Multi-Cipher Single Message Encryption Algorithm

Mohammad Hjouj Btoush, Khalaf F. Khatatneh and Qutaiba A. Al-Talaq
Department of Computer Science
Prince Abdulah Bin Gazi Faculty for Information Technology
Al-Balqa' Applied University, Salt-Jordan

ABSTRACT
Different types of data are produced, stored, transmitted or exchanged, and in most of the cases the privacy of the data is a requirement; this issue enforces the inventing of a secure way to send the data using the encryption.
These days most of the encryption algorithms based on the idea of (Public - Private Key), so that the process of encryption uses a key known to everyone and the decryption process uses a different private key, such as the RSA.
The problem in these algorithms is the giving of the same cipher-text each time you encrypt a particular text using a specific key, which makes it easier to discover the original text by relating the encrypted text to a well-known decrypted text.
The main purpose of this research is to build a reliable, an efficient, and a more secure algorithm for encryption. This algorithm gives multiple ciphers for a specific message using the same key and produces the original message once we decrypt these ciphers; this will make the process of hacking by relating the cipher to the text so difficult.
This research paper will compare different algorithms with the new algorithm, and will demonstrate the implementation of an application that shows each one of these algorithms including the new one using a well-known programming language.

Keywords: Encryption, Decryption, RSA, DES, AES, Symmetric, Asymmetric

1 INTRODUCTION
1.1 Overview
With the popularization of the computer and the Internet fuelled by the need of information exchange; the need for communication media and strategy to transmit various type of information has appeared.

One of the biggest media which is used to transmit the information is the internet; the information is commonly transmitted via the Internet. However, the important information –which is defined as the data after processing and also could be defined as knowledge when used to understand or doing something- in transmission, is easily intercepted by unknown persons or hackers on the Internet. Therefore, the problem of information security becomes more and more important especially when it comes to data transmit important data.
The internet is a commonly used media to transmit the information in an easy and secure way; communication starts from point to point then it is developed and expanded to reach what we witness now of becoming an essential part of our life, the internet origins dated back to the 1969 as project for the US Defense Department for wartime digital communications, at that time the telephone system was mainly the only communication system in use, The Defense Advanced Research Projects Agency (DARPA) launched the DARPA Internet Program, which played a big rule in the academic and military research, it has progressed over the years reaching what we know today as the Internet in the middle of the 1990s[1].

To protect the important information and make it secure while it is transmitted over an insecure channel we use the Information hiding [2].
Having different types of information that is transmitted through the network especially when it comes to sensitive or confidential information is behind the need for safety and secure transmission for these information types; thus the need for encryption becomes an essential and crucial thing.

The encryption has been used for many years by many organizations and people such as: militaries, spies, and others to create secure information communication channel [3].

The different types of information and the level of the importance of such information create the need for different types of encryption that could efficiently handle the transmitted data.

In the computer science, Secure Transmission refers to the transfer of data such as confidential information over a secure channel [4][5]. Many secure transmission methods require a specific type of encryption.

Data encryption is a good method to protect data, till now, various encryption algorithms have existed and been widely used such as; (DES, RSA, AES etc.), most of which are used for text and binary data.

However, other encryption methods exist to encrypt other types of information (Images, Video …).

The wide use of digital images and videos in various applications brings serious attention to security and privacy issues today. In practical applications, for a video encryption algorithm, security, time efficiency, format compliance and compression friendliness are really important [6][7].

For the importance of encryption regarding the secure information transmission, many algorithms appeared to encrypt various types of information.

1.2 Research Question

This research aims to answer the following questions:

- Do the current encryption algorithms especially those that are popular have some problems?
- Can we generate variant cipher text for a plain text then find the original plain text from these ciphers?
- Does our proposed algorithm have some problems and is it applicable for variant types of information and languages?

1.3 Research Objectives

The main objectives of our research are to:

- Design a proposed algorithm based on a well-known algorithms to create variant encryptions for the same plain text.
- Design an algorithm which decrypts all these different ciphers to generate the original plain text.
- Compare the different existing encryption algorithms with this new algorithm

2 Procedure

2.1 Overview

With the popularization of the computer and the Internet fuelled by of the need of information exchange; the need for communication media and strategy to transmit various type of information has appeared.

To protect the important information and make it secure while it is transmitted over an insecure channel we use the Information hiding, Data encryption is a good method to protect data, till now, various encryption algorithms have existed and been widely used, for example; (DES, RSA, AES etc.); most of which are used for text and binary data.

Two main types of encryption exist: [8][9][10]

- Symmetric Key Ciphers
  The oldest and best-known technique that uses one key for encryption and decryption called secret key.
- Asymmetric Key Ciphers
  Using a pair of keys one for encryption (public key) and the other for decryption (private key). However, it is slower than symmetric encryption and it requires more processing power.

2.2 Problem Statement and Questions

The most commonly used encryption algorithms are RSA, DES, AES, etc[11].

Weather they are Symmetric or Asymmetric they always generate the same cipher text to the same plain text for the same keys.

The main aim of this research is to find a new algorithm which can generate different encryptions for the same plain text using the same key at different times and to find out a procedure that enables us to find the original plain text from these different ciphers.

2.3 Suggested Solution

Finding an algorithm that creates different ciphers for the same plain text with the same key can possibly be achieved by generating random numbers then try to hide the plain text inside this random string.

The main challenge, however; is to find a way to decrypt these ciphers in order to figure out the original plain text and this is what we are going to demonstrate in this research paper.

2.4 Design and Implementation

The main step is to write an abstract (theoretical) algorithm with some limitations then try to make it more complex to fix all the problems.

Then we try to make this algorithm work by writing a program that execute it and get a result from it.

First of all, this algorithm can operate on just the English alphabets (a - z). This limitation is behind the need for a good computer to run the algorithm with minimum requirements of 2.4 GHZ CPU, 1 GB Ram, a free storage of 20 MB and finally the .Net Framework 4.0.

The user enter his/her plain text to be encrypted, then a random cipher text can be generated, by taking the result cipher text and try to encrypt it, it will always give the same original text.

In this algorithm we used the Symmetric Key Cipher which needs one key for encryption and decryption; this key can be a random number between 1 and 9.

Once the user pushes the button to encrypt a specific plain text, a random function will generate random letters and put them in specific positions according to the used key.

The decryption will be done using the same key and will remove the added random numbers.

However, we noticed that the encryption operation may also hide the plain message inside the new generated string; though the algorithm is used only for English letters so far.

Below is a complete description of how the proposed algorithm works:

First, the secret key should be selected.

Then a specific cipher text should be entered and that should be one of the English Letters only.

Encryption of the plain text will be done as follows:

- Transfer the English letters cipher text to a string of corresponding numbers (a: 01, b: 02… z: 26).
- Then put a random number between one and nine before and after each number which accepts the division on the corresponding secret number (i.e. no remainder).
- Check the result string numbers as a pair; if a pair of numbers exists with a value greater than 26 then a zero should be added before and after the first digit in this pair.
- If an original zero exists with no additional zero before or after it then an additional zero should be added before and after this zero, this is to make sure that this zero will stay after the decryption operation and will not be considered as additional zero.
- Finally, the corresponding string of numbers will be taken as pairs then each pair will be changed to its corresponding letters according to the previously defined numbers-letters mapping. i.e. (a: 01, b: 02… z: 26).
- The final generated string of letter will represent the cipher text.

Decryption of the cipher text will be done as follows:

- Choose the same secret key which was used for the encryption operation.
- Parse the cipher text and change the letters to their corresponding numbers according to the previously

defined numbers-letters mapping (a: 01, b: 02… z: 26).

- Then, concatenate the generated numbers on one string.
- Parse this string to remove the additional zeros which can be found on the left and right of each number; else if it exists on one side then it is the original zero.
- The final string will be a string of the pair of numbers of the original string and the random added numbers according to the secret key.
- To remove the generated random numbers we will follow a specific procedure as follows:

Always remove the numbers before and after the second number.

1. If the secret key is one; then you should move three steps each time and take the corresponding number.
2. If the private key is not one, then you should move two steps, and you should take the first number at the first round and in the second round take a group of numbers less than the private key by one.

- Finally concatenate these numbers and transfer them to their corresponding letters by taking them as pairs using the previously defined numbers-letters mapping, i.e. (a: 01, b: 02… z: 26).

Examples:

Example 1: Choose a Private Key = 1, Plain Text = L (12).

Encryption:

12 ➔ X1XX2X (X: are the random generated numbers)
12 ➔ 212325 (No pair is greater than 26 then it will stay the same)
12 ➔ UWY (This is the cipher text for 'L').
Or 12 ➔ 311329 (the existing pairs are greater than 26, so add zeros before and after each pair. The first letter goes with the pair which is greater than 26)
12 ➔ 0301130209
12 ➔ CAMBI (This is the cipher text for 'L').

Decryption:

UWY ➔ 212325 (The corresponding numbers string)
We have Private Key = 1 then we should remove one of three steps starting from the number at second position.
212325 ➔ 1 (Then Remove three steps)
212325 ➔ 2 (End)
212325 ➔ 12 (concatenate the numbers)
12 ➔ 'L' (change the number to its corresponding letter - Plain Text)

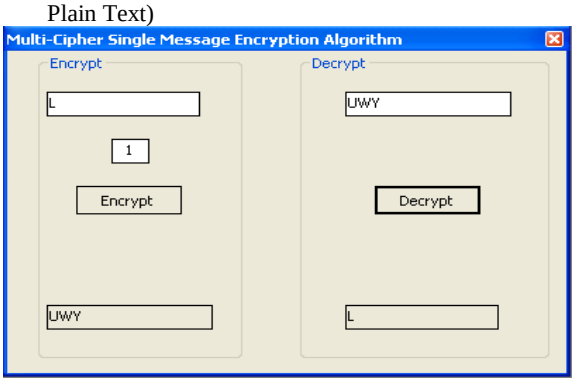

Figure 1: Multi-Cipher Encryption - Decryption (L)

CAMBI ➔ 0301130209
Remove the zeros before and after each number which have them before and after.
0301130209 ➔ 311329
We have Private Key = 1 then we should remove one of three steps starting from the number at second position.
311329 ➔ 1 (Then Remove three steps)
311329 ➔ 2 (End)
311329 ➔ 12 (concatenate the numbers)
12 ➔ 'L' (change the number to its Corresponding letter - Plain Text)

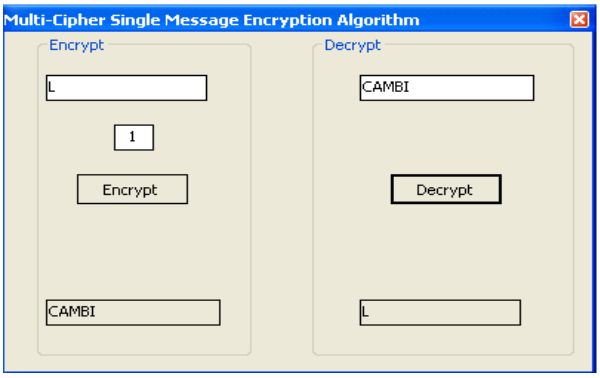

Figure 2: Multi-Cipher Encryption - Decryption (L)

Example 2: Choose a Private Key = 3,
Plain Text = LOG (121507).

Encryption:

121507 ➔ 6152185307
121507 ➔ 060105021805030007
121507 ➔ FAEBREC G

Decryption:

FAEBREC G ➔ 060105021805030007
060105021805030007 ➔ 6152185307
6152185307 ➔ 121507
121507 ➔ "LOG

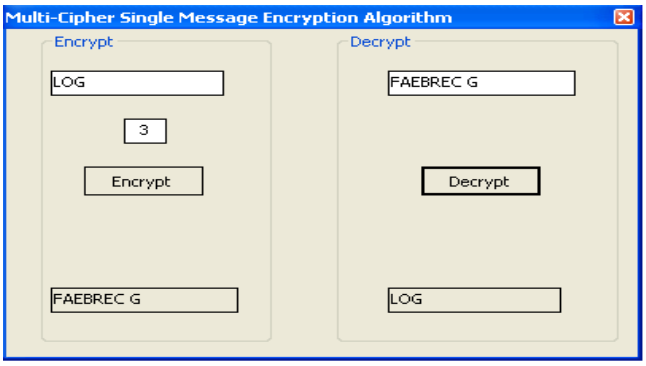

Figure 3: Multi-Cipher Encryption - Decryption (LOG)

3. CONCLUSION

Other encryption algorithms will always generate the same cipher for a specific plain text for a specific key at all times, this enables us to easily find the plain corresponding of a specific cipher for a specific key.
The ability to find an algorithm which can do encryption by generating different ciphers for a single plain text and do the opposite; the decryption of all these ciphers to get the original plain text is possible.
This algorithm works on the English letters only and can be expanded later to include more characters. Moreover, the using of symmetric key cipher with bulks will be more secure if it uses Asymmetric key cipher.
In comparison to other algorithms, our proposed algorithm is simpler and has a more reliable security because of it being a random one.

4. REFERENCES:

1. http://www.freesoft.org/CIE/Topics/57.htm
2. T.G. Gao, and Z.Q. Chen. (2008). "Image encryption based on a new total shuffling algorithm, Chaos, Solitons and Fractals," vol. 38, no.1, pp. 213-20.
3. Brendan M. Palfreyman (2009). Note, Lessons from the British and American Approaches to Compelled Decryption, 75 BROOK. L. REV. 345, 349-50 (describing historical uses of cryptography and the development of cryptography over time).
4. Shiguo Lian, Dimitris Kanellopoulos and Giancarlo Ruffo (2009). "Recent Advances in Multimedia Information System Security," International Journal of Computing and Informatics, Vol. 33, No.1, pp. 3-24.
5. Menezes, A., P. Van Oorschot and S. Vanstone (1996). Handbook of Applied Cryptography, CRC Press, pp.4-15, 516.
6. Fred Cohen (1995). "A Short History of Cryptography" Guy E. Blelloch (2000).
7. Goldwasser S. and Bellare M., A.(2001), "Lecture Notes on Cryptography", Cambridge, Massachusetts.
8. Carter B. and Magoc T., S.(2007), "Classical Ciphers and Cryptanalysis", Technical Report (2007).
9. Meyer P., (1997), "An Introduction to the Use of Encryption", http://www.hermetic.ch/crypto/intro.htm
10. Adleman L., Rivest R., Shamir A., and Williamson M., (2000), "Public Key Cryptography (PKC) History", http://www.livinginternet.com/i/is_crypt_pkc_inv.htm
11. Lenstra K. A., (2001), "*Unbelievable Security Matching AES security using public key systems*", 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology