ISSN NO. 2320-5407

Journal homepage:http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

A New Modified Cesar Cipher Cryptographic Method Along With Rail Fence to Encrypt Message

Fahad Naim Nife
Department of Mathematics and Computer Applications,Al-Muthanna University, Iraq

Manuscript Info *Abstract*

Manuscript History:

Received: 15 December 2014
Final Accepted: 26 January 2015
Published Online: February 2015

Key words:
Cesar Cipher, Rail Fence, Dynamic Key, Repetition exclusion, Cryptography,

Corresponding Author

FahadNaimNife

This paper presents a new cryptographic technique to prevent the repetitive terms in a message, when it is to be encrypted, so that it becomes almost impossible for a person to retrieve or predict the original message from the original message.In modern world, cryptography hackers try to break a code or cryptographic algorithm or try to retrieve the key, which is needed to encrypt a message, by analyzing the insertion or presence of repetitive characters in the message and encrypted message to find out the encryption algorithm or the key used for it. So it is must for a good encryption method to exclude the repetitive terms such that no trace of repetitions can be tracked down. For this reason we apply new cryptographic method that uses idea of dynamic key to exclude repetitive terms from a message, which is to be encrypted. In this method the repetitive characters are removed and there is no trace of any repetition in the message.The problem of distributing the secret key has been also overcome by adopting a new technique to hide the key inside the encrypted text in a nearly proposed way.

INTRODUCTION

Computer security is an important field of study for most day to day transactions. It arises when we turn on our cellular phones, check our voice mail and e-mail, use debit or cred it cards, order a pay per view movie, sign on to online video games, and even during visits to the doctor (Denis et al). For example we can assume the situation where a military commander is instructing his fellow comrades about an attack and the strategies used for the attack, but while the instructions are sent to the destination, the instructions get intercepted by enemy soldiers and they use the information for a counter-attack. This can be highly fatal and can cause too much destruction (Stallings at al, 2011).So, different cryptographic methods are used by different organizations and government institutions to protect their data online. But, cryptography hackers are always trying to break the cryptographic methods or retrieve keys by different means and one of such methods include the process of inclusion of repetitive texts or characters in a message and then encrypt them to study the cryptanalysis of the method and retrieve the key, which is needed for cryptographic method, or break the algorithm.This proposed algorithm is a cryptographic method to exclude the repetitive characters in a message to be encrypted and this technique is a type of symmetric key cryptography.

Cipher Systems

The process of encoding the plaintext into cipher text is called Encryption and reverse the process of decoding ciphers text to plaintext is called Decryption. This can be done by two techniques symmetric-key cryptography and

asymmetric key cryptography. Symmetric key cryptography involves the usage of the same key for encryption and decryption (Stallings et al, 2011), (Nath et al, 2010). But the Asymmetric key cryptography involves the usage of one key for encryption and another, different key for decryption. Secret key cryptography includes DES, AES, 3DES, IDEA, Blowfish algorithms etc. and public key cryptography includes RSA, Digital Signature and Message Digest algorithms (Singh et al, 2013), (Kahate, 2007).Symmetric key algorithms are well accepted in the modern communication network. The main advantage of symmetric key cryptography is that the key management is very simple. Only one key is used for both encryption as well as for decryption purpose. There are many methods of implementing symmetric key. In case of symmetric key method, the key should never be revealed / disclosed to the outside world or to other user and should be kept secure(Stallings at al, 2011).Classical encryption methods depend on two basic encryption method, namely Mono Alphabet and Poly Alphabet. In this research, we developed a hybrid encryption algorithm to overcome the weaknesses in both methods and employed the basic methods of themselves. The output ciphertext is characterized with the high security when it does not give the expected results using the basics to break the code. The problem of distributing the secret key has been also overcome by adopting a new technique to extract the key from the plaintext in a nearly proposed way.

Cipher Technique

The type of operations used for transforming plaintext to Ciphertext is based on two general principles: substitution (in which each element in the plaintext (bit, letter, group of bits or letters) is replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns), and transposition (does not replace the one alphabet with another like the substitution technique but perform the permutation on the plain text to convert it into cipher text)(Kahate, 2007). The fundamental requirement is that no information be lost (that is, that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions (Forouzan).Simple substitution and transposition ciphers individually do not provide a very high level of security. However, by combining these transformations it is possible to obtain strong ciphers.The Proposed algorithm is Product technique which adapt both substitution and transposition ciphers together by using new modified advanced Cesar cipher method by using dynamic key its value extracting from the plain text along with Rail Fence Cipher.

