ISSN:0975-9646

Prachi Patni/ (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) , 2013, 954-959

A Poly-alphabetic Approach to Caesar Cipher Algorithm

Prachi Patni

[#]*Research Scholar, Computer science and Engineering Department,*

Government College of Engineering, Aurangabad [Autonomous]
Station Road, Aurangabad, Maharashtra, India.

***Abstract* -With the exponential growth of internet and network applications such as e-commerce, the demand for data security increasing than ever before. Encryption algorithms play an important role in information security systems**

In this paper, author has proposed some modification traditional Caesar cipher. Classical Caesar cipher is mono-alphabetic and has a constant key length throughout the text file to be encrypted. Once the attacker gets the key of Caesar cipher it can be broken easily. This paper proposes some modification to overcome this drawback of Caesar cipher. The proposed algorithm uses variable key for each character. Using proposed method the plain text is encrypted in such a way that it becomes difficult to decrypt. The plain text message is converted to the encrypted text using a modified Caesar cipher which uses poly-alphabetic cipher technique. The encryption is done using variable length key which depends on the string length, place of character and time of file.

At the receiver end, the time will be given with name of file and if the receiver has appropriate decryption key, he can generate the text message similar to the original message.

This paper is organized into three section I section is introduction which gives brief information about cryptology and its various types, attacks on cryptography etc. Section II is literature survey which includes related work in corresponding topic. Section III contain proposed algorithm. Section IV conclusion.

General Terms-Information Security

Keywords-Cryptography, Plaintext, Cipher text, Key, Caesar Cipher

I. INTRODUCTION

In today's world, it is impossible to imagine without web or internet. This modern era is dominated by paperless transactions in offices by means of use of E-mail messages, E-cash transactions, etc. Due to this there is a great need of interchanging of data through online means. In various business and commercial sectors, there may be confidential information like banking transactions, credit information , government information, confidential information is transferred over web using E-mails, social network etc. To protect this type of confidential information from unauthorized discloser, there is a great need of security methods. So there is a need to develop a scheme that assures to protect the information from the attacker. One of the methods to protect online confidential data from unauthorized disclosure is to convert the online data to non-readable format for human being.

Cryptology is at the heart of providing such guarantee. The word Cryptology has existed for more than 2000 years. The word cryptology is inherited from two Greek words: kryptos, which means "secret or hidden" and logos, which means "description". Cryptology encompasses two competing skills – concealment and solution. The concealment portion of cryptology is called cryptography. The purpose of cryptography is to render a message incomprehensible to the unauthorized reader. Cryptography is often called "code making." The solution portion of cryptology is called cryptanalysis. Cryptanalysis is often called "code breaking" [17].

Cryptography is the science of building new powerful and efficient encryption and decryption methods. It deals with the techniques for conveying information securely. The basic aim of cryptography is to allow the intended recipients of a message to receive the message properly while preventing eavesdroppers from understanding the message. Cryptography ensures that the message being sent at one end remains confidential and should be received only by the intended receiver at the other end. Cryptography converts the original message in to non- readable format and sends the message over an unshielded channel. The people who are not authorized to read the message try to break the non-readable message but it is hard to do so. The authorized person has the capability or authority to convert the non-readable message to readable one [12]. There are two techniques for converting data into non readable form:[8]

1. Transposition technique
2. Substitution technique

The cryptography is divided into two main categories depending on the type of security keys used to encrypt/decrypt the plaintext. These two categories are: Asymmetric and Symmetric encryption techniques.

i) *Symmetric Encryption*: In symmetric key cryptography same secret key is used for encryption and decryption. The encryption algorithm produces the key and then sends it to receiver section where decryption takes place. It is much effective and faster than asymmetrical key cryptography [11]. Figure 2 shows working of symmetrical key cryptography.

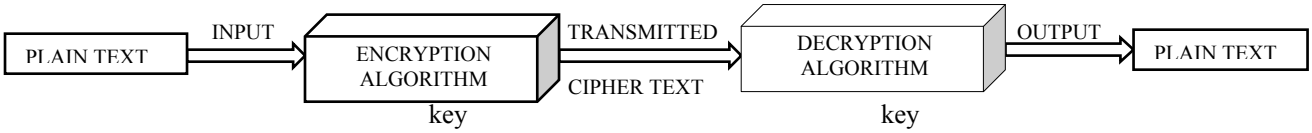

FIGURE 1: Encryption/Decryption process

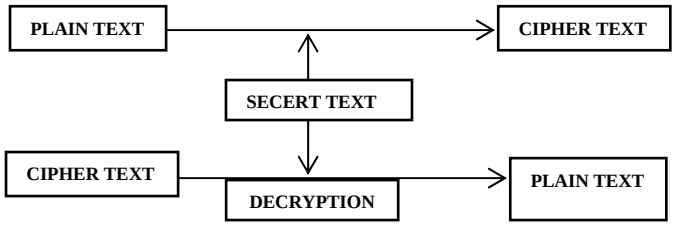

FIGURE 2 shows working of symmetric key algorithm

ii) *Asymmetric Encryption*: Asymmetric key cryptography is also known as public key cryptography. It uses two keys: public key and private key. Public key is known to the public and is used for encryption. Private key is known only to the user of that key and is used for decryption. The public and the private keys are correlated to each other by any mathematical means[11]. Figure3 shows working of asymmetrical key cryptography.

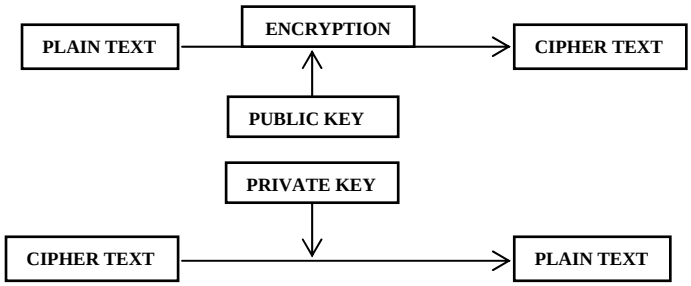

FIGURE 3 shows working of asymmetrical key algorithm

There are various types of cryptographic attacks in which few are given: [18]

i) Known Plaintext and Ciphertext-Only Attacks: A known plaintext attack is an attack in which a cryptanalyst has access to a plaintext and the corresponding ciphertext and seeks to discover a relation between them. A cipher text-only attack is an attack where a cryptanalyst has access to a ciphertext but does not have access to corresponding plaintext.

ii) Chosen Plaintext and Chosen Ciphertext Attacks: This is an attack where a cryptanalyst can encrypt a plaintext of his choice and then study the resulting ciphertext. This is most common against asymmetric cryptography, where a cryptanalyst has acquired a public key. A chosen ciphertext attack is an attack where a cryptanalyst chooses a ciphertext and attempts to find a matching plaintext.

iii) Adaptive Chosen Plaintext and Adaptive Chosen Ciphertext Attacks: In both adaptive attacks, a cryptanalyst chooses further plaintexts or ciphertexts (adapts the attack) based on previous results.

iv) Brute-force attack: A brute force attack systematically attempts every possible key. It is most often occurs in a known plaintext or cipher text-only attack.

At the end of decryption, the input cipher text is passed through the decryption algorithm which decrypts the cipher text using the same key as that of encryption. Finally we get the original plaintext message.

a. *Terminology used in cryptography*:[2]

i) *Plain Text*: It is the original message or the actual confidential message which person wishes to send to other party.

ii) *Cipher Text*: It is the output of encryption algorithm. Cipher text message cannot be understood by anyone or intruder because of in non-readable format.

iii) *Encryption Algorithm*: It is the process of converting plaintext message into cipher text with a use of key.

iv) *Key*: This is also given as a input to encryption algorithm It may be numeric or alpha numeric text or may be a special symbol.

v) *Decryption Algorithm*: It is a reverse method of encryption algorithm. In this the original message is retrieved from the cipher text. Encryption algorithm takes place at the sender end and Decryption algorithm takes place at the receiver end.

b. Goals of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non - alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography [13].

i) AUTHENTICATION (Handbook of Applied Cryptography):

- It should be possible for the recipient of a message to make sure of its origin.
- An intruder should not be able to pretend as someone else.

ii) INTEGRITY (Handbook of Applied Cryptography):

- It should be possible for the recipient of a message to verify that the message has not been modified by an intruder.
- An intruder should not be able to switch a false message for a legitimate one.

iii) *NON-REPUDIATION* (Handbook of Applied Cryptography):
- The person who sends the message should not be able to falsely deny later that he/she sent a message.

iv) CONFIDENTIALITY (ISO-17799):
- It ensures that information can only be accessed by those who have permission to access the message.

c. *Types of cryptography*[15]

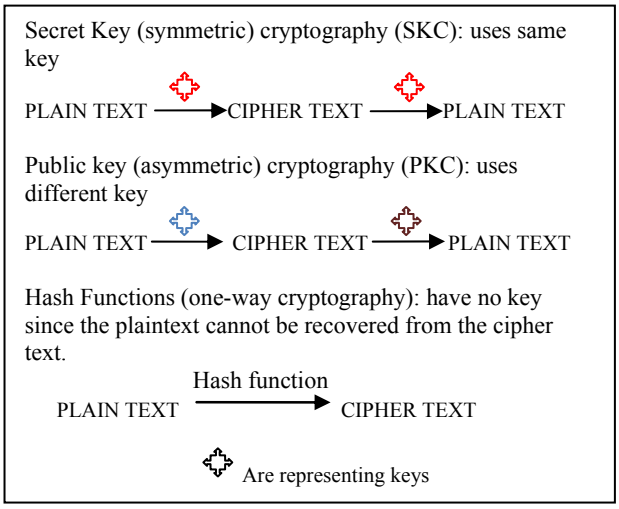

FIGURE 4: Three types of cryptography: secret key, public key, and hash functions

i) *Secret key cryptography (SKC):* It uses single key for both encryption and decryption. SKC algorithms that are in use today
- Data Encryption Standards(DES)
- Advanced Encryption Standards(AES)
- Blowfish etc.

ii) *Public key cryptography (PKC):* It uses one key for encryption and another key for decryption. PKC algorithm that are in use today for key exchange or digital signatures include
- RSA
- Diffie-Hellman
- Digital Signature Algorithm (DSA) etc.

iii) *Hash Functions:* They are the algorithms that in some sense uses no key but use a mathematical transformation to irreversibly "encrypt" information. Hash algorithms that are in common use today include:
- Message Digest (MD) algorithms
- Whirlpool
- Tiger

d. Caesar cipher

Plaintext letters: zyxwvutsrqponmlkjihgfedcba
Ciphertext letters:
SKENHCOZMPFJKRTYFMSMALCBTU

Consider an example; in this a simple plaintext is given with corresponding key. If we want to remember the key it is not possible, so there is another option of writing the key somewhere but it could be problematic for example key might be lost or stolen. It is sensible to have a key that need not be written down [17]. Therefore various algorithms were proposed to solve this problem. Caesar cipher is one of them. It is also known as shift cipher, Caesar's code or Caesar shift. It is one of the simplest and most widely known classical encryption techniques. It is an example of a substitution cipher method [16]. It was used by Julius Caesar to communicate with his army. Caesar is considered to be first person who had employed encryption for the sake of securing messages. It was decided by Caesar that his standard algorithm would be shifting each letter three places left the alphabet in the message, and so he informed all of his generals of his decision, and then he send them secured messages [14]. One of the strengths of the Caesar cipher is its ease of use and this ease of use would be important for Caesar since his soldiers were likely uneducated and not capable of using a complicated coding system.

It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of three, A would become D, B would be replaced by E, and so on. The encryption method performed by a Caesar cipher is often incorporated as part of more complex methods, such as the Vigenère cipher, and are still has importance in modern application in the ROT13 system. As with all single alphabet substitution ciphers, the Caesar cipher can be easily broken and in modern practice offers essentially no communication security [7]. The encryption can also be act as a substitute for modular arithmetic by first replacing the letters by numbers, according to the scheme, A=0, B=1,…..Z=25.

Encryption of a letter x by a shift n can be representing mathematically as:

$$E_n(x) = (x + n) \bmod 26$$

Decryption can be represented similarly

$$D_n(x) = (x - n) \bmod 26$$

The key can be memorized easily because there is a pattern present in it. The ciphertext alphabet is just the plaintext but the only difference is that it is shifted to the right three places. Sender and receiver just need to memorise the shift.

e. *Weaknesses of Caesar Cipher* [6]

- Word structure is preserved-Break message into equal-length blocks.
  -dww dfn dwg dzq
- Letter frequency is a big clue
  -e,t,a,o most common English letters.
  -Using a single key preserves frequency.
- Solution: use multiple keys
  - E.g. shift by (3,5,7)
  - "Attack at dawn" becomes dya dhr dyk dbu.

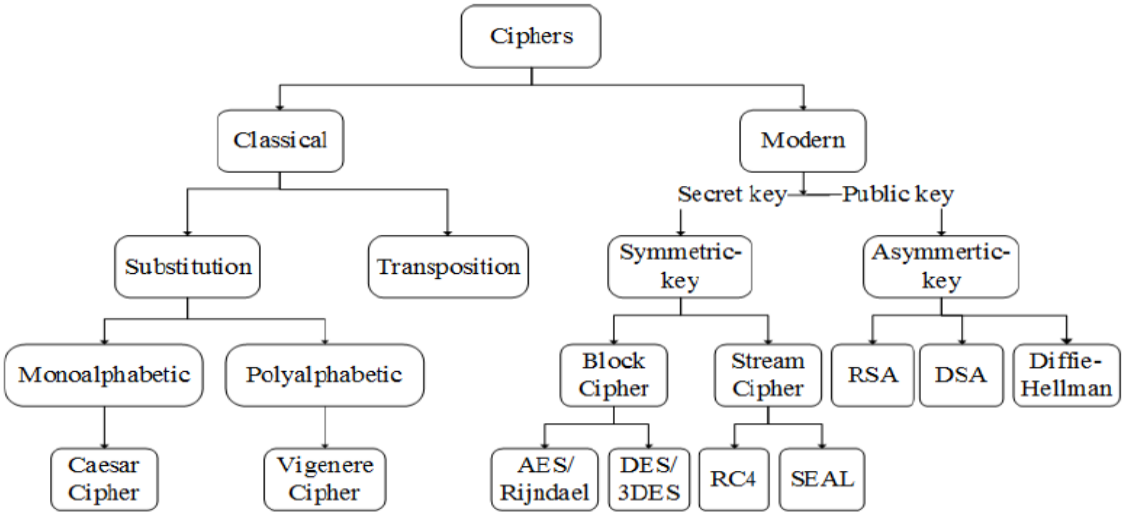

FIGURE 5: Different Encryption Method

Better, but frequency information still present. An attacker that knows the size of the block can separate out character coded with different keys [16].The Caesar cipher is still useful as a way to prevent people from unintentionally reading something.

Fundamental problem: But the main problem is that key length is shorter than the message.

II. Related Work

a. ***Caesar Ciphers*** [17]

In this paper information related to history of cryptography and contribution of various scientists in cryptology is given. Friedman (1891 – 1969) is often called the dean of modern American cryptologists. He was a pathfinder in the application of scientific principles to cryptology. During Second World War, Friedman was the director of communications research for the Signal Intelligence Service (SIS). SIS later became the Army Security Agency (ASA). After Second World War, Friedman served first as a consultant for ASA and then for the National Security Agency (NSA) after its birth in 1952.

Friedman and his wife Elizebeth, who was also a cryptologist, jointly authored the book The Shakespearean Ciphers Examined.

The Italian cryptologist Leon Battista Alberti (1404 – 1472), also called as the Father of Western Cryptology, developed a cipher disk.

The Dutch cryptologist Auguste Kerkhoffs (1835 – 1903) named the cryptographic slide. In 1883, Kerkhoffs published La Cryptographie militarie, which became a major cryptological work.

b. ***Cryptography and Network Security, Fourth Edition*** *[13]*

This is provided as a Student Resource. In this various information regarding cryptography and network security is given in the PDF form which can be easily downloaded. In this contents are divided into chapters like overview, classical encryption techniques etc.

Classical Encryption Techniques *[2]*

It is published by a Ramandeep Sharma, Richa Sharma and Harmanjit Singh. This paper gives information about various classical and modern encryption techniques which are mostly used to solve the problem in open networked systems for example DES, Playfair, AES, Blowfish etc.

