STEM 3: COMMUNICATION
EXTENSION

CODE-BREAKING

raf100schools.org.uk

In this activity, you will explore different ways of breaking an encrypted message.

WHAT YOU SHOULD DO

1. Part of an intercepted message is shown below. One letter has been decrypted for you.

   Can you work out the scrambler setting and finish the decryption?

Intercepted message	**U**	**D**	**L**	**Q**
Decrypted Message				**N**

2. Write another word that can be used to describe the weather. Choose your own scrambler setting and encrypt your word.

   Swap encrypted messages with your partner. Who can break the encryption first? (Use your scrambler to help). Once you think you know the setting, check if you are correct with your partner.

3. As well as looking for common words (eg in a weather report) code-breakers also look at how often certain letters occur.

   The letter E is the most commonly used letter in the English language. Below is an intercepted message. Decide which letter must represent E, and work out what the scrambler setting is to decrypt the message (spaces in between the words are indicated by a dash).

4. During the Second World War, both sides used machines that had rotating scramblers (rotors) to encrypt their messages.

(a) Choose your own three or four word phrase. Don't tell your partner.

(b) Set your scrambler to your chosen setting and encrypt the first letter (make a note of the setting).

(c) Move the scrambler forward one setting. Encrypt the second letter using this new setting.

(d) Move the scrambler forward again by one setting. Use this to encrypt the third letter. Repeat until the whole message is encrypted.

5. Compare your original phrase to the encrypted one. Can you explain why using rotating scramblers make communications more secure?

6. Pass your encrypted message to your partner. Only tell them the starting position of your scrambler. Can they decrypt the message?

Intercepted message	**O**	**A**	**J**	**Z**	**-**	**I**	**A**	**Z**	**E**	**Y**	**W**	**H**	**-**	**O**	**Q**	**L**	**L**	**H**	**E**	**A**	**O**
Decrypted Message																					