Session 2: Basic Principles of Coding and Code Breaking

Explain the workings of the basic Caesar Shift Cipher. Explain to the students the significance of the public key (modulo 26) and the private key (the shift). Get students to try to decipher a message that had been set up using a shift.

Decode this message:

WKLV FRGH ZDV LQYHQWHG EB MXOLXV FDHVDW

(This code was invented by Julius Caesar).

Set up a multiplicative coding system. Give the public key (mod 26) but withhold the private key (x4). The word (LIMBS) becomes:

VJZHX

Show students how to decode using modular arithmetic (provide them with the private key).

In the case of 'V', this equates to '22' in the alphabet, so:

$4x = 22 \pmod{26}$

$4x = 22 + 26k$

If $k = 1$, $x = 12$

Get students to create their own coded message and swap it with someone else along with the private key. Students need to look for problems involved in the decoding process. When does the process break down?