Secret Codes
How to make them
How to break them
TODAY IS JUNE TWENTIETH
SCYTALE
The Pigpen Cipher

| A | B | C |
| D | E | F |
| G | H | I |

| J | K | L |
| M | N | O |
| P | Q | R |

| S | T | U |
| V | X | Y |

| > | E | F | V | U |
| > | N | O | V | A | C |

| > | E | F | V | U |
| > | N | O | V | A | C |

| X | M | A | R | K | S | T | H | E | S | P | O | T |
RSA Encryption

Message: I AM HERE

Change to numbers: 90001130008051805
(A=01, B=02, ... Z=26, Space=00)

Compute $90001130008051805 \div 65537$

Divide by 12193263122374638001
The remainder is 7695811381280782132

This is the secret message that you send.
Your friend receives

7695811381280782132

Compute 7695811381280782132 12191402595354763373

Divide by 12193263122374638001

The remainder is 90001130008051805

Change to letters:  I AM HERE
Shift Ciphers

To encrypt a message, shift every letter by a fixed amount.

For example, to encrypt HELLO we could shift each letter by 3:

HELLO ---\rightarrow KHOOR
Decrypt:
qcmbsioqylybyly

rdn...
seo...
tfp...
ugq...
vhr...
wis...

\[\text{Shift by 6}\]

wishyouwerehere
Frequencies of Letters in English
Frequencies of Letters in Message
The most commonly used six character password is one two three four five six. It is not recommended that you use it as yours.
Vigenere Cipher

Choose a sequence of shifts, for example 2, 5, 4, 7. Then apply these shifts successively to the message:

```
t h i s i s a m e s s a g e
2 5 4 7 2 5 4 7 2 5 4 7 2 5
v m m z k x e t g x w h i j
```
Suppose we know that the key length is 3. Look at the 1\textsuperscript{st}, 4\textsuperscript{th}, 7\textsuperscript{th}, \ldots letters.

This looks like a shift by 11.
Now look at the $2^{\text{nd}}$, $5^{\text{th}}$, $8^{\text{th}}$, \ldots letters:

This looks like a shift by 2.
Finally, look at the 3\textsuperscript{rd}, 6\textsuperscript{th}, 9\textsuperscript{th}, \ldots letters:

This looks like a shift by 22 (or by -4).
We guess that the shifts are by 11, 2, and 22.

Try decrypting and see:

The method used for the preparation and reading of code messages is simple in the extreme and at the same time impossible of translation unless the key is known. The ease with which the key may be changed is another point in favor of the adoption of this code by those desiring to transmit important messages without the slightest danger of heir messages being read by political or business rivals, etc.
The method used for the preparation and reading of code messages is simple in the extreme and at the same time impossible of translation unless the key is known. The ease with which the key may be changed is another point in favor of the adoption of this code by those desiring to transmit important messages without the slightest danger of their messages being read by political or business rivals, etc.

(from Scientific American, 1917)
Secret
Sharing
You are the manager of a bank. You want to allow your employees to open the safe.

Requirements:

1. One person alone cannot open the safe.

2. Any two people can open the safe.
Two People
determine a Secret
Two Points determine a Line
The secret combination to the lock is 

\[ ab \quad cd \quad ef \]

For example, the combination could be 

14 15 03
Let \( M = 2.abcdef5 \)

The 2 is chosen randomly.
The 5 is to avoid round-off errors.
The first 6 digits after the decimal point
Give the combination.

Choose a random \( B \)

We now have a line \( y = Mx + B \)
For example, if the combination is
14 – 15 – 03,
then
\[ M = 2.1415035. \]
We could randomly choose
\[ B = 3.456789. \]
The line is
\[ y = 2.1415035 \times + 3.456789 \]
If there are 30 people, compute 30 points on the line \( y = Mx + B \):

\[
(1, M+B), \\
(2, 2M+B), \\
(3, 3M+B), \\
\ldots \\
\ldots \\
(30, 30M+B)
\]

Give each person one point.
Each of you has a point \((x, y)\).

Your job is to find the combination.
There are spies in our midst!

Find out who they are.
Each envelope contains some points. Each person takes a point. One of the points is a forgery. If it is your point, you are a spy.

Are you a spy?