Encryption Keeps Your Secrets

Professor Bob Brown – Kennesaw State University
Bob.Brown@Kennesaw.edu

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.

This Code	Means this
CAMEL	BICYCLE
HOUSE	PLAYGROUND
KICK	GO TO
STOP	PLAY
POPCORN	BASKETBALL

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

LET'S **KICK** THE **HOUSE** ON OUR **CAMELS** AND **STOP POPCORN**.

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.

Exercise: 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:

Last update: 2018-03-14

A *substitution cipher* substitutes symbols in a message.

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

Pick a key word, cross out duplicate letters. Example: CRYPTOL~~O~~G~~Y~~
From the alphabet, cross out letters in the key word: AB~~C~~DEF~~G~~HIJK~~L~~MN~~O~~~~P~~Q~~R~~S~~T~~UVWX~~Y~~Z
Your key is the remaining letters from the key word followed by remaining letters from the alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
CRYPTOLGABDEFHIJKMNQSUVWXZ

Your keyword: ______________________ Cross out any duplicate letters.

From the alphabet, cross out letters in the keyword: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Now copy the letters from your keyword (not crossed out) and the letter from the alphabet, not crossed out to "Your key" below.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Your key: ____

Write a short message in all capitals, no spaces, and encrypt it using your key.

Message: ____

Cipher text: ____

Copy the encrypted message and key to a piece of scratch paper and give it to your neighbor. Decrypt your neighbor's message and your neighbor will decrypt yours.

Further Reading

If this has been fun, read *The Kids' Book of Secret Codes, Signals, and Ciphers* by E.A. Grant or, for older students, The *Code Book* by Simon Singh. There are several versions of this with differing publication dates and subtitles. Any one will do. *Hint:* You don't have to buy this; the library is your friend.

KENNESAW STATE UNIVERSITY
College of Computing and Software Engineering