

Codes

Codes, like police radio 10- codes, substitute words or numbers for other words. A *codebook* gives codes and their meanings. Here is a very small codebook.

| Codebook | |
|------------|------------|
| CAMEL | BICYCLE |
| HOUSE | |
| ██████████ | GO TO |
| STOP | PLAY |
| POPCORN | BASKETBALL |

Exercise: Using the codebook above, decode the following message.

LET'S THE ON OUR AND .

Ciphers

Ciphers change or scramble the letters in a message. Most modern cryptosystems are ciphers.

A *transposition cipher* keeps the same symbols, but scrambles them in a specific way.

Decrypt a message encrypted with the up-and-down cipher:

MEMATRCOLETEFESHO

- Count the letters of the message
- Divide the message in the middle. (If an odd number of letters, the first “half” gets the extra letter.)
- Copy one letter from the left half, then one from the right, going back and forth.

Decrypted message:

A *substitution cipher* substitutes symbols in a message.

Create your own key word substitution cipher. Here is an example

Pick a key word, cross out duplicate letters. Example: