An Efficient Implementation for the Cryptanalysis of Caesar's Cipher

[1,*]Gaylord O. Asoronye, [2]Goodluck I. Emereonye, [3]Christian O. Onyibe & [4]Ibiam A. Agha

[1]Electronic Library Unit, [2]Computer Science Department, [3]Computer Engineering Department

[1,2,3] Akanu Ibiam Federal Polytechnic, Unwana, Ebonyi state, Nigeria.

[4]Computer Science Department, Federal Polytechnic Oko, Anambra State, Nigeria.

[*]Correspondence: asorgay@gmail.com

Abstract

One of the oldest algorithms for symmetric key cryptography is the Caesar's cipher. Cryptography or message coding techniques are fundamental data security tools. In order to secure data to be transmitted from source to a particular destination there is need for encrypting the data at source and the decrypting of the encrypted data only made possible at the designated destination. The process of decrypting data known as cryptanalysis proves to be a herculean task if the symmetric key (Caesar's shift) is not known by the cryptanalyst. In this work, a cryptanalysis of the encryption algorithm using the encryption formula CipherText = PlainText + (Key mod 26) that generates the cipher text and the decryption algorithm using the decrypting formula PlainText = CipherText – (Key mod 26) that returns the cipher text to the original plaintext for the Caesar's cipher was implemented using file operations in the C programming language. At the instance of inputting a key, it is subjected to modular arithmetic operation with 26 to get a value less or equal to 26, hence transforming the plaintext to a cipher text written into the encrypt.txt file while the decrypted cipher text is written into the decrypt.txt file.

Keywords: cryptography, security, encryption, cipher, decryption.

Introduction

Data in its processed state is known as information, which is the lifeblood of any organization. It is a formidable asset since the more the access to the information concerning an organization one has the more powerful and dangerous the person becomes. Organizations may have confidential data such as financial forecasts, earnings, customer lists, product roadmaps, staff and customer contacts, and strategic corporate data that is meant for internal usage on a classified mode; data sniffing or outright theft of these classified information could lead to the violation of individual or the organizations privacy thereby limiting the organizations competitive advantage over her rivals (Acharya, Sajwan, & Bhargava, 2013). On the other hand, secret information comprising organizational secrets like design details, research and development discoveries, intellectual properties, usernames and passwords, production formulas, encryption and decryption codes or keys; if in the possession of wrong

individuals can seriously endanger the reputation of an individual or organization. This information's are usually in the possession of a few persons or units in an organization. The level of safe access by personnel who need to use confidential or classified data in an organization is determined by the level or mode of security control measures deployed by the organization.

The drill of keeping one's assets out of the reach of unauthorized persons or intruders who prey into peoples properties illegally is an ancient practice that has existed from the origin of man. When the property is in form of data or information, it is called data or information security. Data or information security provides three main services; Confidentiality, Integrity and Accessibility (Zban, 2017). Zban (2017) posited that, "The protection of sensitive information against unauthorized access to fraudulent changes has been of prime concern throughout the centuries". As far back as we had secrets to keep, secret message writing (cryptography) has been in use, which may be in the form of messages between individuals, messages in war or just private coded messages.

Although cryptographic techniques were used extensively during World War I and II, it can be traced from Egypt about 4,000 years ago (Siper, Farley, & Lombardo, 2005). According to Hernandez-Castro & Avoine (2016), Cryptography was derived from two Greek words. 'Krypto' meaning secret or hidden and 'Graphene' meaning writing; hence cryptography refers to "secret writing". Ismael Imran & abdulameerabdulkareem (2014), defines cryptography as the science and art of concealing information using some special techniques, called cryptographic algorithms or ciphers, such that only the anticipated user can have access to them. They see cryptography as the process of converting messages in their readable form referred to as plaintext to an unreadable form referred to as ciphertext. It is possible to convert the ciphertext back to the original plaintext through the process called cryptanalysis.