Proposed Encryption Process

The Proposed algorithm is also a symmetric key cryptographic method and can be used with other cryptographic method to make those encryption strong enough to be broken by hackers. In this paper the authors present the cryptographic technique , which is a both substitution and transposition cryptographic technique. First the message is divided into two equal parts (say LPT and RPT) and it is saved in a two metrics .Then the first Matrix which contain LPT will be the Key for the second matrix to get (RCT) , where this key will have changed value ,where its value depend on the position of the character and the ASCII of the character , after that, the result (RCT) will be the key for the first unchanged matrix (LPT) to get (LCT) . Then we apply a modified form of Rail Fence Cryptographic Method. In cryptography, a Caesar cipher, also known as a Caesar's cipher or the shift cipher or Caesar's code or Caesar shift, is one of the simplest and basic known encryption techniques. It is a type of replace cipher in which each letter in the plaintext is replaced by a letter with a fixed position separated by a numerical value used as a "key", but with this proposed system each letter in the plaintext is replaced by a letter with variable position separated by a unexpected value used as a " Dynamic key" .AS explained above we can see that the algorithm will go through two main operations are substitution followed by transposition .

1-Dynamic Key Generation

The first step of this algorithm is dividing the plaintext into two equal parts (Lets call LPT and RPT) , Then we will encrypt the LPT first followed by the RPT using new modified Cesar cipher , In tradition Cesar cipher the key value is fixed and is provided by the user but with this algorithm no need for any Key at all .We will extract the Key for RPT from the LPT and extract the Key for LPT from the RPT, where for each letter in the message will be encrypt by different key value , So for a message with a N length , there will be N different key value .The question is how we can generate this Key values ? The answer is , when we start with Encrypt the LPT and we start with the first character , the key value will be calculated from the following equation , The Position of the current character (in this case 1) multiplied by the ASCII of the character that be in the equivalent position of RPT , if the

value is greater than 256 then will take remaining of dividing that value by 256.Go on with this equation to calculate different key value for each character in LPT till the last character in LPT is encrypted to get LCT. After that we will start with RPT to encrypt it , also we start with the first character , the key value will be calculated from the following equation , The Position of the current character (in this case length of LPT plus one) multiplied by the ASCII of the character that be in the equivalent position of CPT , if the value is greater than 256 then we will take remaining of dividing that value by 256.Go on with this equation to calculate different key value for each character in LPT till the last character in LPT is encrypted to get RCT. Now on combine both RCT and followed by LCT to get one Ciphertext.

2-Apply Transposition Technique

Now we will Apply the Rail Fence Technique which is the simplest transposition cipher technique , in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. Here we will use a Rail Fence with depth of three rows .

The Proposed Encryption Algorithm :

1- Read the Plaintext.
2- Divide the Plaintext into two equal parts (LPT and RPT).
3- Start with the LPT by encrypt each character using the following equation :
   LCT =LPT +[(position of (LPT) * RPT) % N]
   Where N is the number of character in the used language .
4- When encryption of LPT finish , start with RPT.
5- Encrypt each character using the following equation :
   RCT =RPT +[(position of (RPT) * LCT) % N]
6- Combine the two parts (LCT and RCT).
7- Apply the technique of Rail Fence on the result of step 6, where the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows .

Decryption Process

The proposed encryption method can be reverse engineered to get back the original text (message) and thus decryption of the encrypted text can be executed. In case of decryption of Rail Fence process can be reversed, i.e. the Cipher text is divided into three equal parts, the new Cipher text by collecting one character from each part, After that the new advanced Cesar cipher method is executed in reverse direction, to get back the original text. Remember that we must divide the Cipher text that we get from decrypt by Rail Fence into two equals part (LCT and RCT) and then start with decrypting the RCT first with main formulae :
RPT =RCT -[(position of (LCT) * RCT) % N]
Now we take the result that we have get to decrypt the LPT using main formulae :
LPT =LCT -[(position of (RCT) * RPT) % N]
Then we combine the two parts together to get the original Plaintext.Note: If, ASCII value of text[i] < 0, then set text[i] = (text[i] Modulus 255) ‘i’ is the position of each character in the text and text[] is the message to be encrypted, where text[i] denotes each character of the text[] at position ‘i’.

The Proposed Decryption Algorithm :

1. Read the Ciphertext.
2. Decrypt the ciphertext with Rail Fence , by dividing it into two parts and then star reading one character from each part.
3. Divide the ciphertext into two equal parts (LCT and RCT).
4. Start with the RCT by decrypt each character using the following equation :
5. RPT =RCT -[(position of (LCT) * RCT) % N]
6. When decryption of RCT finish , start with LCT.

7. Decrypt each character using the following equation :
8. LPT =LCT -[(position of (RCT) * RPT) % N]
9. Combine the two parts (LCT and RCT) to get the Original message .

Spectral Analysis Of Frequency Of Characters

The classical cryptanalysis method is by detecting the frequency of characters in the encrypted message (Ciphertext) (Fiddler, 1998). The effectiveness of the proposed method can be checked by spectral analysis of the frequency of characters. Using this method we run many analysis and tested different strings as input and used various methods of cryptanalysis. To show the usefulness and integrity of this cryptographic module, we used spectral analysis of the frequency of characters.

Table (1) Encrypting Palindrome

message	Encrypted message
ffffffhhhhiihhhhffffff	Ï ž n 2 þ Ë & Â Ð ® š 6 Ê ˜ d H ê > Ø

In Fig (1) we show the spectral analysis of the string of'ffffffhhhhiihhhhffffff'.

