Adaptation for Vigenère Cipher Method for Auto Binary Files Ciphering

Ammar Waysi AlTuhafi[1*]

[1]Department of Computer Science, Knowledge University, Erbil, Iraq

Abstract. Protecting the private information from third party became an important issue in computer science nowadays; cryptography is a science of encryption and decryption information. The first use of cryptography was in ciphering text messages, with the developing of computer usage; other type of files has been appeared such as: picture, audio, video, etc. These types of files can carry private information that needs to be saved from the third part. This paper based on design and implement system for auto encryption/decryption binary files by adapting well-knownVigenère encryption methods, by converting binary files to stream of bytes and encrypting each byte of this stream. The result shows the complete auto protection for the binary files.

1 Introduction

Usually security in computer science can be divided into two main types; network security and information security, the old term of information security usually bounded with texts, whereas, there are numerous number of algorithms that deal with text encryption and decryptions; although most of these algorithms has been proved as perfect algorithms in text encryption, there is no use for these algorithm with another type of data (files) beside text files. Therefore, this study deals with how to use one of these algorithms for encrypt and decrypt binary files [1].

Cryptology is the science where security engineering meets mathematics to make communication mysterious to people except those who are involved in this communication and have the right to read it. Cryptology provides us with tools to do encryption process. The cryptography deals with the secrecy system itself and its design, and cryptanalysis is how breaking this secrecy system [2].

The first use of cryptography was in military and secret agents. In these days we need cryptography everyday because of the daily use of computers and the Internet; and the need to security become personal need beside institutions or organizations, especially when there are commercial transactions over the internet [2].

From the previous, can be concluded, that the first and main use of cryptography is with texts encryption, which is the message between two sides that can be transmitted in secure way because no one can understand the message except the two sides. These days the information

*Correspondingauthor:ammar.waysi@knu.edu.iq, dr.ammar.altuhafi@ieee.org

can be represented in many shapes, such as pictures, video, audio, etc. therefore, encrypt these type of data (files) is required; needing new algorithm to find suitable key for these files is required too, whereas, the key is a basic need in encryption and decryption [3].
Basically every file is a series of bytes in sequence. The value of each byte is between 0 and 255. In general every file is a binary file, but it depends on the data in it, if it contains only text like: letter, numbers, symbols used in writing, then this file can be considered as text file. The binary file is computer readable, not a human readable. All implemented programs are stored in binary files also numeric data files, beside video, audio, picture, etc , in other words text files can be readable, while other file are not[4, 5]. The aim of this research is to design and implement auto cryptosystem for encrypting and decrypting binary files

2 Background

2.1 Vigenère Ciphering Method

This name is back to the Frenchman Blaise de Vigenère, a diplomat who served King Charles IX. Vigenère cipher is a method of encrypting alphabetic by using either the Vigenère square or algebraic way. The Vigenère square is 26X26 table with row heading and column heading from A to Z. The first row of this table has the 26 English letters sequentially, but with starting with the second row to the last one the letter will be shifted one position to the left and the previous letter will moves to the end in cyclic way. i.e. in second row B is shifted to the first position, and A take the last position.

This method the keyword repeated until it equal the length of the plaintext. For example, consider the plaintext is TECHNOLOGY and the keyword is PEN. The keyword repeated as following: TECHNOLOGY
PENPENPENP

To encrypt, take a letter in the plaintext and its corresponding in the keyword, use the keyword letter as row index and plaintext letter as column index, the cross index is the letter in the cipher text. In the example above the first letter is T and its corresponding is P, the cross between them is I which is the first letter in cipher text, repeating this process until all plaintext is encrypt and get the result. The cipher text is: IIPWRBASTN [6].

To decrypt, take the letter in cipher text and its corresponding in the keyword, use the keyword letter and find its row and search in this row for the letter of cipher text, then the head of the column of this letter is the corresponding plaintext letter. So the result of this cipher text IIPWRBASTN is TECHNOLOGY.

To decrypt, take the letter in cipher text and its corresponding in the keyword, use the keyword letter and find its row and search in this row for the letter of cipher text, then the head of the column of this letter is the corresponding plaintext letter. So the result of this cipher text IIPWRBASTN, is TECHNOLOGY.