A system that converts plaintext to ciphertext through the application of a set of transformations to each character or letter in the plaintext is known as a cipher. The exact transformation to be implemented at any time is determined by a key used at that time and the security of the ciphertext lies solely in the secrecy of the key (Dey, Nath, & Nath, 2012). Caesar cipher, one of the earliest cryptographic models was first used by Julius Caesar around 50 BC (Purnama & Rohayani, 2015). It works by shifting the alphabet a number of

places known as Caesar's shift to the right and wrapping the last letters back unto the first letters, thus;

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 I J K L M N O P Q R S T U V W X Y Z A B C

For the purpose of explanation the chosen key (Caesar shift) here is three (3) any other key value between 1 and 25 can be used. Caesar cipher operates on modulo 26 for the English alphabets this makes for 26 different keys. For example, the plaintext **bed** is transformed using 3 Caesar shifts to **ehg.** In essence this transformation can be executed by a computer using modular arithmetic (Yan, 2012). Any message can be expressed in its digital form as it corresponds to its index number.

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

In using Caesar cipher to encrypt any plaintext message, it requires the transformation based on the encryption formula:

$C = P + (K \bmod 26)$ …… Equation 1

Where;

C = the corresponding numeric value of the ciphertext letter

P = the corresponding numeric value of the plaintext letter

K = the symmetric key value

To decrypt the ciphertext is based on the decryption formula;

$P = C - (K \bmod 26)$ …… Equation 2

Equation 2 is a reverse of the encryption formula in Equation 1.

This research work is based on the implementation of Caesars cipher a symmetric key cryptography using the file operations in C programming language. Whereas Julius Caesar used tedious hand written method to implement the cipher, and others used various computing techniques, this work proposed an efficient C code for the cryptanalysis of the Caesar cipher for better data security.

Literature Review

The study of the cryptosystems known as Cryptology comprises of two disciplines: cryptography and cryptanalysis. Cryptography is concerned with the design of cryptosystems, while cryptanalysis studies the breaking of cryptosystems (Yan, 2012). Cryptography is the branch of science that deals with data transmission security (Sengupta & Holmes, 2013). It is one of the major study areas in Information Security. There are other areas of study like steganography and network security. Encryption is the technique of mystifying a plaintext so as to hide the original data from an unauthorized person while decryption is the demystifying of the ciphertext to the original plaintext. Purnama & Rohayani (2015), defines cryptography as the science and art of encrypting and decrypting data with the use of special techniques and methodologies. In their work, Caesar's cipher was modified using a java applet program to analyze the frequency of occurrence of the Indonesian alphabets to implement a legible monoalphabetic cipher. In this work the C programming language which is very close to assembly language was used for implementation making it easy to use file operations. Hernandez-Castro & Avoine (2016), on the other hand opines that cryptanalysis is the branch of science that deals with breaking the code and extracting the secret message. Siper et al., (2005) defines a cipher as an algorithmic function that converts plaintext into a meaningless form by applying a set of transformation techniques to each letter in the plaintext. The technique used in Caesars cipher at any time is controlled by a cryptographic key called the Caesar shift and the security of the ciphertext rest solely on the secrecy of this key. Gowda (2016) in his work used the Diffie-Hellman's method to obtain the Caesar shift. This method according to his findings made his algorithm more secured but in terms of execution time, it took longer time than the naïve Caesar's approach used in this work. According to a study in 2009, Poschmann wrote that ciphers can be classified using several criteria. In one of such criteria, the ciphers are classified as symmetric key and asymmetric key. In symmetric key ciphers, the same key is used for both encryption and decryption. The main challenge is that both the sender and receiver must know the key before transmitting their message. In asymmetric key cipher different keys are used for encryption and decryption both of them being mathematically related. The key for encryption is called the public key while the key for decryption is called private key.

Poschmann (2009), further wrote that, in symmetric encryption, ciphers can be classified into stream ciphers and block ciphers; stream ciphers obtain ciphertext by using the XOR of the plaintext and keystream (bi-wise). They are grouped into two: synchronous stream cipher, whose key sequence does not depend on the plaintext and ciphertext but only on the previous elements of the key sequence and the initial key, e.g. One-time password (OTP); and asynchronous stream cipher, whose keystream depends on the plaintext or ciphertext, e.g. Cipher Feedback mode (CFB). Other examples of stream ciphers include RC4 and SEAL. Block ciphers, on the other hand, operate on a fixed length block size. It can be considered simply as a large lookup-table (substitution cipher). In particular, identical plaintext blocks encrypt to identical ciphertextblocks. Examples include Data Encryption Standard (DES), 3Data Encryption Standard (3DES), Advanced Encryption Standard (AES), Blowfish, etc.