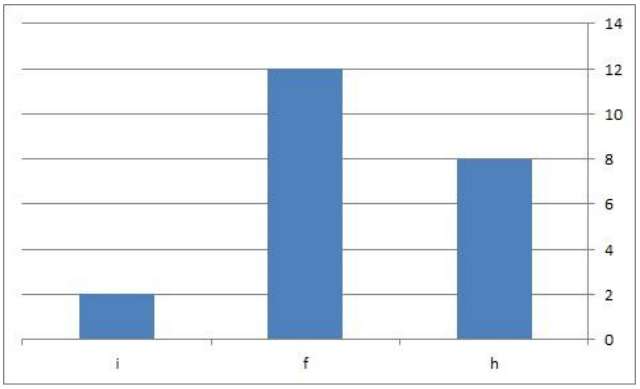

Figure (1) Spectral Analysis of frequency of characters of string 'ffffffhhhhiihhhhffffff'

We encrypted the string 'ffffffhhhhiihhhhffffff ', which is a palindrome, and as an output we got ' Ï ž n 2 þ Ë & Â Ð ® š 6 Ê ˜ d H ê > Ø', (shown in Table 1.1). Fig (2) shows the spectral analysis of the frequency of characters of the encrypted string. From the figures it is evident that this method is very effective to exclude repetition and provide no trace of that in the encrypted text.

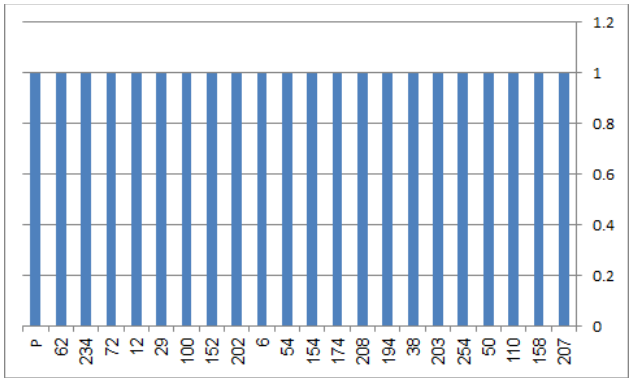

Figure (2) Spectral Analysis of Frequency of Characters of the Encrypted String of the Palindrome

General Cryptanalysis

The goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme, thus permitting its subversion or evasion(Fiddler,1998).If we analyze the proposed method, we can see that the use of dynamic Key in

the method have significantly increased the strength of encryption. Not only this, but the inclusion of substitution along with transposition has also increased the security of the cryptographic method. Although this technique is based on the Caesar Cipher method but modifying Caesar Cipher by introducing a strong cryptographic method. This helps the encrypted text to be almost impossible to be detected by including repetitive characters and it also makes the method strong against Differential Attack (Differential Cryptanalysis).

Results and Discussions

In the following table few results are given:

Table (2) Message Encrypted

Plaintext	Ciphertext
Computer security is an important field of study for most day to day transactions	² Æ ¾ ´ Z I P r ž ^ Ü ë , « š Å g M • — Ú ´ / % “ p Š m x ‰ ¼ ; @ Ì ¢ Ù © Á ‰ › > ÓE ª ² ô D ú ¾ Í ¤ # ð x ¡ x î Í ô 9 ›
Ffffffff	Ì ˜ b Ž 2 þ ’ V
&&aa&&	‡ Ó ` r }
‘ko{«’ after execution	ž ¤ S Ï Í ‡ ‡ « [ä Ê –¥ K 5
LLbbbbLL	® F È 6 ’ Â Ü

From table (2) , we can see that, all the repetitive terms are excluded from the encrypted text and it can never be figured out just from the encrypted text that there was any repetition in the text message. The proposed method is a provable good method to exclude repetitive terms.

Conclusion

This new cryptographic technique try to prevent the repetitive terms in a message, when it is to be encrypted, so that it becomes almost impossible for a person to retrieve or predict the original message from the original message.The problem of distributing the secret key has been also overcome by adopting a new technique by extract the key from the encrypted text in a nearly proposed way. The algorithm is get rid of the previous problems by making the key length variable as it depends on the length of the text ,any changes to the length of the text , the key will be changes

References

DenisT. S., JohnsonS., “Cryptography for Developer ” , Syngress Publishing, Inc., 800 Hingham Street , Rockland, MA 02370.

Stallings, **William**,(2011)"Cryptography and Network Security", principles and practice, Prentice Hall of India.

NathA., **Ghosh S.**, **MallikM. A.**, (2010) "Symmetric Key Cryptography using Random Key generator" , Proceedings of International conference on security and management(SAM’10”, USA).

SinghS., **Maakar S. K.**, **Kumar S.**, (2013) "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, 464-471 .

Kahate A., (2007) “Cryptography and Network Security ”, Tata Mcgraw Hill ,.

ForouzanB.A.,"Cryptography & Network Security ",Tata-Mcgraw Hill Book Company.

FiddlerM., (1998)"An Examination of Encryption Technology in Everyday use", Cecil Larry,PW-10 submission, matters of science.