

5wITs ™
BOSTON
PRESENTS



CRYPTOGRAPHY MANUAL

SIMPLE CODES

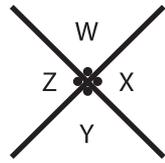
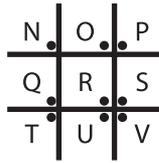
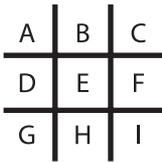
Here are two simple codes you can use any time you want to send a secret message.

Tick-Tac-Tricky:

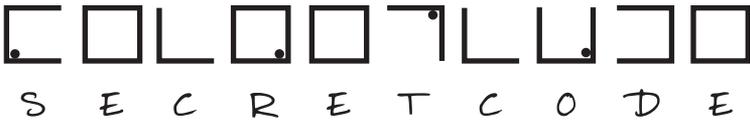
Use a simple grid to make a code out of shapes that will leave most people guessing.

How It Works:

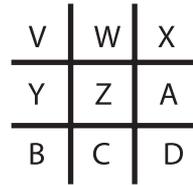
By using each cell's image, you can communicate a whole message just by using their shapes.



Example:



Now, you have to make sure to use the same method we wrote our chart out above. Always starting at the top-left in the nine-section grids and in the top position of the 4-section grids. If you really want to mix it up, you and your friend can agree to mix it up a bit by starting the alphabet at a random letter. If you started with "V" your chart would start like this one on the right. Just make sure your friend knows where you're starting your alphabet!



Crack The Code:



-----?

Dictionary/Book Code:

By using your favorite book or a dictionary you can create a very secure code by listing the coordinates of the words you're using as they appear in the book. As long as your friend has the same book, they can decipher your code just by turning the pages!



The Format:

Sticking to a specific format is essential for this code to work! Write the number of the page, followed by the number of the line the word appears on, and finally, what number the word is on that line. Put a period between them, and you'll have your coordinates.

If your word doesn't appear exactly as it should in the book, you can add letters to the numbers to complete it.

Example:

If "My Secrets Are Coded" is your message, you might find the word "My" on page 10 of your book, on the 3rd line and 5 words in. Your first coordinate would be "10.3.5" Secrets might only come up as "Secret" on the 50th page of your book, on the 8th line and 1 word in, so you could write your coordinates as "50.8.1s" and that way your friend will know to add the "S" at the end. "Are" might be on the 20th page, 13th line and 8th word in, so "20.13.8" for your third coordinate and finally, we'll say that "Code" was found on page 135, line 19, word 4, which leaves us with the following for our final code:

10.3.5 | 50.8.1s | 20.13.8 | 135.19.4d

Which doesn't look like much of anything if you don't know what you're looking for! The code below uses this book as it's reference.

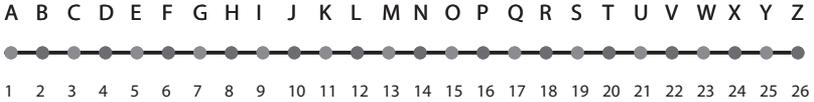
1.7.1 | 2.14.2e | 3.13.10 | 3.1.15

CAESAR CIPHER

Caesar was a smart guy, and this simple code was the least of his clever means of secret communication. This is the most basic form of encoding your messages.

How It Works:

Most codes are easier to use if you treat the letters like numbers. Like so:



Now, by using simple "modular addition" (in simple modular addition when you reach the end of a number set, 1-26 in this case, you start over from the beginning again.) you can encode a message.

Example:

If you wanted to send the message "Brutus is coming" to Caesar you would pick a number to modify by (5 in this case) add that to your letters, and write down the letter that matches your new number.

| | | | | | | | | | | | | | | |
|-------|---|----|----|----|----|----|----|----|---|----|----|----|----|----|
| | B | R | U | T | U | S | I | S | C | O | M | I | N | G |
| | 2 | 18 | 21 | 20 | 21 | 19 | 9 | 19 | 3 | 15 | 13 | 9 | 14 | 7 |
| + | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| <hr/> | | | | | | | | | | | | | | |
| | 7 | 23 | 26 | 25 | 26 | 24 | 14 | 24 | 8 | 20 | 18 | 14 | 19 | 12 |
| | G | W | Z | Y | Z | X | N | X | H | T | R | N | S | L |

In order to decipher this code Caesar would need to know what number you used to modify the letters. This would be a pretty simple code to crack even if you didn't know. Just trying each number would eventually give the answer.

Crack The Code:

W K H V H F U H W L V R X W

— — — — — — — — — — — — — —

TRANSPOSITION

In a "Columnar Transposition" cipher you first pick out a key word. This must be known to both the encoder and decoder for the cipher to work. The alphabetical order of the key word is also important. For this example we'll use the key word of "WITS" which, if we take it alphabetically, will be "ISTW". It's important to remember this as we build the code.

How It Works:

Using your key word to regulate the number of columns (in our case 4, one for each letter in WITS) you write out the text you want to encode in short lines with no spaces. Then, you rearrange the columns by the alphabetical position of the letters of key word. Write the letters back out in a line and you have your code.

Example:

We'll encode the phrase "I Love Cryptography"

First, we write our key word out at the top. Then, 4 letters at a time, we'll write out our phrase. When we get to the end, however, we have a couple of blank spaces, so we'll just fill those in with some random letters. In this case "LBR". Now, rearrange the columns by the alphabetical order of our keyword:

| | | | |
|---|-----|-----|-----|
| W | I | T | S |
| I | L | O | V |
| E | C | R | Y |
| P | T | O | G |
| R | A | P | H |
| Y | (L) | (B) | (R) |

| | | | | |
|---|---|---|---|--|
| I | S | T | W | With the columns mixed up we can write out the code by |
| L | V | O | I | reading from left to right. (Don't include the keyword!) |
| C | Y | R | E | Our scrambled code is: LVOICYRETGOPAHPRLRBY. |
| T | G | O | P | When the person we're sending it to needs to decode |
| A | H | P | R | it, they write out the key word in alphabetical order and |
| L | R | B | Y | the encoded message below it. (Just like the diagram to |
| | | | | the left) Then rearrange the columns to follow the written |
| | | | | order of the word and they will see our original message! |

Crack The Code:

Our key word is "CODEX"

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| G | O | D | O | L | U | K | W | C | I | T | T | |
| H | H | E | N | X | T | E | O | N | F | W | E | Z |

GRACK THE GODE

Each step in this code has to be used to solve the next step. If your answers seem confusing, keep going. The text will be scrambled until the very end. If you do everything right, you'll get the final code word. Good luck! This one is HARD!

Step 1:



Step 2:

Caesar
Cipher

Step 3:

Key Word:
"CRYPT"

C R Y P T

| | |
|-------|-------|
| ----- | ----- |
| ----- | ----- |
| ----- | ----- |
| ----- | ----- |
| ----- | ----- |

Step 4: One time pad on the back cover

What is the code word? _____

KEEP LEARNING!

Want to learn some of the history behind these codes? Log on to 5-wits.com/codex to read about how these codes have been used throughout history and discover some more advanced methods to make your secrets even safer!

You'll also find a tool that will let you create your own One Time Pads and do quick Caesar Ciphers. The last lesson for you is this: Keep making codes! All of the codes we showed you today were invented by different people throughout history. You can invent your own, and if you're very good at it? You might even be able to get a job doing it professionally some day. Think you can be a cryptographer? Good luck, and keep learning!



Copyright - address - credits - blah blah blah
Schuyler Towne - stowne@5-wits.com

G J K R T L Z Q F G W N A X D C K P C L