

Make a Scytale

In this activity, you will use a scytale to encode a message, then try to decrypt another group's message. You can find out more about how scytales were used in history [here](#).

You will need the following materials:

- Scytales (PVC pipe and wooden dowels)
- Paper strips (half inch width)
- Tape
- Something to write with

A scytale is a tool used to scramble (change the order) and unscramble the letters in a message. It is a rod (stick) that you can wrap a long strip of paper around. If you write a message across the rod, rather than down the strips, when you unwrap the paper strip, the letters are in a different order. To read the message, you need to wrap the paper back around a rod of the same diameter.

In your group, choose your scytale from the pile in the middle of your table. Don't let the other groups see which one you choose. Next, take several strips of paper and tape them together to make a long strip that will wrap around your chosen scytale enough times.

Next, choose the message that you will encrypt. Your message should be long enough to be interesting (at least five words). Write the message along the length of the scytale, with one letter per paper strip, as in the picture on the right. You may choose to leave the spaces in your message or omit them. Once your message is complete, continue to "pad" your message by writing random characters until your scytale is full.



Last, unwrap your message from the scytale and exchange with another group. Try to decrypt the other group's message without knowing which scytale they chose.

Discussion Questions

What is the algorithm in this cryptosystem?

What is the key?

What method did you use to crack the cipher?

Is this cipher secure according to Kerchoff's Principle? Why or why not?