Cryptography Mentor's Guide

The main thing a mentor needs to do for this activity is to convince students to try it. You can offer that they will get a large supply of cheesy jokes if they come work with you. You can ask then if they want to learn a skill that every true spy knows.

Give many high fives. Laugh at the jokes, or shake your head and say that's not funny. Ask what the next joke is.

Most students will figure out to wrap around when the numbers get larger than 25 in the letters to numbers section. If a student does not see what letter to assign to 34, ask a series of easier questions:

> What is letter 24? letter 25? letter 26? letter 27?
>
> Once they can count around make a larger jump – What is letter 47? what is letter 108? The student should be able to figure out that they can subtract 26, or any multiple of 26. Eventually, they should figure out that they can divide by 26 and take the remainder.

Some students will not know what $x \mapsto 3x + 7$ means. You can tell them that it means multiply by 3 and add 7. Thus 4 becomes 19 since $3 \times 4 = 12$ and $12 + 7 = 19$.

Decoding affine i.e. $x \mapsto mx + b$ ciphers requires Euclid's algorithm (long division). For example to decode $x \mapsto 15x - 4$ one would first want to find numbers a and b so that $15a + 26b = 1$. This process is explained in the rational tangle dance. *Ask the students if they have seen the rational tangle dance. If they have ask them if it could help them break the codes. If they haven't seen the dance yet, suggest that they go watch it when they want a break from the codes.* Indeed,

$$\begin{aligned}
15 \cdot 0 + 26 \cdot 1 &= 26 \\
15 \cdot 1 + 26 \cdot 0 &= 15 & \frac{26}{15} &= 1\frac{11}{15}, \text{ so subtract } 1 \\
15 \cdot (-1) + 26 \cdot 1 &= 11 & \frac{15}{11} &= 1\frac{4}{11}, \text{ so subtract } 1 \\
15 \cdot 2 + 26 \cdot (-1) &= 4 & \frac{11}{4} &= 2\frac{3}{4}, \text{ so subtract } 2 \\
\text{note } -1 - 2 \cdot 2 &= -5 \text{ and } 1 - 2 \cdot (-1) = 3 \text{ so} \\
15 \cdot (-5) + 26 \cdot 3 &= 3 \\
15 \cdot 7 + 26 \cdot (-4) &= 1\,.
\end{aligned}$$

Thus we can decode multiplication by 15 by multiplying by 7. Indeed multiplying any code letter c by 15 gives $15c$. Multiplying this by 7 gives $7 \cdot 15c = (1 + 26 \cdot 4)c$ which returns c after the wrap around.

A code that just makes substitutions between 26 symbols is not very secure. This is the point of the frequency analysis. In problem 14, the answer does not always follow the general frequency pattern, but all of the code strings are coded with the same code so once someone figures out what one letter is, it can be used on the entire page. **Ask the students if they can guess why the frequency pattern here does not follow the pattern for the general English language.** One reason is that this is a list of jokes, *Why did...*, *What did,...* so question words are used much more often than in typical writing samples.

Some answers/hints

5. 26 – not shifting at all is a cipher! It isn't very difficult to break, but mathematicians usually include trivial cases.

11. Since $3x + 7$ is decoded by $9x - 11$, students may be able to guess that $9x + 2$ will be decoded by something with $3x$.

12. Since $2 \times 13 = 26$ and this wraps around to 0, both 0 and 13 map to the same thing. Can the student guess another number that would give a problem? (13, 26, 0, 4, ... any number not relatively prime to 26.)