IOP Conference Series: Materials
Science and Engineering

PAPER • **OPEN ACCESS**

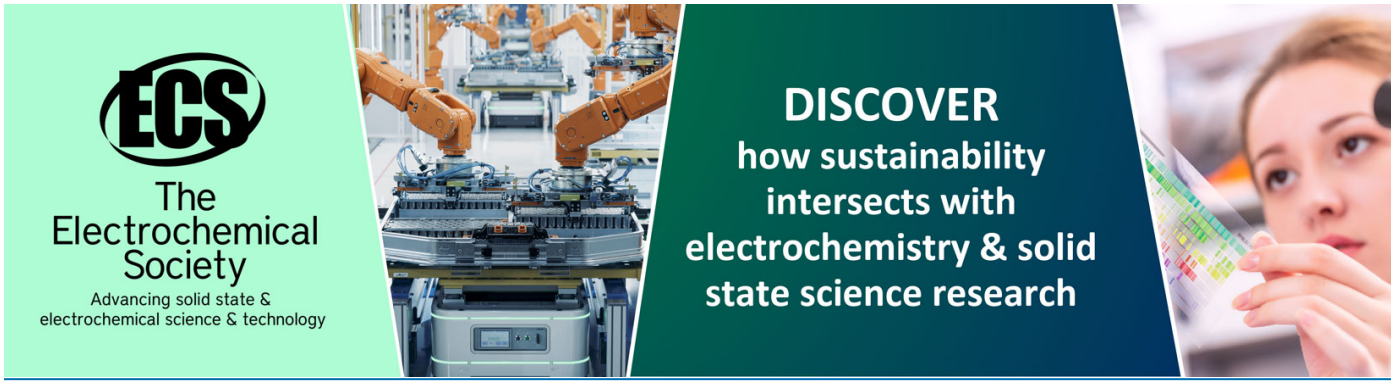
Security analysis in file with combinations One Time Pad Algorithm and Vigenere Algorithm

To cite this article: H Mawengkang *et al* 2018 *IOP Conf. Ser.: Mater. Sci. Eng.* **420** 012129

View the article online for updates and enhancements.

You may also like

- Optical voice encryption based on speckle-illuminated fourier ptychography and plaintext-related chaotic random phase mask
Jiaxin Li, Wenjun Xu, Yonghui Wang et al.
- A new method of image encryption using advanced encryption Standard (AES) for network security
Saba Inam, Shamsa Kanwal, Rabia Firdous et al.
- Roadmap on optical security
Bahram Javidi, Artur Carnicer, Masahiro Yamaguchi et al.



This content was downloaded from IP address 18.216.230.107 on 05/05/2024 at 05:24

Security analysis in file with combinations One Time Pad Algorithm and Vigenere Algorithm

H Mawengkang*, I L Sitepu, and S Efendi

Departemen S2 Teknik Informatika, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Jl. Universitas No. 9-A, Kampus USU, Medan 20155, Indonesia

*ivana.sitepu@gmail.com

Abstract. Security is a big issue and securing important data is so important that it can't be tapped or misused for illegal purposes to the detriment of others. Cryptography is a way used to maintain security where messages are disguised into encrypted messages. One-time cryptography pad is one type of cryptographic technique that uses substitution method by giving special terms to the key used that is made of characters or random letters (random key or pad), and the randomness does not use a certain formula. The Vigenere code includes a poly alphabetic subtitution cipher which in subtitle technique each text have many possible original texts. Super Encryption is a method of combining between the two algorithms that aims to get a stronger cipher making it very difficult to solve. The result of this research is the process time stated that the average time of plaintext encryption process with 50 characters is 3 milisecond while the mean time of plaintext encryption process with 100 characters is 7.33 milisecond. Then for the average time of encryption ciphertext process with 50 characters is 75,333 milisecond while the mean time of ciphertext encryption process with 100 characters is 132,333 milisecond.

1. Introduction

Security is a big problem and securing critical data is so important that the data can't be tapped or misused for illegal purposes to the detriment of others. For this reason the government and other institutions try to secure their data as hard as possible in order to avoid tapping. Even so still there are those who try to break it by using various keys and methods. To avoid it the data sent is converted into data that can't be read by the cryptanalys then the data is changed back in a form that can be read by the recipient. Techniques and sciences to create data that can't be read so that only authorized people are able to read data, this is called cryptography [1].