c. Somdip Dey et al[5] presents a new cryptographic technique, SDAREE to removes the repetitive terms in plaintext, when the plaintext is to be encrypted, so that it becomes almost impossible for a person to retrieve or predict the original message from the encrypted message. SD-AREE is a modified Caesar Cipher Technique along with advanced bit-manipulation cryptographic method. In this the key will be given by user in the form of string. Then this string will be used to generate to numbers "code" and "power_ex". "Code" will be generated as follows: The ASCII value of each character of the key is multiplied with the string-length of the key and with 2^i, where "i" is the position of the character in the key, starting from position "0". Then adding up the resultant values of each character, which they got from multiplication, and then each digit of the resultant sum is added to form the „pseudo_code". Then the code will be generated from the pseudo_code by doing modular operation of pseudo_code by 16, i.e. code = (pseudo_code Modulus 16). If code==0, then we set code =pseudo_code.

d. Amit Joshi and Bhavesh Joshi [1] propose an algorithm which uses a randomized technique in order to encrypt and decrypt the plaintext. The proposed algorithm uses various techniques of cryptography using versions of Caesar Cipher and a protocol to implement this algorithm using public key generation and randomized technique. The algorithm uses actual global time of the sending of message to generate the public key.

The paper reviews about the proposed algorithm and implements the algorithm by taking five plain texts (of a single statement) an input and calculates the corresponding cipher texts. Secrete key will be generated by adding up all the digits of time i.e. hh-mm-ss.

e. Anju [6] introduces Encryption and Decryption in terms of Cryptography Techniques. This paper gives the Fundamental Requirements for the Data Transmission, various security attacks like Modification, Interception and Interruption of the data Transmission. This paper also includes a Cryptographic Process explaining through a generalized function through which encryption and decryption is done by the algorithm to encipher and decipher the data for a word/line.

f. Eric [18] gives information about various types of cryptographic attacks.

g. Mathur et al. [7] proposed an algorithm for data encryption and decryption this algorithm is based on ASCII values of characters in the plain text. This algorithm is used to encrypt data by using ASCII values of the data to be encrypted. The secret used will be modifying another string and that string is used as a key to encrypt or decrypt the data. So, it can be said that this is symmetric encryption algorithm because this algorithm uses same key for encryption and decryption but by slightly modifying it. This algorithm works when the length of input and the length of key are same.

h. Saroha et al. [8] have discussed There are two techniques for converting data into non readable form:

1. Transposition technique
2. Substitution technique

Caesar cipher is an example of substitution method. Caesar cipher has various limitations. This paper gives a perspective on combination of techniques substitution and transposition. On Caesar cipher a double columnar transposition method can be applied in order to overcome all limitation of Caesar cipher and provide much more secure and strong cipher.

i. Srikantaswamy et al. [9] have proposed a method to improve Caesar cipher with random number generation technique for key generation operations. Here Caesar cipher has been expanded so that it can also include alphanumeric and symbols. Classical Caesar cipher was restricted only for alphabets. The key used by Caesar Substitution has been derived using a key Matrix Trace value limited to Modulo 94. The Matrix elements are produced using recursive random number generation equation, the output of which only depends on the value of seed selected. In this author made an effort to incorporate classical cipher with modern cipher properties. In the second stage, encryption has been done using columnar transposition with arbitrary random order column selection. Thus the proposed Scheme is a mixed version of classical and modern cipher properties. The proposed method provides enhanced Security with high throughput and occupies minimum memory space. The method is secured against brute-force attack with 93! Combination of keys, for Caesar.

j. Singh et al. [10] proposed a method that uses Caesar cipher substitution and Rail fence transposition techniques separately, cipher text obtained by both the methods is easy to crack. These papers present an idea of combining techniques substitution and transposition. Combining classical Caesar cipher with Rail fence technique can eliminate their fundamental weakness and can produce a cipher text that is hard to crack.

III. PROPOSED METHOD

In this section the proposed algorithm and its working is described with the help of an example. The algorithm is used to encrypt as well as decrypt the plain text. The proposed system is divided into two phases:

Phase 1: Improved Key generation technique

Phase 2: Caesar cipher algorithm

The phase 1 will describe some improvements that are applied over key generation technique of classical Caesar cipher by applying dynamic key for each letter in a string. In Dynamic key is depends on the length of the string, position of the character in the string and time of file to be encrypted and for each letter in the string to be encrypted key changes as encryption proceeds through the length of the string.

In phase 2, traditional Caesar cipher is applied.

Algorithm

Step 1: Take the string which you want to encrypt.
Consider an example given
plaintext:" encrypt the data"

Step 2: Read a word form that file.
The word will be: "encrypt".

