Scytale

Image source: https://commons.wikimedia.org/wiki/File:Skytale.png

A scytale (rhymes approximately with Italy) is one of the earliest known implementations of cryptography. The first mention of the scytale is from the Greek poet Archilochus who lived in the 7th century BC. That is over 2,600 years ago! It is believed the Greeks and the Spartans used the scytale to send messages to and from their battlefields. The type of encryption used by the scytale is known as a *transposition cipher*. A transposition cipher will shift the original letters according to a regular system so that it is more difficult for someone who doesn't know the system to read the original message.

Try it out at home

To send a secret message with a scytale, you'll need:

- Two tubes or cylinders of the same size. These are your scytales. An empty toilet paper or paper towel tube are two items you may have at home that would work.
- Thin, long strips of paper to wrap around your scytales. You may want to use masking tape to combine strips to allow for even longer messages.
- Something to write with

Instructions

1. Wrap your strips of paper around your scytale like you see in the picture above
2. Carefully write your secret message going across the paper with one letter on each strip
3. Unwrap the paper and deliver it to your partner. Try not to let anyone intercept the message!
4. See if your partner can successfully decode the message by wrapping the strip of paper around their scytale.

Other things to try

What would happen if someone tried to read your secret message, but the scytale they had wasn't the same size as yours?

This type of encryption isn't very secure by today's standards. How might you be able to figure out someone's secret message if you didn't have the correct sized scytale? Have someone write a message and see if you can crack the code!

Want to learn more?

Cryptography has come a long way in the past 2,600 years. If you want to learn more or have questions, just get in touch. You can find us at http://dc402.org or on Twitter @defcon402

Caesar Cipher

The Caesar Cipher, named after Julius Caesar who was known to use the technique, is another early example of cryptography. Sometimes referred to as a *shift cipher*, this method of encryption is a type of *substitution cipher*. The Caesar Cipher works by *shifting* the alphabet a set number of positions and substituting the resultant alphabet for the original message. In the case of Julius Caesar, he chose to shift the letters by three, which results in the following:

Normal: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Shifted: DEFGHIJKLMNOPQRSTUVWXYZABC

If Caesar wanted to protect the message “Attack at dawn”, it would be sent as “DWWDFN DW GDZQ”

Below is a visual representation to shows how the Caesar Cipher works

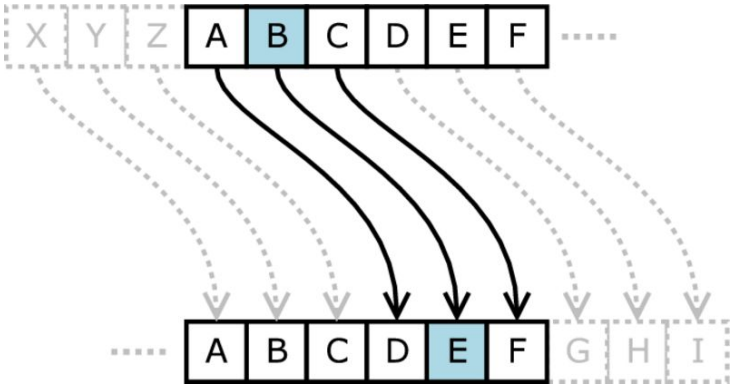

Image source: https://en.wikipedia.org/wiki/File:Caesar_substition_cipher.png

Try it out at home

While you can write out a substitution cipher alphabet like the one above, it can get a little repetitive to have to re-write the alphabet every time you want to change the key. To make this easier, you can construct a *cipher wheel*, shown at right. When completed, you can quickly rotate the wheel to the desired setting and quickly encrypt and decrypt. There are a wide variety of templates and instructions available online, simply search for ‘create a cipher wheel’ and you should be on your way in no time.