Cryptography is divided into two types: classical and modern cryptography. In the application, modern cryptography is more trusted by the public as a technique for securing data, but not a few people still use classical cryptography by combining two classical cryptographic algorithms [2].

One-time pad cryptography is one type of cryptographic technique that uses substitution method by giving special terms to the key used that is made of characters or random letters (random key or pad), and the randomness does not use a certain formula. In other words a one-time pad is a system which a randomly generated secret key is used only once to encrypt a message which is then decrypted again with the same key. This method was invented by Gilbert Vernam in the first world war.

The Vigenere code includes a poly alphabetic subtitution cipher which in its subtitle technique each text can have many possible original texts [3]. The advantage of this algorithm is the difficulty of performing cryptanalysis by the method of frequency analysis because the

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

same two letters in the text of the code may not necessarily be described as the same two letters in the original text. However, this algorithm uses a short key and its repeated use.

One Time Pad and Vigenere are part of the early development of cryptography, or part of classical cryptography. This algorithm utilizes the shift of existing letters to data or messages to be secured by using a key in the number of shifts and words or wording for the process of randomizing data or messages. The process that is done is encryption and decryption. This thesis discusses the use of the combination of one time pad and Vigenere to secure text data on messages, so that the content of the message can only be read by the recipient of the message.

2. Method

The first encryption process will be done with One Time Pad algorithm and then encrypted again using Vigenere algorithm. And then the first decryption process will be done with the Vigenere algorithm then One Time Pad algorithm.

One Time Pad algorithm (OTP) is a symmetric key type algorithm which means that the key used to perform encryption and decryption is the same key. In the encryption process, this algorithm uses a stream cipher derived from the XOR result between the plaintext bit and the key bit. In this method plaintext is converted into ASCII code and then subjected to XOR operation against the changed key into ASCII code.

Encryption can be described as the sum of modulo 26 of a plaintext character with one key character one time pad. Mathematically this process can be explained by the following equation [4]:

$$ci = (pi + ki) \bmod 26 \quad (1)$$

Explaination :
pi : plaintext character
ki : key character
ci :ciphertext character

After the sender encrypts the message with one time pad, it destroys the one time pad (so-called one-time or one-time). The recipient of the message uses the same one time pad to decipher the ciphertext characters into plaintext characters with the equation:

$$pi = (ci - ki) \bmod 26 \quad (2)$$

An algorithm is said to be good security, if there is no or no way to find its plaintext. Until recently, only the One Time Pad (OTP) algorithm was declared unbreakable although unlimited resources.

The principle of encryption in this algorithm is to combine each character on the plaintext with one character on the key. Therefore, the key length must be at least equal to the length of the plaintext. In theory, it is impossible to encrypt ciphertext without knowing the key. Because if the key used is wrong, the result will be wrong, or not the plaintext. Then each key should only be used for a single message. Key retrieval must be done randomly so that the opponent cannot be guessed and the number of key characters must be as many as the number of message characters.

The vigenere password is a classic password that has a relatively simple concept and it is widely used today. The idea of this vigenere password is a modified caesar password. If the Caesar password uses a single password keyword, the vigenere password uses as many repeating keywords as needed with the length of the message. The letters to be encoded are adjusted with numbers, a = 0, b = 1, c = 2, ..., z = 25. Then add the keyword numbers and message numbers. Then the result is preceded by 26, and the result of that number is

converted into letters to get encoded letters [5]. Vigenere password is a classical cryptographic algorithm, this algorithm is classified as a basic algorithm because it uses a character-based algorithm [6].

The Vigenere Cipher algorithm is well known for being easy to understand and implement [7]. Techniques to produce ciphertext can be done using numeric substitution and Vigenere square. Vigenere's substitution technique using numbers is done by exchanging letters with numbers, almost the same as the sliding code.

The vigenere password can be written mathematically, as with the description of vigenere above which uses addition and modulus.

Encryption Formula:
$Ci = (Pi + Ki) \bmod 26$

Decryption Formula:
$Pi = (Ci - Ki) \bmod 26$

Explaination:
Ci = decimal value of (a = 0) i-encode character
Pi = decimal value of the i-message character
Ki = decimal value of the i-key character

3. Result and Discussion

The system was built using Sharp Develop 4.4. with the programming language is C#. This system is tested with personal computer with 1.0 GHz processor specification AMD C-70 APU, 2 GB Memory.

The result of the average test of process time in One Time PAd algorithm with the number of characters 10, 50 and 100 is 1 ms, 3 ms and 7,333 ms while the result of average test of process time on Vigenere algorithm with number of characters 10, 50 and 100 that is 48,667 ms, 75,333 ms and 132,333 ms. The results can be illustrated in a graph of figure 1.

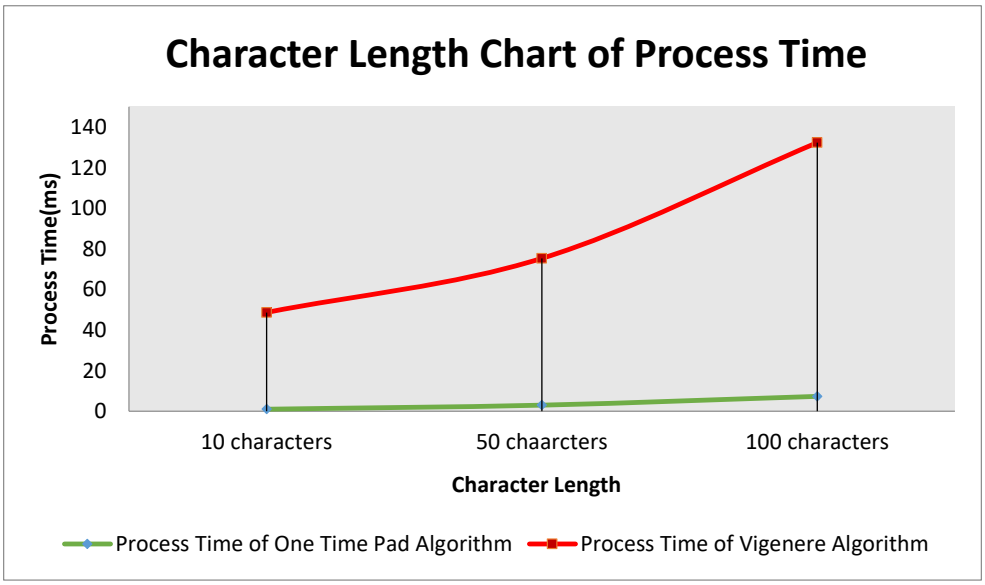


Figure 1. Graph of plaintext length against the process time of one time pad algorithm and vigenere algorithm

Figure 1 shows a graph of plaintext length for the process time of the One Time Pad Algorithm, and Vigenere algorithm, where the length of the plaintext is directly proportional to the processing time. The longer character will be processed, then the required process time will also be longer.

4. Conclusion

- The test results at the time of the process obtained that the algorithm process time is directly proportional to the length of the plaintext character. This means that the longer the plaintext used, the longer it will take for encryption and plaintext decryption.
- The results of the processing time One Time Pad algorithm and the Vigenere algorithm show that the One Time Pad algorithm processing time is faster than the Vigenere algorithm.
- Vigenere's encryption algorithm is sometimes shorter than One Time Pad encryption algorithm even though the plaintext is inputted the same thing.
- The combination of the One Time Pad and Vigenere algorithms in the super encryption scheme is successfully applied even when the decryption process has characters in the plaintext that are incompatible with the original but can still be understood by the meaning of the word.
- In the encryption process of the Vigenere algorithm if repeated encryption experiments using plaintext and the same key will result in different ciphertext.

5. References

[1] Goyal, Kashish & Kinger, Supriya. 2013. Modified Caesar Cipher for Better Security Enhancement. *International Journal of Computer Applications* **73(**3): 0975 –8887.
[2] Sadikin, R. 2012. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. Andi Offset: Yogyakarta.
[3] Ariyus, D. 2008. *Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi*. ANDI: Yogyakarta
[4] Mollin, R.A.2007.*An Introduction to Cryptography 2nd Ed*. Taylor &Francis Group: LLC. United State of America.
[5] Bruen, A. A., & Forcinito, M. A. (2011). *Cryptography, information theory, and error-correction: a handbook for the 21st century* (Vol. 68). John Wiley & Sons.
[6] Mushlih, Hijasma. 2012. Pembuatan Aplikasi Kripto sistem Menggunakan Metode Algoritma Vigenere Cipher. Skripsi. Amikom Yogyakarta.
[7] Anraeni, S., Herdianti & Mursyid. 2016. *Hybrid Methods of Ciphertext and RSA Cryptographic Algorithm Using Classical Vigenère. International Journal of Computing and Informatics (IJCANDI)* Vol. 1, No. 2. Sekolah Tinggi Ilmu Komputer Jayapura: Indonesia.