A Clear and Concise Commentary on Caesar Cipher

3rd edition
Soup

March 2016

I A Foreword by CTF God

"When I heard the learn'd astronomer, When the proofs, the figures, were ranged in columns before me, When I was shown the charts and diagrams, to add, divide, and measure them, When I sitting heard the astronomer where he lectured with much applause in the lecture-room, How soon unaccountable I became tired and sick, Till rising and gliding out I wander'd off by myself, In the mystical moist night-air, and from time to time, Look'd up in perfect silence at the stars." — Walt Whitman.

One of the simplest yet functionally practical algorithms for cryptography remains the Caesar cipher, documented by the Roman historian Suetonius and utilized by the great Julius Caesar himself, the cipher's namesake. Prevalently used yet nearly impossible to crack, it is fundamentally straightforward and an important milestone for beginners looking into the field of cryptography in today's world. All in all, its simplicity is as elegant as its usage is ubiquitous.

Weaving a deeper understanding of variegated topics into the minds of others is at the heart of nicebowlofsoup's work. When it comes to quintessential subjects such as the structure of the Caesar Cipher, she precisely describes how it can be employed in a non-technical sphere of usage while delving into its details to perfectly evoke a sort of transcendental wonder. Her explanations and developments not only serve to enrich all perspectives on each topic but also present a singular solution to any muddled perception—much like the very nature of the Caesar cipher itself.

II Introduction

Many beginners who are interested in cryptography first learn about a simple cipher called the Caesar cipher. It is a widely used cipher for the lazy and casual

conversers. Contrary to popular belief, the Caesar cipher continues to be an increasingly useful tool, however challenging its concept may seem. It is, at least, an incredibly noteworthy device that should be forever preserved in culture.

Regardless of previous education, you should pick up the Caesar cipher for several reasons:

- secure, private conversations
- to learn the alphabet
- bragging rights
- for an introduction to other ciphers
- because it's named after Caesar
- pursuit of knowledge
- winning sCTF

As you can see, this is the optimal and most practical cipher known to mankind. So, just continue reading and we will provide you with: A Clear and Concise Commentary (and tutorial) of the Caesar Cipher.

III A History

The Caesar Cipher was created as an ingenuous way for Julius Caesar to encrypt his correspondence. This later became the standard for secret messages,

IV Ciphers

A full understanding of ciphers must be necessary to understand the Caesar Cipher. In cryptography, a cipher is an algorithm (a set of operations (calculations from a number of values to create more values) to be performed on (applied on or done to) a data structure (a way to store (to keep, to hold) information (In Claude E. Shannon's (American mathematician (person who does math) and cryptographer) terms, the logarithm (a function defined as some multiple ($\exists k$ s.t. $g(x) = kf(x)$) of the integral (opposite of a (one (1)) derivative ($\lim_{x\to\infty} f(x)$)) of the reciprocal function ($1/x$)) of the number of total states (number of distinct ways something (a thing) can be in with given information (defined earlier)) divided (multiplied by the reciprocal (defined earlier)) by the number of states (defined earlier) that a message represents))) for performing encryption (the process of encoding (changing the text in an organized way) messages (strings (character arrays) containing information) in such a way that only selected parties (or people) are able to read

(understand) it) and decryption (the process of undoing (reversing) encryption (defined earlier)).

Ciphers generally (vast majority ($p > 0.95$) of the time) substitute (replace (substitute) one element (thing within an array (ordered (having a $>$ operator (a symbol representing operations (calculations from a number of values to create more values)) defined such that for all a, b, c (variables) if $a > b$ and $b > c$, then $a > c$) collection (set) of objects (things))) with another object of the same type (another object that acts the same way under the same operations)) different (distinct, not equal ($=$)) length (size, or information value/content) strings of characters (letters, numbers, ascii stuff) in the output (thing that comes out of the cipher), while ciphers generally substitute the same number (integer ($n \in \mathbb{Z}$), or real number ($z \in \mathbb{R}$), or occasionally complex number ($z \in \mathbb{C}$), depending on context (other text nearby, skipping parentheses)) of characters as in the input (stuff that goes in).

IV.I Semi-Formal Definition

A *symmetric* cipher is a computable multivariate function $f(x, \hat{k})$ of two values such that there exists computable inverse function g such that $g(f(x, \hat{k}), \hat{k}) = x$. In other words, a function f is a cipher if its a bijection from strings to other strings. The string x is known as the *message*, and each of the values in the vector $\hat{k}$ is known as *keys*. The result of the function, $f(x, \hat{k})$, is known as the *ciphertext*.

Attacks (methods for circumventing (going around) the security (unbreakable-ness) of a cryptographic system (such as a cipher) by finding a weakness (a point that breaks easily)) on ciphers typically involve attempting (trying very very hard (a lot)) to find (or derive, in this case) the message x given some information; this information typically does not include the key, because that would be too easy.

