Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 7, Issue, 12, pp.23610-23612, December, 2015

INTERNATIONAL JOURNAL
OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

NEW ALGORITHM FOR ENCRYPTION BASED ON SUBSTITUTION CIPHER AND TRANSPOSITION CIPHER

*Orooba Ismaeel Ibraheem Al-Farraji

Department of Computer Science, Al-Technology University, Iraq

ARTICLE INFO

Article History:
Received 15th September, 2015
Received in revised form
27th October, 2015
Accepted 29th November, 2015
Published online 21st December, 2015

Key words:

Cryptography,
Substitution cipher,
Transposition cipher,
Private key.

ABSTRACT

The new algorithm based on substitution cipher and transposition cipher, we replace the plaintext by another characters but in new method based on delete some bits from plaintext after convert it in binary code and put this bits in another place in plain text And traced back to the text, the algorithm is simple and use two keys.

Citation: Orooba Ismaeel Ibraheem Al-Farraji, 2015. "New Algorithm for Encryption Based on Substitution Cipher and Transposition Cipher", *International Journal of Current Research*, 7, (12), 23610-23612.

INTRODUCTION

Cryptography involves creating written or generated codes that allows information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without anyone decoding it back into a readable format, thus compromising the data (Buchmann A. Johannes, 2001). Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored. Cryptography also aids in non-repudiation. This means that neither the creator nor the receiver of the information may claim they did not create or receive it (Paine. Thomas, 2001).

In cryptography, ciphertext or cyphertext is the result of encryption performed on plaintext using an algorithm, called a cipher (Boneh *et al*., 2006).

Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it (Zotos *et al*., 2005).

Decryption, the inverse of encryption, is the process of turning ciphertext into readable plaintext. Ciphertext is not to be confused with codetext because the latter is a result of a code, not a cipher (Keijo Ruohonen, 2014).

Common Cryptographic Algorithms

There are two basic kinds of encryption algorithms in use today:

- Private key cryptography, which uses the same key to encrypt and decrypt the message. This type is also known as *symmetric key* cryptography.
- Public key cryptography, which uses a *public key* to encrypt the message and a *private key* to decrypt it. The name public key comes from the fact that you can make the encryption key public without compromising the secrecy of the message or the decryption key. Public key systems are also known as asymmetric key cryptography (Ian Curry, 2001).

Substitution Cipher

Simple Substitution Ciphers Substitution is one of the easiest ways of "hiding" text – you simply replace one letter with another letter or perhaps a number or symbol. Sounds simple, but the catch is in how you replace each letter.

Corresponding author: Orooba Ismaeel Ibraheem Al-Farraji,
Department of Computer Science, Al-Technology University, Iraq.

It has to be done in a way that lets both the sender and the receiver encipher / decipher accurately (quickly would be nice to, but accuracy is more important). In other words, both sides must know the algorithm (a fancy way of saying "process") for replacing each letter.

As a practical matter, encoding / decoding algorithms that involve remembering huge charts or going through 20 separate steps are no good – people just won't do it. So the method has to be easy to use (Chris Spackman, 2003). Substitution cipher, data encryption scheme in which units of the plaintext (generally single letters or pairs of letters of ordinary text) are replaced with other symbols or groups of symbols (Gustavus J. Simmons, 2015).

Transposition Cipher

transposition systems, the plaintext is left unchanged but re-ordered in such a way that if an unintended recipient should get the message and does not know the decryption key, the plaintext would remain unreadable. There is virtually no limit to the number of ways plaintext can be transposed (Salomon and David, 2005).

The New Algorithm

The new algorithm consider symmetric key cryptography and mixing between Substitution Cipher and Transposition Cipher in new technique that make the algorithm more security and difficult to attack.

The Step of Algorithm

Algorithm to encrypt Text

Step 1- Input the text that we want to encryption.

Step 2-Delete all space in text.

Step 3-Convert text to Ascii and then convert to Binary code.

Step 4-Every six bit delete two bit and save in another file call (withouttb) and after delete every two bits from file we store together in another file called (twob).

Step 5-We take the file of two bits (twob) and divided into three parts

Step 6-The first parts of three parts input in begin of the file (withouttb) and the second parts in middle of file (withouttb) and the third part in end the file (withouttb) and save the result in new file called "encrp-file"

Step 7-Convert binary code file after delete again to ascii code and then to string .

Step8- End

Example

We incrypt the text "College of medicine" in this Algorthim
College of medicine

a-Delete space

College of medicine

b-Convert to Ascii code then to binary code

C=67 o=111, l=108, l=108 , e=101, g=103, e=101, o=111, f=102, m=109, e=101, d=100, i=105, c=99, i=105, n= 110, e= 101

01000011011011110110110001101100011001010110011101
10010101101111011001100110110101100101011001000110
010101100011011001010110111001100101

c-Every six bit delete two bits

01000011011011110110110001101100011001010110011101
10010101101111011001100110110101100101011001000110
010101100011011001010110111001100101

d- Save the string after delete two bits in file (withouttb)

01000001101101101101101101100101100101100101101101
10010110110110010110010110010110000110010110110110
01 =102

e- Save delete two bits in another file (twob).

1111000001110111100101000111011001

f- Divided the file (twob) into three parts

111100000111
011110010100
0111011001

The first part input in begin the text (the file withouttb) and the two part in middle text (the file withouttb) the third part in end text (the file withouttb).

11110000011101000001101101101101101101100101100101
10010110110110111100101000010110110110010110010110
010110000110010110110110010111011001

g- Convert string from binary to Ascii then to string

11110000 01110100 00011011 01101101 10110110 01011001
01100101 10110110 11110010 10000101 10110110 01011001
01100101 10000110 01011011 01100101 11011001

240 116 27 109 182 89 101 182 242 133 182 89 101 134 91 101 217

240= _, 116=t, 27=Escap, 109=m 182=Ä , 89=Y 101 = e 182= Ä, 242= -133= á, 182 = Ä, 89=Y 101=e 134= a 91=[101= e 217=J

Plain Text= college of medicine

Cipher Text= _tmÄYeÄ-áÄYea[eJ

Algorithm to Decrypt Text

Step 1- Input the key 1 (length of twob) and key 2 (length of plaintext)

Step 2- Divided the key1 by 3 and save the result in BB

Step 3- Divided the plain text by 2 and save the result in CC

Step 4- Convert the ciphertext to Ascii code then to binary code

Step 5- Save the BB bits in begin of ciphertext in file 1 and save the (CC-BB) bits of ciphertext in file 2 and then save the BB bits from ciphertext in file 1 and (CC-BB) bits in file 2 and save the rest bits in file 1.

Step 6- Open new file and save the six bits from file 2 and then the two bits from file 1 and then the six bits from file 2 then the two bits from file 1 and so on until end of two files.

Step 7- Convert the new file to Ascii code then to string
Step8- End

The Keys of Algorithm

We use two keys in algorithm, the first key the number of bits that delete from plaintext. The second key length of plaintext

Conclusion

a- The algorithm is very simple and can run in all programming language.
b- It is very security and difficult to attack
c- We can increase from security by using steganography after cryptography.
d- We can use the algorithm with the long and short text.

REFERENCES

Berti, Hansche, Hare, 2003. *Official (ISC)² Guide to the CISSP Exam*. Auerbach Publications. p. 379. ISBN 0-8493-1707-X.

Boneh. Dan, Canetti. Ran, Halevi. Shai, Katz. Jonathan, “Chosen-Ciphertext Security from Identity-Based Encryption”, June 13, 2006.

Buchmann A. Johannes,” Introduction to Cryptography”, 2001

Chris Spackman, “An Introduction to Traditional Cryptography and Cryptanalysis for Amateurs”, August 2003. P. 4.

Gustavus J. Simmons , “Substitution cipher”, Encyclopedia Britannic Inc., 2015.

Ian Curry, “An Introduction to Cryptography and Digital Signatures”, Copyright 2001-2003 Entrust.

Keijo Ruohonen, “Mathematical Cryptology”, 2014, p. 1.

Paine. Thomas, “Social Insurance History”, Social Security website, www.ssa.gov

Salomon, David, “Coding for Data and Computer Communications”, 2005, P. 227-242.

Zotos. Kostas, Litke. andreas, “Cryptography and Encryption”, 2005.

****