International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 11, Issue 02 (February 2015), PP.38-43

A New Modified Version of Caser Cipher Algorithm

FAHAD NAIM NIFE
Dept. of MCA, Muthanna University, Iraq.

Abstract:- Computers uses a file which is a collection of information. The information is sensitive part of the organizations , and can be classified into simple, important, and critical information. Any loss or threat to information can prove to be great loss to the organization as well to people. The most important goal for designing any encryption algorithm is the security against unauthorized attacks. This paper introduces a new method to enhance the performance of the (Cesar Cipher algorithm). This is done by replacing the single key (Offsite) that used by the standard algorithm with dynamic key his value is changed for each letter depending on its position and the value of the previous letter. This replacement adds a new level of protection strength and more robustness against breaking methods. One more powerful technique added by the proposed algorithm is repeat the encryption for the entered text several times**.**

Keywords:- Caser Cipher, Dynamic Key, Cycle Technique, Encryption, Decryption.

I. INTRODUCTION

Information Security has become a very critical aspect of modern computing systems. With the global acceptance of the Internet, virtually every computer in the world today is connected to every other. While this has created tremendous productivity and unprecedented opportunities in the world we live in, it has also created new risks for the users of these computers. The users, business and organization worldwide have to live with a constant threat from hackers and attackers, who use a variety of techniques and tools in order to break into computer systems, steal information, change data and havoc[1]. Cryptography plays a very vital role in keeping the message safe as the data is in transit[2]. It ensures that the message being sent at one end remains confidential and should be received only by the intended receiver at the other end[3][10]. Cryptography converts the original message to non-readable format. The people who are unauthorized to read the message try to break the non-readable message but it is hard to do it so. The authorized person has the capability to convert the non-readable message to readable one. The original message or the actual message that the person wishes to communicate with the other is defined as Plaintext see Fig. 1.The message that cannot be understood by anyone or meaningless message is what we call as Ciphertext. Encryption is the process of converting plaintext into cipher text with a key. A Key is a numeric or alpha numeric text or may be a special symbol [4]. A decryption is a reverse process of encryption in which original message is retrieved from the ciphertext [5][12].

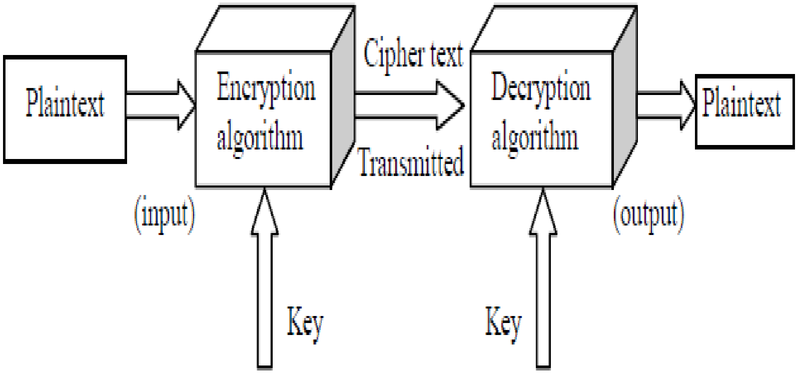

Fig. 1: Encryption/Decryption process

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.

II. ALGORITHM USED IN THE PRESENT WORK

A- Encryption Process

In this method we develop an advanced form of Caesar Cipher 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[6].It is a type of replacement 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"[7][11].

But, in this method, any character (ASCII value 0-255) are not separated by a fixed numerical value, in fact it is a variable numerical value, which is dependent on the position of the letter to be encrypted multiplied by the ASCII code of the previous letter. In the present method, the user not need to enters a secret key, where the key will be generated by the algorithm, which is calculated for each individual character, see Fig 2.

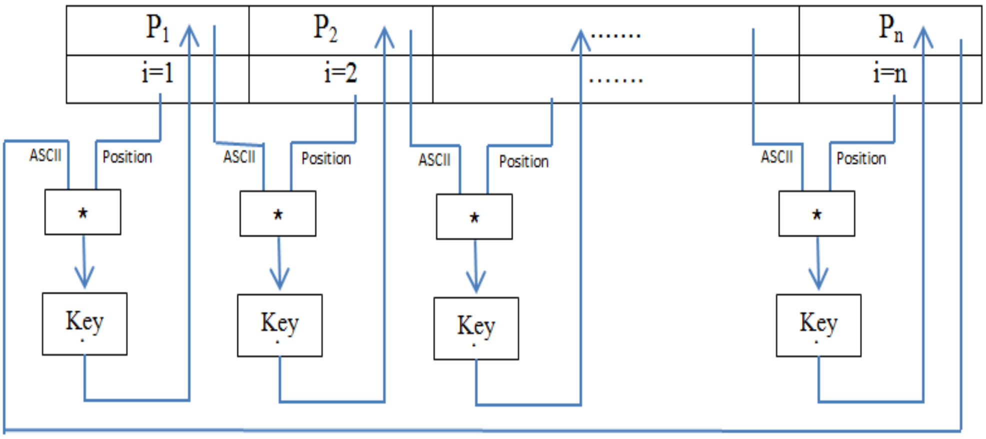

Fig. 2: The process of encryption for proposed algorithm

The proposed algorithm start with the second character of Plaintext to encrypt it , so it will calculate the Key by multiplying i by the ASCII code of the previous character, where 'i' is the position of the character to be encrypted in the plaintext, starting from position '1' as the starting position, this key will ensure that the value of key is changed dynamically to give key with different value for each letter. Now we apply the Caser cipher algorithm : C=(P + K) % 255.[1] After then, the algorithm will go to the next character and do same operation and so on. When whole the Plaintext encrypted, the algorithm will encrypt the first character, but there is no previous character to use, so the algorithm will take the ASCII code of the last encrypted character in the text, this will give a cycle form for standard Caesar Cipher .This algorithm will repeated for N times, where N is the length of Plaintext Mod 26 which will give more strong for the algorithm.

The Proposed Encryption Algorithm:

```
1- Read the Plaintext.
2- Calculate N number that is (the number of characters in the plain text Mod 26) .
3- Do step 4 for N times :
4- For each Plaintext letter P :
     A. Calculate K from:
          $K = \begin{cases} (i * P^{:}_{i-1}) & if\,(i > 1) \\ (i * C^{:}_{N}) & if\,(i = 1) \end{cases}$
          i : is the position of the letter to be encrypted.
     B. substitute the Ciphertext letter C as  [ C= ( P + K) Mod 255].
```

B- Decryption Process

For decryption we use reverse process to get back the original plaintext. During decryption again the user do not need to enter or provide any secret key, and now we will describe in detail the decryption procedure. At the first of all we calculate the N value which is the modulus of dividing the length of ciphertext by 26, this value will decide the number of rounds we will decrypt the ciphertext. The proposed decryption process will start with the first character of the Ciphertext and will calculate Key for it , this key will calculated by multiplying ‘i’ by the ASCII code of the last character in the ciphertext, where ‘i’ is the position of the character to be decrypted in the ciphertext, starting from position ‘1’ as the starting position. Now we apply the Caser cipher decryption algorithm : C=(P - K) % 255 [4].

After that, the algorithm will go to the next character and do same operation, where the Key will calculated by multiplying i by the ASCII code of the previous character, and so on.

The Proposed Decryption Algorithm:

```
1- Read the Ciphertext.
2- Calculate N number that is (the number of characters in the plain text Mod 26) .
3- Do step 4 for N times :
4- For each Ciphertext letter P :
     A. Calculate K from:
          $K = \begin{cases} (i * P_{i-1}) & if\ (i > 1) \\ (i * C_N) & if\ (i = 1) \end{cases}$
          i : is the position of the letter to be encrypted.
     B. substitute the Ciphertext letter C as   [ C= (P-K) Mod 255].
```

III. RESULT AND DISCUSSIONS

All By applying the proposed algorithm on some texts which selected randomly we will get the following results, see table I below:

Table I. Message Encrypted

Plaintext	**Ciphertext**
Multiple encryption is a technique in which an encryption algorithm is used multiple times In the first instance plaintext is converted to ciphertext using the encryption algorithm This ciphertext is then used as input and the algorithm is applied again This process may be repeated through any number of stages Triple DES makes use of three stages of the DES algorithm, using a total of two or three distinct keys	w u Ë ‰ ¦ ö □ Ý » ' m o ñ „ - ™ É Ô Í □ § Ž _ Ç ó è • ‘ & q “ □ w Ê = ð Ù ý ç Ô ¥ □ Ì ¥ □ ù q J O - R G 7 Á ñ ©] b , E Q — í µ k ä Ã ™ D í Z š í Ñ ª / • 2 µ / b Ò (• t ¹ o - 8 a ˜ û X Ù ¬ ÷ u Å * J é æ r t Õ % ² ¡
aaaaabbbbbb	W) Ü Ñ v & l Â 4 j ð M ó
aaaaabbbbbbaaaaa	, í (□ f Æ Ì Â 4 j ð ¡ Ž % Œ ! > f
yyyy	4 ? 6 Q
yyyyy	^ i ´ I æ

From table I , we can see that, each letter in the plaintext is replaced by a letter with a variable position separated by a numerical variable value, where there is no relation between the key used for the first key as example and the key used for any letter within the plaintext, this will does not give any track of the plaintext for the attackers, moreover 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. We can notice from encrypt the text "yyyy" which give "4 ? 6 Q "and the text "yyyyy" which give " ^ i ´ I æ " that is add even one more character to the original plaintext will change the entire ciphertext, because of adding one character to the plaintext will change the Value of N and the number of loops in the algorithm.

IV. SPECTRAL ANALYSIS OF FREQUECY OF CHARACTERS

To test the effectiveness of the proposed algorithm we detect the frequency of characters in the encrypted text (message) [8], where it is considered one of the classical cryptanalysis method. Using this proposed algorithm, we ran 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. First, as a test case we chose, a Plaintext consists of 100 Letter (A) and used this method to encrypt the data. Fig. 3 shows the spectral analysis of frequency of character A and Fig. 4 shows the spectral analysis of frequency of characters of the encrypted data.

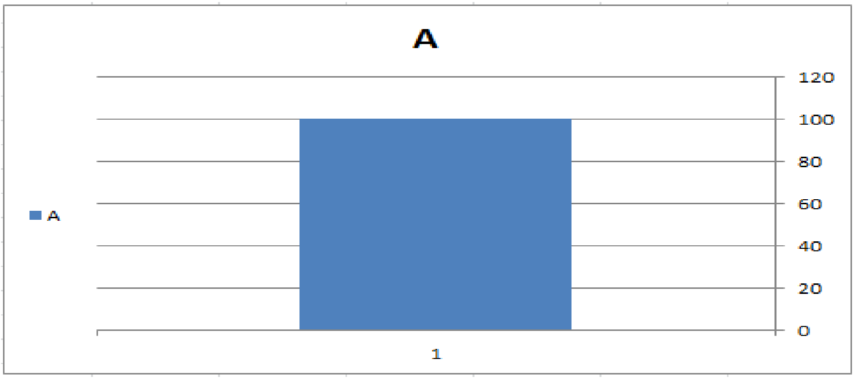

Fig 3: Spectral Analysis of Frequency of Character A

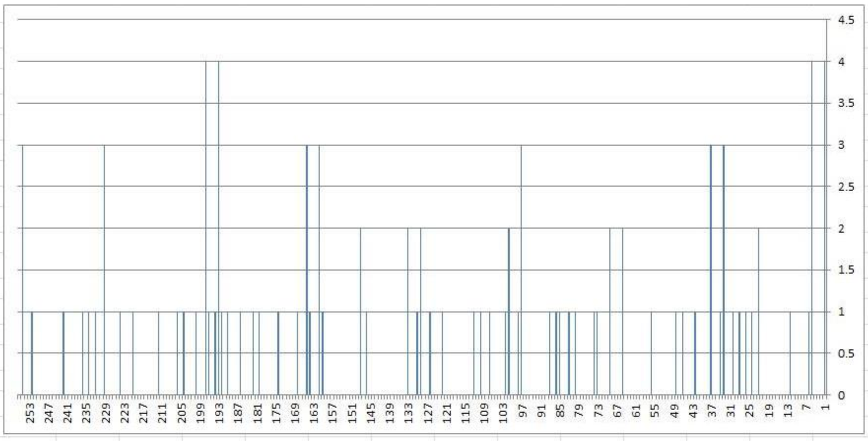

Fig 4: Spectral Analysis of Frequency of Characters of Encrypted data of 512 ASCII value (A)

Another test case we chose a random Plaintext. The spectral analysis of the frequency of characters of the plaintext is shown in Fig. 5 and Fig. 6 shows the spectral analysis of frequency of characters of encrypted text.

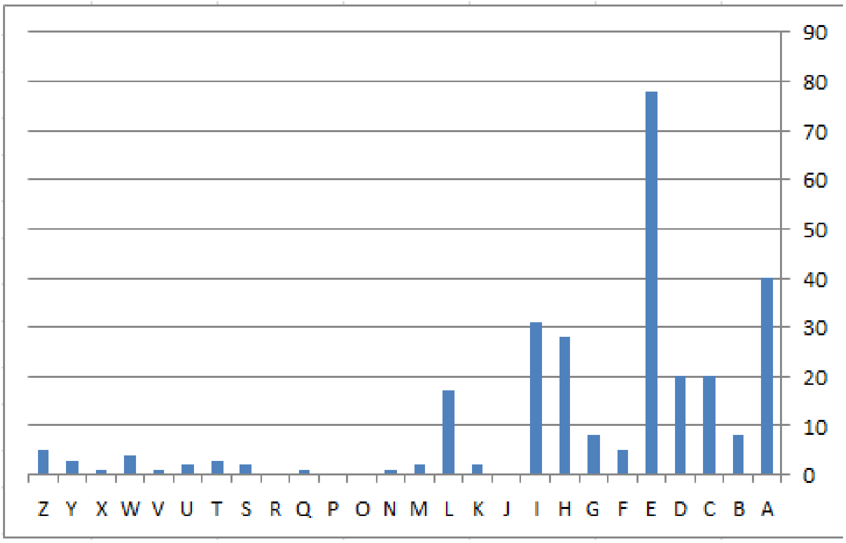

Fig 5: Spectral Analysis of Frequency of Characters of 1024 ASCII Value(1)

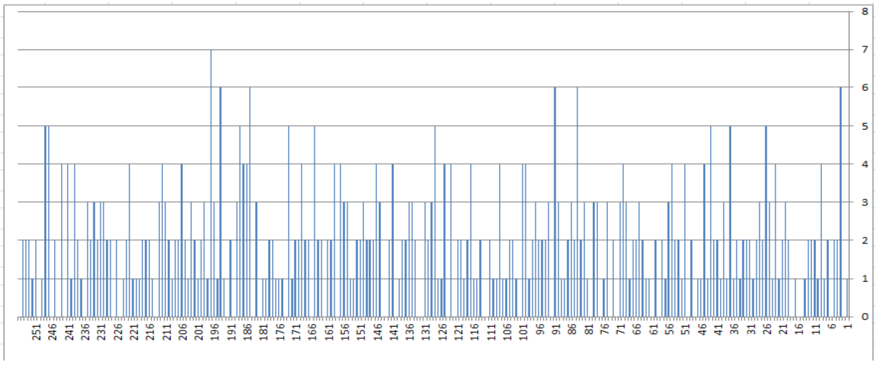

Fig. 6: Spectral Analysis of Frequency of Characters of Encrypted data of 512 ASCII value (A)

Thus from the above spectral analysis it is evident that the method, used here is very effective and there is no trace of any pattern in the encryption technique. Since this cryptographic technique uses dynamic key that its value changed for each character ,and apply the encryption for several times depending on the Plaintext length, for this reason, the method used here is unique and almost unbreakable because there is no trace of any pattern. And this method is also effective against both Differential Cryptanalysis (Differential Attack) and Brute-Force Attack.