The Algorithms

This research performs a symmetric key cryptography and a cryptanalysis of both the encryption algorithm for transforming the plaintext to ciphertext and the decryption algorithm for transforming the ciphertext back to the original plaintext. It is designed and implemented using the file operations of C programming language in a Code::Blocks IDE windows environment. The algorithms generate .txt files for Plaintext, Encrypted text and Decrypted text respectively. The message is read from the plaintext.txt file while both the encrypted and decrypted text are written to the encrypted.txt and decrypted.txt files respectively.

3.1. Encryption algorithm

These are the steps followed:

Step 1: Start

Step 2: Write message into the plaintext.txt file

Step 3: Enter Caesar shift

Step 4: Call encryption function

Step 5: Write output to encrypted.txt file

Step 6: Stop

```
30  void enCipher(char message[]){
31
32    int ch,i;
33
34    for(i = 0; message[i] != '\0'; ++i){
35          ch = message[i];
36
37          if(ch >= 'a' && ch <= 'z'){
38              ch = ch + r;
39
40              if(ch > 'z'){
41                  ch = ch - 'z' + 'a' - 1;
42              }
43
44              message[i] = ch;
45          }
46          else if(ch >= 'A' && ch <= 'Z'){
47              ch = ch + r;
48
49              if(ch > 'Z'){
50                  ch = ch - 'Z' + 'A' - 1;
51              }
52
53              message[i] = ch;
54          }
55      }
56  }
57
```

Figure 1. A code snippet of the encryption function

3.2. Decryption algorithm

These are the steps followed:

Step 1: Start

Step 2: Read message from the encrypted.txt file

Step 3: Enter Caesar shift

Step 4: Call decryption function

Step 5: Write output to decrypted.txt file

Step 6: Stop

```
58  void deCipher(char message[]){
59
60      int ch,i;
61
62      for(i = 0; message[i] != '\0'; ++i){
63              ch = message[i];
64
65              if(ch >= 'a' && ch <= 'z'){
66                  ch = ch - r;
67
68                  if(ch > 'z'){
69                      ch = ch + ('z' - 'a') + 1;
70                  }
71
72                  message[i] = ch;
73              }
74              else if(ch >= 'A' && ch <= 'Z'){
75                  ch = ch - r;
76
77                  if(ch > 'Z'){
78                      ch = ch + ('Z' - 'A') + 1;
79                  }
80
81                  message[i] = ch;
82              }
83      }
84  }
85
```

Figure 2. A code snippet of the decryption function

Results and Discussion

System testing technique is used to test the model. When the program is run, a command prompt dialog box which asks the user to enter the cipher key is displayed.

```
Enter your Cipher key!      3
Hello world,
Cryptography or message coding techniques are fundamental data security tools.
In our society today, where data sniffing has become prevalent, most individuals

and organizations are so concerned in the full protection of their data.

Process returned 0 (0x0)   execution time : 3.245 s
Press any key to continue.
```

Figure 3. A screenshot of displayed command prompt showing the chosen key and plaintext.

Once the user enters the cipher key, the original message is copied from the text.txt file. The Plaintext (message) is encrypted by the encrypt function and the result (ciphertext) written in the encrypted.txt file.

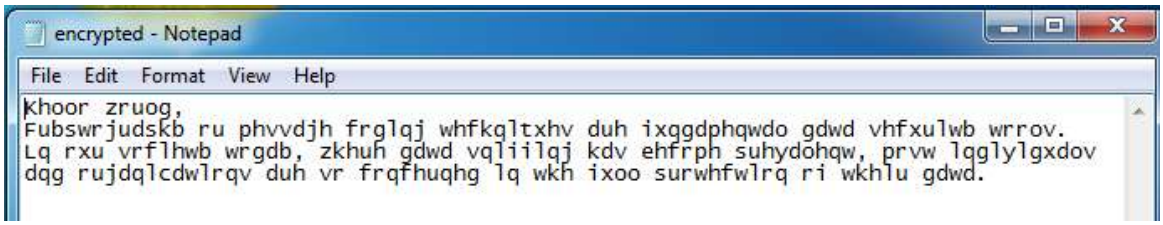

Figure 4. A screenshot showing the encrypted message (ciphertext)

During the decryption process, the ciphertext is decrypted by the decrypt function and the result (plaintext) written in the decrypted.txt file.

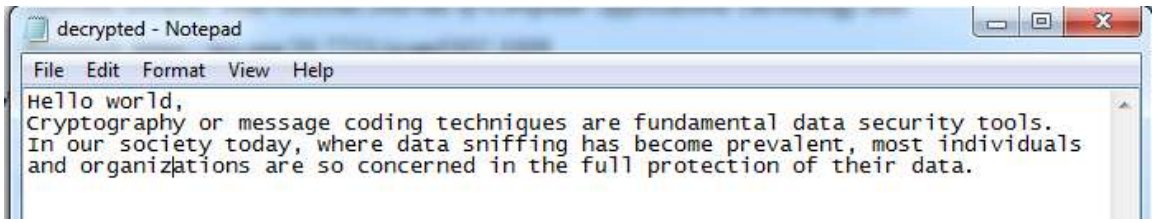

Figure 5. A screenshot showing the decrypted message (plaintext)

Conclusion

This work implemented a symmetric key cryptography known as Caesar's cipher an efficient but tedious manual data security tool using the C language. The cryptanalysis of the algorithms for generating ciphertext and decrypting it back to the original plaintext were fully implemented. It was observed that when a key (Caesar's shift) was entered the original text was transformed into a cipher text and when decrypted by the decryption algorithm using the same key the ciphertext was transformed back to the plain text. In addition to other techniques proposed and implemented by other scientists, the use of file operations of the C programming language used in this work, conveniently presents an efficient implementation for the cryptanalysis of Caesar's cipher, reiterating it as viable data security tool that can be employed for the security of an organizations Information.

Conflicts of Interest: The authors declare no conflicts of interest

References

Acharya, K., Sajwan, M., & Bhargava, S. (2013). Analysis of Cryptographic Algorithms for Network Security. *International Journal of Computer Applications Technology and Research*. https://doi.org/10.7753/ijcatr0302.1009

Dey, S., Nath, J., & Nath, A. (2012). An Integrated Symmetric Key Cryptographic Method –

Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal method: SJA Algorithm. *International Journal of Modern Education and Computer Science*. https://doi.org/10.5815/ijmecs.2012.05.01

Gowda, S. N. (2016). Innovative enhancement of the Caesar cipher algorithm for cryptography. *Proceedings - 2016 International Conference on Advances in Computing, Communication and Automation (Fall), ICACCA 2016*. https://doi.org/10.1109/ICACCAF.2016.7749010

Hernandez-Castro, J., & Avoine, G. (2016). Cryptanalysis of ubiquitous computing systems. *Proceedings of the 18th Mediterranean Electrotechnical Conference: Intelligent and Efficient Technologies and Services for the Citizen, MELECON 2016*. https://doi.org/10.1109/MELCON.2016.7495307

Ismael Imran, P. E., & abdulameerabdulkareem, P. F. (2014). Enhancement Caesar Cipher for Better Security. *IOSR Journal of Computer Engineering*. https://doi.org/10.9790/0661-16350105

Poschmann, A. (2009). Lightweight Cryptography: Cryptographic Engineering for a Pervasive World. *Ph. D. Thesis*. https://doi.org/10.1.1.182.1450%20

Purnama, B., & Rohayani, A. H. H. (2015). A New Modified Caesar Cipher Cryptography Method with LegibleCiphertext from a Message to Be Encrypted. *Procedia Computer Science*. https://doi.org/10.1016/j.procs.2015.07.552

Sengupta, N., & Holmes, J. (2013). Designing of cryptography based security system for cloud computing. *Proceedings - 2013 International Conference on Cloud and Ubiquitous Computing and Emerging Technologies, CUBE 2013*. https://doi.org/10.1109/CUBE.2013.20

Siper, A., Farley, R., & Lombardo, C. (2005). The rise of steganography. *Proceedings of Student/Faculty Research Day*.

Yan, S. Y. (2012). Computational Number Theory and Modern Cryptography. In *Computational Number Theory and Modern Cryptography*. https://doi.org/10.1002/9781118188606

Zban, J. (2017). Information security. *62nd Annual Business Aviation Safety Summit, BASS 2017*.