How to Simply Encrypt and Decrypt a Message

Dustin Ingram, Hahna Kane, Jacob Lukas

October 15, 2009

Intended Audience

- Someone with little to no background in cryptography
- Someone interested in solving puzzles

A Need for Cryptography

- Concealing information is prevalent throughout history
- Historical and modern applications in government, military, and personal domains
- Sensitive, personal, electronic data is exchanged daily: ATMs, Internet commerce, computer passwords, etc.

Defining Cryptography

Cryptography is:

- The science of designing systems to study and secure communication over non-secure channels
- The process of creating, analyzing and deciphering ciphers

A cipher is:

- A concealed message or collection of data
- Also known as a “code” or “cryptogram”

Conventions of Cryptography

Before messages can be encrypted and decrypted, the following conventions need to be understood:

1. *plaintext* will be presented as italicized, lowercase letters and CIPHERTEXT will be presented as all capital letters.
2. The letters of the alphabet are assigned numbers as follows

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

3. Spaces and punctuation are omitted.

A Simple Cipher

- A cipher encrypts every string of characters by some algorithm
- Modern ciphers require the use of a computer and are usually computationally impossible to break
- However, some ciphers are simple enough to execute by hand

Caesar Cipher

The Caesar Cipher is a "shifted" cipher, first recorded to be used by Julius Caesar to protect messages of military significance. In general, shifted ciphers require a key κ with $0 \leq \kappa \leq 25$. For encryption,

$$x \mapsto x + \kappa \tag{1}$$

Similarly, decryption is

$$x \mapsto x - \kappa \tag{2}$$

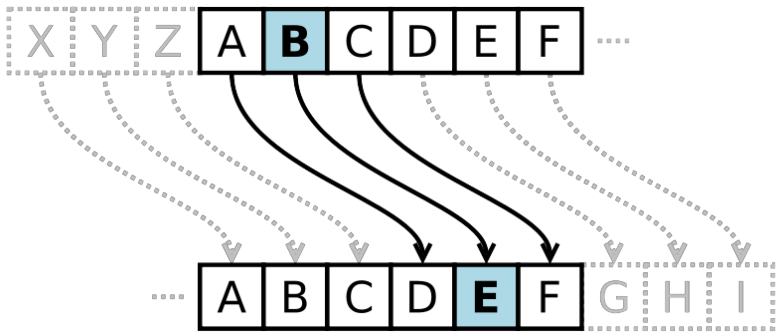
Traditionally, when using the Caesar cipher, $\kappa = 3$.

The Caesar Cipher

Suppose Alice wanted to send the plaintext

technical communication rocks

to Bob, but she wanted to hide the message from Eve. Alice simply shifts each letter by three places



The resulting ciphertext becomes

WHFKQLFDOFRPPXQLFDWLRQURFNV

Cryptanalysis of the Caesar Cipher

- Cryptanalysis is the process of attacking or breaking into a system to figure out what was communicated
- In the previous example, there are four possible scenarios in which Eve could decipher Alice's message without a key
  1. Eve discovers Alice's encryption machine
  2. Eve discovers Bob's decryption machine
  3. Eve knows at least one letter of the plaintext and the letter it maps to in the ciphertext
  4. Eve only knows the ciphertext

Cryptanalysis of the Caesar Cipher

- Best strategy: perform an exhaustive search

κ	Plaintext
0	WHFKQLFDOFRPPXQLFDWLRQURFNV
1	*vgejpkecneqoowpkecvkqptqemu*
2	*ufdiojdbmdpnnvojdbujpospdlt*
3	*technicalcommunicationrocks*
4	*sdbgmhbzkbnlltmhbzshnmqnbjr*
5	*rcaflgayjamkkslgayrgmlpmaiq*
...	...

- Next best alternative: examine the frequency count of the letters

Conclusion

- Learned the history and significance of ciphers
- Learned how to encrypt and decrypt a message using a Caesar cipher
- Learned how to attack a Caesar cipher message in four different ways

Questions?