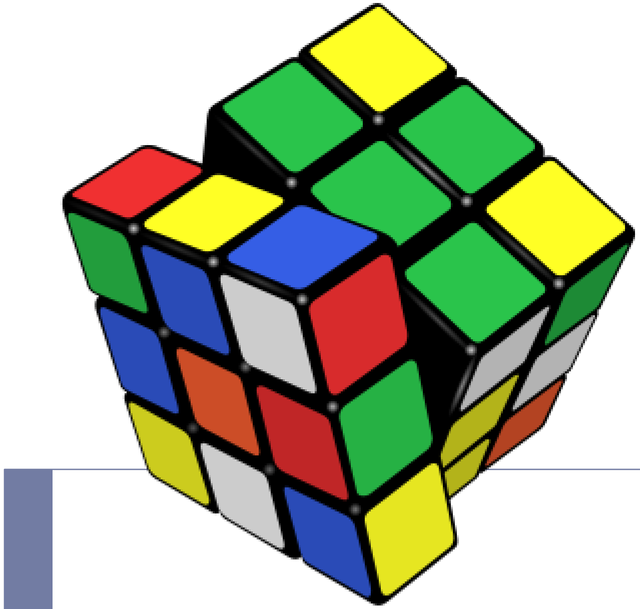

Discrete Mathematics

Cryptography

Classical Cryptography

- One of the earliest known uses of cryptography was by Julius Caesar. He made messages secret by shifting each letter three letters forward in the alphabet (sending the last three letters of the alphabet to the first three).

- For instance, using this scheme the letter B is sent to E and the letter X is sent to A.

- This is an example of encryption, that is, the process of making a message secret.

Classical Cryptography

- To express Caesar's encryption process mathematically, first replace each letter by an element of Z26, that is, an integer from 0 to 25 equal to one less than its position in the alphabet.
- For example, replace

A by 0,
K by 10, and
Z by 25.

Caesar's encryption method can be represented by the function f that assigns to the nonnegative integer p, $p \leq 25$, the integer f (p) in the set $\{0, 1, 2, \ldots, 25\}$ with

$$f(p) = (p + 3) \bmod 26.$$

In the encrypted version of the message, the letter represented by p is replaced with the letter represented by $(p + 3) \bmod 26$.

EXAMPLE 1

What is the secret message produced from the message "MEET YOU IN THE PARK" using the Caesar cipher?

Solution: First replace the letters in the message with numbers. This produces

12 4 4 19   24 14 20   8 13   19 7 4   15 0 17 10.

Now replace each of these numbers p by

$$f(p) = (p + 3) \bmod 26.$$ This gives

15 7 7 22   1 17 23   11 16   22 10 7   18 3 20 13.

Translating this back to letters produces the encrypted message "PHHW BRX LQ WKH SDUN."

EXAMPLE 2

- Encrypt the plain text message "STOP GLOBALWARMING" using the shift cipher with shift k = 11.

Solution:

- To encrypt the message "STOP GLOBAL WARMING" we first translate each letter to the corresponding element of Z26. This produces the string

  18 19 14 15   6 11 14 1 0 11   22 0 17 12 8 13 6.

- We now apply the shift f (p) = (p + 11) mod 26 to each number in this string. We obtain

  3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17.

Translating this last string back to letters, we obtain the cipher text "DEZA RWZMLW HLCXTYR."

EXAMPLE 3

Decrypt the cipher text message

"LEWLYPLUJL PZ H NYLHA ALHJOLY"

that was encrypted with the shift cipher with shift k = 7.

Solution:

To decrypt the cipher text

"LEWLYPLUJL PZ H NYLHA ALHJOLY"

we first translate the letters back to elements of Z26.

We obtain

11 4 22 11 24 15 11 20 9 11 15 25 7 13 24 11 7 0 0 11 7 9 14 11 24.

Next, we shift each of these numbers by $-k = -7$ modulo 26 to obtain

4 23 15 4 17 8 4 13 2 4 8 18 0 6 17 4 0 19 19 4 0 2 7 4 17.

Finally, we translate these numbers back to letters to obtain the plaintext.

We obtain

“EXPERIENCE IS A GREAT TEACHER.”

We can generalize shift ciphers further to slightly enhance security by using a function of the form

$$f(p) = (ap + b) \bmod 26,$$

where a and b are integers, chosen so that f is a bijection. (The function $f(p) = (ap + b) \bmod 26$ is a bijection if and only if $\gcd(a, 26) = 1$.)

Such a mapping is called an affine transformation, and the resulting cipher is called an affine cipher.

EXAMPLE 4

What letter replaces the letter K when the function f (p) = (7p + 3) mod 26 is used for encryption?

Solution: First, note that 10 represents K. Then, using the encryption function specified, it follows that f (10) = (7 · 10 + 3) mod 26 = 21. Because 21 represents V, K is replaced by V in the encrypted message.

We will now show how to decrypt messages encrypted using an affine cipher. Suppose that c = (ap + b) mod 26 with gcd(a, 26) = 1. To decrypt we need to show how to express p in terms of c. To do this, we apply the encrypting congruence c ≡ ap + b (mod 26), and solve it for p. To do this, we first subtract b from both sides, to obtain c − b ≡ ap (mod 26). Because gcd(a, 26) = 1, we know that there is an inverse a of a modulo 26. Multiplying both sides of the last equation by a gives us a(c − b) ≡ aap (mod 26). Because aa ≡ 1 (mod 26), this tells us that p ≡ a(c − b) (mod 26). This determines p because p belongs to Z26.

Suppose that we intercepted the cipher text message

ZNK KGXRE HOXJ MKZY ZNK CUXS

that we know was produced by a shift cipher. What was the original plain text message?

Solution: Because we know that the intercepted cipher text message was encrypted using a shift cipher, we begin by calculating the frequency of letters in the cipher text.

We find that the most common letter in the cipher text is K. So, we hypothesize that the shift cipher sent the plaintext letter E to the cipher text letter K. If this hypothesis is correct, we know that

$$10 = 4 + k \bmod 26, \text{ so } k = 6.$$

Next, we shift the letters of the message by −6, obtaining

THE EARLY BIRD GETS THE WORM.

Because this message makes sense, we assume that the hypothesis that $k = 6$ is correct.