Vigenère can also represent in algebraic way with the following equation for encryption:

$$C = (P + K) \; Mod \; 26 \quad (1)$$

While used the following equation for decryption:

$$C = (P - K) \; Mod \; 26 \quad (2)$$

While C represents cipher text letter, P represents the letter of plaintext, and K represents the letter of keyword. The letters A-Z are taken as numbers 0-25 so each letter takes his number and implemented in the equations [7].

3 Methodology

The meaning of encryption of binary file is transfer a normal binary file to encrypted binary file, to produce encrypted binary file. No one can understand the contents except the sender and receiver; the following are the steps of encryption with details.

3.1 Key Extraction from Binary File

The key that will be used in the operations will be extracted from the binary file itself, this will be done by choosing two different numbers (K1 and K2), whereas, K1 represents the frequency of repeating the key, while K2 represents the length of the key, i.e. if K1=9 and K2=7, this mean each nine bytes will choose the last byte as a part of the key, this process will continue until the length of the key become seven which is the value of K2; therefore the values of bytes number (9, 18, 27, 36, 45, 54, 63) become the key of Vigenère encryption method.

The key that will be used in the operations will be extracted from the binary file itself, this will be done by choosing two different numbers (K1 and K2), whereas, K1 represents the frequency of repeating the key, while K2 represents the length of the key, i.e. if K1=9 and K2=7, this mean each nine bytes will choose the last byte as a part of the key, this process will continue until the length of the key become seven which is the value of K2; therefore the values of bytes number (9, 18, 27, 36, 45, 54, 63) become the key of Vigenère encryption method, the K1 will be choose at the time when user sends the message, K1and K2 will be extracting from device clock, K1 represent the seconds while K2 represents the milliseconds at the time when user sends the message as said .

3.2 Binary File Encryption by Vigenère

After extracting the key from binary file, the encryption of binary file will happen by Vigenère ciphering method with some modifications to be adaptive, the formula for encryption will be as the following:

$$C= (M + K) \; MOD \; 256 \quad (3)$$

In this operation we add M to K, where M is the number of the bit from the binary file, K is the key that has been extracted, the MOD here is 256 because the ciphering here on binary

files not text, whereas the maximum value of the byte is 255. The key's bytes will be inserted in the same places in encrypted binary file.

3.3 Keys Insertion in Encrypted binary File

The K1 and K2 will be sent to the receiver inside file, therefore, the sender and receiver have to know the position of both keys inside the encrypted fil, sometimes can be the first two or last two bytes or any position known for both sides, this insertion will happen before sending the encrypted binary file. Fig.1 shows the methodology of encrypting binary files.

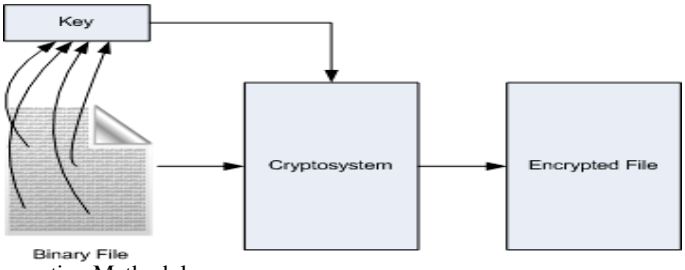

Fig.1. Encryption Methodology

3.4 Decryption Binary Files

Each encrypted item (message or file) need decryption to get it back to original value; the following are the steps of decryption with details.

3.5 Key Extraction from Encrypted Binary File

The method of extracting key from encrypted binary file it is the same method that explains the key extraction in encryption process by using the K1 and K2 which they also extracted from the binary file assaid in section 3.3, based on the position of them in binary file.

3.6 Binary File Decryption by Vigenere

Taking the encrypted file and the extracted key, then apply decryption according to Vigenère method rules by using the following formula:

$$(C - K) = M \quad (4)$$

$$If\ X < 0\ Then\ \ X = X + 256 \quad (5)$$

In this operation subtract K from C, in case the result in minus (less than zero), the number 256 will be added to get positive number which represent the original value of the byte, after applying this process for the whole file, then the original binary file can be retrieved, fig 2 show decryption of the binary files.