V. GENERAL ANALYSIS

The main goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme[9]. Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme[4]• Cryptanalysis: rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. • Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. The most difficult problem is presented when all that is available is the ciphertext only. In some cases, not even the encryption algorithm is known, but in general, we can assume that the opponent does know the algorithm used for encryption. One possible attack under these circumstances is the brute-force approach of trying all possible keys. If the key space is very large, this becomes impractical.

So, when we analyse the proposed method, we can see that the use of dynamic Key in the method have significantly increased the strength of encryption, where this method will provide key with size is the same size of Plaintext. Not only this, the technique of repetition of the encryption for N times will give more powerful to 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.

VI. CONCLUSIONS

The proposed cryptographic algorithm try to overcome the problem of "key agreement" or "Key distribution" in traditional symmetric key cryptography by extracting the key from the Plaintext itself. The weakness of the standard Caser cipher algorithm, where any character (ASCII value 0-255) are separated by a fixed numerical value, are solved where a variable numerical value, which is dependent on the position of the letter to be encrypted and the ASCII code of the previous letter in the Plaintext are used, any changes to the length of the text , the key will be changes.

REFERENCES

[1]. **A. Kahate**, “Cryptography and Network Security ” 2nd Ed., Tata Mcgraw Hill, India, 2007 .

[2]. **T. S. Denis, And S. Johnson**, “Cryptography for Developer ”, Syngress Publishing, Inc., 800 Hingham Street , Rockland, MA 02370, 2007.

[3]. **D. Salama, H. Mohamed, and, M. Mohamed,** "Performance Evaluation of Symmetric Encryption Algorithms", International Journal of Computer Science and Network Security, Vol.8 No.12,pp. 280-286, Dec. 2008.

[4]. **Stallings**, And **William**, "Cryptography and Network Security", principles and practice , 5th Ed., Prentice Hall of India, 2011.

[5]. **M. Agrawal, P. Mishra**, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm", International Journal of Engineering and Advanced Technology, ISSN: 2249 – 8958, Vol.1, Issue 6, pp. 79-83, Aug. 2012.

[6]. **S. Dey, J. Nath, A. Nath,** "An Integrated Symmetric Key Cryptographic Method–Amalgamation of TTJSA Algorithm , Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm", I.J. Modern Education and Computer Science, 2012, 5, 1-9, Published Online June 2012.

[7]. **G. Singh, A. K. Singla, K.S. Sandha,** "Performance Evaluation of Symmetric Cryptography Algorithms", International Journal of Electronics & Communication Technology, Vol. 2, Issue 3, pp. 144-146, Sept. 2011.

[8]. **S. Kruti, B. Gambhava,** "New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering, ISSN: 2231-2307, Vol. 2, Issue1,pp. 322-325, March 2012.

[9]. **G. Suman, Ch. Krishna**, "Improved Cryptosystem Using SDES Algorithm with Substitution Ciphers", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 3, Issue 7, Jul. 2013.

[10]. **A. Patil, R. Goudar,** "A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices " , International Journal Of Scientific & Technology Research, ISSN 2277-8616 , Vol. 2, Issue 8, pp. 61-65, Aug. 2013.

[11]. **A. Nath**, **S. Ghosh**, And **M. A. Mallik**, "Symmetric Key Cryptography using Random Key generator", “Proceedings of International conference on security and management(SAM’10” held at Las Vegas, USA Jull 12-15, 2010), P-Vol-2, 239-244(2010).

[12]. **S. Singh**, **S. K. Maakar**, And **S. Kumar**, "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 6, pp. 464-471, Jun. 2013 .