Cryptography and Encryption

Take-home exercise: the One-Time Pad, an unbreakable Vigenère cipher

You will need the background from the Vigenère exercise before you attempt this one.

The Vigenère cipher is breakable because of regularities in the key. If the key were completely random and did not repeat, that is, the key is as long as the message, then the cipher is unbreakable, provided the key *is never re-used*. The problem, then, is how to generate a long, random key. The solution: Scrabble tiles. You can get Scrabble tiles at places like Wal-Mart, Amazon, and Michaels without buying a Scrabble set.

Write out your secret message, then use Scrabble tiles to generate a key. Put 26 tiles, one for each letter, in a small box. Resist the temptation to use all the tiles. If you do, your key will not be random and your cipher can be broken. Generate your key like this:

1. Shake the box thoroughly.
2. Without looking, take one tile from the box.
3. Write the letter on the tile as one letter of your key.
4. Put the tile back in the box.
5. Go to step 1.

Keep going until you have a key letter for every letter in your plain text message. For a relatively long message, this cipher is unbreakable, but, of course, the recipient of the message must have a copy of the key, and the key must not fall into the hands of adversaries. (*Beware:* Using even unbreakable encryption to cover wrongdoing does not work because we leave other evidence.)

Random letters with dice

If you don't have Scrabble tiles, you can generate random letters with dice.

For each letter, shake and throw two dice. Subtract one from the value of each die. For example, the dice at the right would be two and three. Multiply the value after subtraction of the leftmost or uppermost die by six. So, for the example, $2 \times 6 = 12$. Add the value after subtraction of the remaining die, so $12 + 3 = 15$, and your random letter is the 15^{th} letter of the alphabet, or the letter O. If a throw of the dice gives a number greater than 26, ignore it and throw the dice again.

Kennesaw State University
College of Computing and Software Engineering

Last update: 2018-10-29