and were also able to crack Royal Navy ciphers - giving German U-boats an advantage in their attacks on Allied ships.

The art of writing and solving ciphers and codes is called cryptography.

Both codes and ciphers convert legible messages into series of symbols that can only be understood by certain recipients. A code does this by substituting code groups (groups of either letters or numbers) for components of the original message. For example, President = Eagle or Tank = 4036. To understand the code, the sender and recipient must have a code book. A code book lists all the code grips along with their assigned meanings.

Ciphers use a system of fixed rules (an algorithm) to transform a legible message (plaintext) into an apparently random string of characters (ciphertext). The algorithms are performed on individual letters or small groups of letters. For example, a cipher might be defined by this rule: 'For every letter of plaintext, substitute a two-digit number specifying the plaintext letter's position in the alphabet plus a constant between 1 and 73 that shall be agreed upon in advance.' Incorporation of a variable term into a fixed algorithm is typical of real-world ciphers. The variable component is called a key.

Ciphers are the corner stone of cryptography today. Unlike code, which is limited to messages that can be expressed using the terms defined in the codebook, ciphers can transmit all possible messages. Rather than replacing a code book that has been captured, the key–algorithm concept makes cipher secrecy dependent on small units of information (keys) that can be easily altered. Modern cryptography relies almost entirely on ciphers implemented by digital computers. All communication technologies, including the *internet*, *mobile phones*, *digital television* and *ATMs* rely on ciphers in order to maintain both security and privacy. Ciphers are widely employed by industry, diplomacy, espionage, warfare and for personal use.

Second and Third Level

Tasks

1. Substitution ciphers have a long history of use. The Roman Emperor Julius Caesar used a substitution cipher, for example. The key to his cipher was to substitute each letter of the alphabet with one three letters ahead, so A with D, B with E and so on. This is called a key.   There are other variations of this cipher and, depending on what key you use, you will get a different message.

   Can the pupils crack this key? We will be using it to decipher messages in step 3.   If the word BIRD would be encrypted UBKW, what is the key?

2. The key is a substitution of each letter with a letter 19 places ahead on the alphabet. Give each pupil a copy of the cipher wheel (Activity Sheet 1). They will need to cut it out and clip it together in the middle. It works by matching A on the inner wheel to the appropriate shift letter on the outer wheel - so A would be lined up with T.   The wheel is a early machine that makes it easy to encrypt and decipher messages.   Ask the pupils to work in pairs to decipher one or more of the messages on Activity Sheet 2 using the wheel.

3. Ask the pupils as a class how secure they think the cipher is. Do they think an enemy code breaker without the key would easily be able to decipher the messages if they were intercepted? Can they think of way to make it more secure?

Curriculum Experiences & Outcomes

Second Level

Having explored more complex number sequences, including well-known named number patterns, I can explain the rule used to generate the sequence, and apply it to extend the pattern. **MTH 2-13a**

Third Level

Having explored number sequences, I can establish the set of numbers generated by a given rule and determine a rule for a given sequence, expressing it using appropriate notation. **MTH 3-13a**

Core Skills

- Thinking
- Communication
- Numeracy

Approaches & Methods

- STEM-based learning
- Creative learning

Materials & Resources

Communicating in Code Activity Sheet 1	Code wheel template
Communicating in Code Activity Sheet 2	Secret messages