KNOWLEDGE NUGGET: DAY 4 - SECRETS	
Topic	Cryptography

Learning objectives	Success criteria
Students will… • be introduced to cryptography and the popular Caesar (substitution) cipher • see a simple overview of how the Enigma machine works • be shown how encryption keys are used in the modern world Advanced Encryption Standard (AES) • be shown how CyberChef can be used to help encrypt or decrypt ciphers • take part in a cryptography challenge	- Watching and understanding the video in its entirety. - Participating in the cryptography challenge.
Resources	**Suggested use of teaching time**
- Knowledge Nugget Video - Enigma challenge worksheet	Video – 10 minutes Cryptography Challenge – 10 Minutes (introduced as part of the video)

Learning activity

The video will talk through the basics of cryptography from the Caesar cipher to how the Enigma machine was used during WWII, then discuss how encryption is still relevant to the modern world.

Students will be introduced to CyberChef, a free tool created by GCHQ, nicknamed "The Cyber Swiss Army Knife" as it is a simple, intuitive web app which allows both technical and non-technical people to explore data formats, encryption and compression.

The students will then be shown two encrypted messages (see worksheet) that they can have a go at decrypting themselves using the CyberChef tool.

Please note that the correct answers and walkthrough for this are provided as part of the Day 5 knowledge nugget video.

Evaluation and next steps

Websites:

https://gchq.github.io/CyberChef/ CyberChef - use this free tool to encrypt or decrypt your own messages.

These links are being provided for informational purposes only; they do not constitute an endorsement or an approval by CyberFirst or the NCSC. The NCSC bears no responsibility for the accuracy, legality, or content of the external site or for that of subsequent links.

https://www.ncsc.gov.uk/cyberfirst/girls-competition to register for the next CyberFirst Girls' Competition.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©