We will now look at one type of cipher called the Caesar Cipher.

V Caesar Cipher

Essentially you keep shifting the letters of a message by a set number, which we refer to as the key.

VI Cracking the Code

Here we have an example of a Caesar'ed sentence. This is your ciphertext.

```
JXYI YI CO UDSETUT IUDJUDSU.
```

So how can we approach cracking this code? There are several ways:

1. Clever Guessing
2. Giving up
3. Brute-forcing

So the first one, clever guessing, turns out to be a brilliant method to crack codes! Much like with the Enigma machine, which was once thought to be impregnable, sometimes clever guessing is necessary. In this case, we can see that "YI" and "CO" are two-character words. There are only a few of these in the English language: "is," "or," "my," "if," and a few others. However, there is only one key that would allow both "YI" and "CO" to decode to valid English words. Through process of elimination, you will find that everything was shifted by +16. Thus, the message will decode to:

`THIS IS MY ENCODED SENTENCE.`

... and that is how you use method one.

The second method is what we call giving up. We understand that breaking the Caesar Cipher can sometimes we extremely difficult. That said, we often find that the time taken to decrypt a Caesar'ed string is not worth the outcome. This is because there is a tendency for people to encode their random, useless messages using the Caesar Cipher. So giving up is a completely valid option.

The last method is brute-forcing. The concept of brute-forcing is to go through every single possible key for the Caesar Cipher. This is thankfully computationally feasible, but it is a tedious task, considering that there are 27 entire letters in the alphabet. Due to the sheer amount of letters there are, this makes brute-forcing the less-preferred option. Moreover, this option demonstrates very little creativity and very little resourcefulness. But necessary, one can always use this site for help with Caesar Cipher:

`http://www.dcode.fr/caesar-cipher`

This C program (which can easily be translated into any other language) will be sure to give you the proper plaintext if you test some keys:

```c
#include <stdio.h>
#include <ctype.h>
#define MAXSIZE 1024
void encrypt(char*);
void decrypt(char*);
int menu();

int main(void)
   {
   char c, choice[2], s[MAXSIZE];
   while(1)
```

```
    {
        menu();
        gets(choice);
        if((choice[0]=='e')||(choice[0]=='E'))
        {
            puts("Input text to encrypt->");
            gets(s);
            encrypt(s);
        }
        else if((choice[0]=='d')||(choice[0]=='D'))
        {
            puts("Input text to decrypt->");
            gets(s);
            decrypt(s);
        }
        else
            break;
        }
        return 0;
    }
void encrypt(char*str)
{
   int n=0;
   char *p=str,
       q[MAXSIZE];
    while(*p)
   {
       if(islower(*p))
       {
          if((*p>='a')&&(*p<'x')) q[n]=toupper(*p + (char)3);
          else if(*p=='x') q[n]='A';
          else if(*p=='y') q[n]='B';
          else q[n]='C';
       }
       else
       {
          q[n]=*p;
       }
       n++;
       p++;
   }
   q[n++]='\0';
   puts(q);
}

void decrypt(char*str)
{
   int n=0;
   char *p=str,
```

```
        q[MAXSIZE];
    while(*p)
    {
        if(isupper(*p))
        {
           if((*p>='D')&&(*p<='Z'))
              q[n]=tolower(*p - (char)3);
           else if(*p=='A')
              q[n]='x';
           else if(*p=='B')
              q[n]='y';
           else
              q[n]='z';
        }
        else
        {
           q[n]=*p;
        }
        n++; p++;
    }
    q[n++]='\0';
    puts(q);
}

int menu()
{
    puts("To encrypt, input e or E\n");
    puts("To decrypt, input d or D\n");
    puts("To exit, input any other letter\n");
    puts("Your choice:->\n");
    return 0;
}
```

VII Practise Problems

Here are some good practise problems to work with to hone your Caesaring skills!! Don't worry if this may seem tedious at first; they'll become easier as you solve more!

- `omz kag odmow ftue oubtqd`
- `h fns sghr qhfgs sghr shld`
- `WKLV LV QRW WKH IODJ`
- `xaywqoa fqheqo eo ykkh hega pdwp`

- `ldnv bdzrzq hr dzrx`
- `RNFLPGS{LBHTBGVG}`
- `omt vbvdi`
- `gmbbbbbbbbbbbbh`

VIII Advantages of Caesar Cipher

VIII.I What Makes a Cipher Secure?

IX Usage

Caesar Ciphers are often the most challenging cryptography problems found in Capture-the-Flag games, which are cybersecurity and hacking competitions. Understanding and breaking the Caesar Cipher will indicate your level of cryptography mastery and earn you much respect. But the real-life uses?

You can find the Caesar Cipher everywhere if you just look for it. For example, it can be used for cheating or unfaithfulness. It can also be used to exchange private keys! Just kidding.

X A Closing Note

We hope you learned a lot about Caesar Cipher! You will now be able to proceed with the CTF. :)