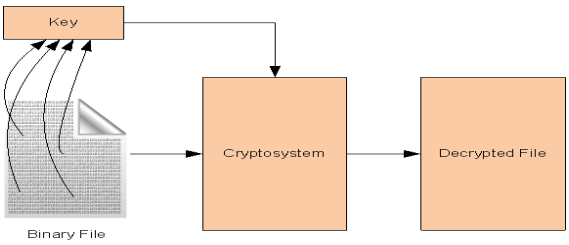

Fig.2. Decryption Methodology

4 Results

The complexity of the algorithm can be written as following: O (m+n+2)

Whereas m is the length of the key that will be extracted from the binary file, n is the length of the binary file because the adapted Vigenère equation will be applied for the whole binary file. The number 2 represents of the K1 and K2; from the previous it is clear that the complexity of the algorithm is low.

Appling this algorithm for on binary files in different types, such as image, video, audio, etc, shows the ability to encrypting the binary files and make software such as photos viewers and audio/video players not able to view or play the file.

Algorithm evaluation against brute-force attack can be calculated according to the number of possible combinations, the following formula shows the possibility of brute-force attack [8].

$$Possible\ combinations = CL \quad (6)$$

Whereas C =possible number of characters and L = password length

The value of C in this algorithm is 256; which is the possible values of a byte because the range of the value of byte is (0-255), while the length of the key can be any number less than file length.

i.e. if the key length is 100, then possible combinations will be as following:

$$possible\ combinations = 256^{100} = 6.668 * 10^{240} \quad (7)$$

To calculate the time that needed to break the key, supposed that an attacker uses China's Tianhe-2 supercomputer, which is the fastest supercomputer. This computer is able to perform $33.86 * 10^{15}$ floating point operations force per second.

To calculate the time needs to break the key with length 100 byte the following formula can be used.

$$t = \frac{c^{L}}{33.86\times10^{15}\times(3600\times24\times30\times12)} \quad (8)$$

Applying this formula for key with length 100 byte, the result is $6.33*10^{216}$ years the time that needed to try all the possible combinations [9].

The comparison between the adaption algorithm and well-known Data Encryption Standard (*DES*) ciphering method; DES method cipher depends on bitwise operations which is considered closest ciphering method to this research; DES use key with 56 bit by applying equation 7 for DES, the result shown as following: $6.9*10^{110}$ years the time that needed to try all the possible combinations; which is less $1.1*10^{106}$ years than time needs for the adaptation algorithm [10, 11].

5 Conclusion

This study focus on adaptive encryption method of text messages for binary files. The study shows the ability of encrypting binary files based on Vigenère ciphering method. The key that used to encrypt binary file extracted from the file itself; then this key become a key of Vigenère encryption method, and adding this key to the binary file before sending it. Whereas the binary file acts like text message and combined with the extracted key according to Vigenère encryption method equation, while the sequence of choosing the key parts will be sent as well as inside encrypted binary file. This study shows the ability to encrypt the binary file and disabling any application for reading binary files to open and show its contents.

References

[1] S. Schwartz, "Cryptology for Beginners," *Wissahickon HighAmbler, Pa,* vol. **19002**, (2004).
[2] C. P. Pfleeger and S. L. Pfleeger, *Security in computing*: Prentice Hall Professional Technical Reference, (2002).
[3] R. J. Anderson, *Security engineering: a guide to building dependable distributed systems*: John Wiley & Sons, (2010).
[4] G. Szabo. (2016). *What is a text file and what is a binary file?* Available: https://perlmaven.com/what-is-a-text-file
[5] M. Rouse. (2012). *Binary File.* Available: https://whatis.techtarget.com/definition/binary-file
[6] Q.-A. Kester, "A hybrid cryptosystem based on Vigenère cipher and columnar transposition cipher," *arXiv preprint arXiv:**1307.7786**, (*2013).
[7] Q.-A. Kester, "A cryptosystem based on Vigenère cipher with varying key," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* vol. **1**, (2012).
[8] AceBIT. (2018). *Brute-Force Attacks*. Available: https://www.password-depot.com/know-how/brute-force-attacks.htm
[9] F. L. Malallah*, et al.*, "Irreversible Biometric Template Protection by Trigonometric Function," *International Review on Computers and Software (IRECOS),* vol. **11**, (2016).
[10] P. V. Saraswathi and M. Venkatesulu, "A block cipher algorithm for multimedia content protection with random substitution using binary tree traversal," *Journal of Computer Science,* vol. **8**, (2012).
[11] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Workshop on the Theory and Application of of Cryptographic Techniques*, (1993).