**Math 314 - Fall 2019**
**Notes 8/26/2019**

---

## Caesar's Cipher

Caesar's Cipher is one of the most popular and earliest example of an encrypting method. Caesar's Cipher assigns a number to each letter in the alphabet (*starting with 0 and ending with 25*) and then shifts each letter's position by some amount (*known as a "key"*).

For example, to create a cipher with a key of 3, we would start by writing the alphabet and assigning each letter with its position:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Then we would shift the letters in the alphabet 3 (*the key*) places to the left:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| D | E | F | G | H | H | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

So if we were to encrypt the word **"door"** we can see that the letter 'D' corresponds to the letter 'G', the letter 'O' to the letter 'R', and the letter 'R' to the letter 'U'. **"door"** encrypted with a shift 3 would be: **"GRRU"**.

Here is a visual representation of how the cipher works:

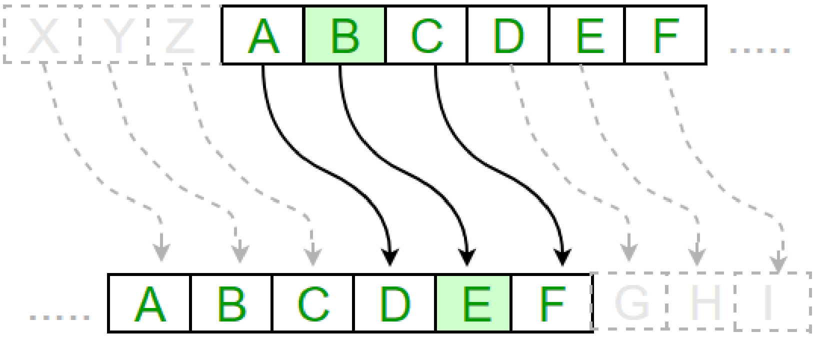

Figure 1: Source: GeeksforGeeks.org

In a more mathematical sense, we can write an encryption function that takes in an alphabet letter, "x", and then returns its encrypted version , "E(x)". The encryption function would look like this:

$$E(x) = x + k \mod 26$$

Where "x "is any letter from A to Z, "k" is how much you are shifting, and "mod" is the remainder after division.

**Example 1.** Use the encryption function to encrypt the word "bat" with a key of 7.

'b' has an index of 1 in the alphabet, so solve for E(1):

$$E(1) = 1 + 7 \mod 26$$
$$E(1) = 8 \mod 26$$
$$E(1) = 8$$

The letter 'b' corresponds to the letter 'I' since I's position in the alphabet is 8 (*see above tables*). Now do the same for the rest of the letters ‘a’ has an index of 0 in the alphabet, so solve for E(0):

$$E(0) = 0 + 7 \mod 26$$
$$E(0) = 7 \mod 26$$
$$E(0) = 7$$

The letter ‘a’ corresponds to the letter ‘H’ since H’s position in the alphabet is 7.

‘t’ has an index of 19 in the alphabet, so solve for E(19):

$$E(19) = 19 + 7 \mod 26$$
$$E(19) = 26 \mod 26$$
$$E(19) = 0$$

The letter ‘t’ corresponds to the letter ‘A’ since A’s position in the alphabet is 0. With each letter encrypted, we can now concat them together to create the encrypted word: “IHA”.

---

Suppose we now want to decrypt an encrypted message; we can write a decryption function that takes in an encrypted letter, “y”, and returns its original decrypted version, “D(y)”. The decryption function would look like this:

$$D(y) = y - k \mod 26$$

Where “y “is any letter from A to Z, “k” is how much you are shifting, and “mod” is the remainder after division.

**Example 2**. Use the decryption function to decrypt the word “IHA” with a key of 7.

‘I’ has an index of 8 in the alphabet, so solve for D(8):

$$D(8) = 8 - 7 \mod 26$$
$$D(8) = 1 \mod 26$$
$$D(8) = 1$$

The letter ‘I’ corresponds to the letter ‘b’ since b’s position in the alphabet is 1 (*see above tables*). Now do the same for the rest of the letters

‘H’ has an index of 7 in the alphabet, so solve for D(7):

$$D(7) = 7 - 7 \mod 26$$
$$D(7) = 0 \mod 26$$
$$D(7) = 0$$

The letter ‘H’ corresponds to the letter ‘a’ since a’s position in the alphabet is 0.

‘A’ has an index of 0 in the alphabet, so solve for D(0):

$$D(0) = 0 - 7 \mod 26$$
$$D(0) = -7 \mod 26 \equiv 19 \mod 26$$
$$D(0) = 19$$

The letter ‘A’ corresponds to the letter ‘t’ since t’s position in the alphabet is 19. With each letter decrypted, we can now concat them together to create the original decrypted word: “bat”.

---

**Kerckhoff’s Principle**: when analyzing the strength of a cryptographic system, you should assume thte attacker knows everything about the system except the key

## Three Types of Attacks

**1) Ciphertext Only Attack**: attacker only has knowledge of encrypted ciphertext and goal is to decrypt it and find the key.

**2) Known Plaintext Attack**: attacker learns the contents of a message along with its ciphertext counterpart and goal is to find the key.

**3) Chosen Plaintext Attack**: attacker gains access to the encryption machine and can encrypt any message and see its ciphertext counterpart and goal is to find the key.

Examples of these attacks using Caesar Cipher as an example

**Chosen Plaintext Attack**: attacker would choose the letter 'a' to encrypt since E(0) would return the key; proof:

$$E(0) = 0 + k \mod 26$$

$$E(0) = k \mod 26$$

$$E(0) = k$$

**Known Plaintext Attack**: if attacker knows that 's' encrypts to 'N', attacker can figure out the key; proof:

$$E(18) = 18 + k \equiv 13 \mod 26$$

$$k \equiv -5 \mod 26$$

$$k = 21$$

**Ciphertext Only Attack**: attacker would have to either use frequency analysis on the ciphertext or use a brute-force approach exhausting all possible keys.