Step 3: Calculate the length of the string.
Length of the string (Strlen): 7

Step 4: For the secret key consider the time of file and add number of hours, minutes and seconds [1].
Let the time of file is 20: 23: 23. So the sum of digit would be (Time): 2+0+2+3+2+3=12

Step 5: Create the secret key (SK): SK= Strlen + Time
If the sum exceeds 25 then it is processed again following the same procedure
SK = 7 + 12 = 19

Step 6: Find the odd and even positioned character from the given word & divide them into two separate groups.
i.e. group of odd position character in "encrypt" is " nrp ",
group of even position character in "encrypt" is "ecyt"

Step 7: Reverse both the strings.
Reversed "nrp" is: "prn"
Reversed "ecyt" is: "tyce"

Step 8: Step 8: Apply Caesar cipher to the reversed odd position character group for which the SK depends on the time when the file is closed and length of original string. Apply substitution cipher for the right ends to the left end i.e. apply SK for last character and will go on decreasing towards first character.
Apply Caesar to "prn". ASCII value of n is 110
SK is 19 so Caesar cipher will be calculated for "n" as (110+19) mod 26 = 25
So "n" will be shifted by 25 resulting "‡". After this SK will be decreased by 1.
Similar procedure will be applied for "r" and "p" giving result "t" and "p" respectively.

Step 9: Apply Caesar cipher to the reversed even position character group for which the SK depends on the time when the file is closed and

length of original string. Apply substitution cipher for the left ends to the right end i.e. apply SK for first character and will go on decreasing towards last character.

Apply Caesar cipher to "tyce" same as that of "prn".

Step 10: Apply steps 2 to 9 on all the other strings.

Step 11: Replace the character at the start position, middle position & end position of the string, with a new character whose ASCII value is equal to the ASCII value of the original character at that place + SK - 26.

Step 12: End

IV. CONCLUSIONS

This method of plain text encryption can be applied to any form of text or any text file format like txt, doc, docx, rtf, etc. The proposed system is an improvement over traditional plain encryption methods using key length and separation of plaintext string in two different substrings. The text encrypted using proposed method, can't be decrypted using traditional crypto-analysis tools. The brute force attack technique also fails to decrypt the text which is encrypted by using proposed technique.

ACKNOWLEDGMENT

I am thankful to Prof. S. D. Sapkal, and to Principal, Government College of Engineering, Aurangabad [Autonomous] and Prof. V. P. Kshirsagar, HOD, Computer Science and Engineering Department, Government College of Engineering, Aurangabad [Autonomous]

REFERENCES

[1] Amit Joshi and Bhavesh Joshi "*A Randomized Approach for Cryptography*" in Emerging Trends in Networks and Computer Communications (ETNCC), 22-24 April 2011.

[2] Ramandeep Sharma, Richa Sharma and Harmanjit Singh "*Classical Encryption Techniques*" published in International Journal of Computers & Technology. Volume 3. No. 1, AUG, 2012 .

[3] O.P Verma, RituAgarwal, DhirajDafouti and ShobhaTyagi, "*Peformance Analysis Of Data Encryption Algorithms*",IEEE DelhiTechnological University India, 2011.

[4] Quist-Aphetsi Kester" *A hybrid cryptosystem based in Vigenere cipher and Columnar Transposition cipher*" ISSN No: 2250-3536 Volume 3, Issue 1, Jan. 2013 141.

[5] Somdip Dey"*SD-AREE: An Advanced Modified Caesar Cipher Method to Exclude Repetition from a Message*" published in International Journal of Information & Network Security (IJINS). Vol.1, No.2, June 2012, pp. 67~76

[6] Anju and Ms. Ayushi Aggarwal "*Enciphering Data for Larger Files*" published in International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE). Volume 3, Issue 5, May 2013.

[7] Akanksha Mathur, "*A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms*", International Journal on Computer Science and Engineering (IJCSE). Vol. 4 No. 09. pp .1650-1657, September 2012.

[8] Vinod Saroha, Suman Mor and Anurag Dagar, "*Enhancing Security of Caesar Cipher by Double Columnar Transposition Method*", International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 2, Issue 10. pp .86-88, October 2012.

[9] S G Srikantaswamy, Dr. H D Phaneendra, "*Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption*", International Journal on Cryptography and Information Security (IJCIS). Vol. 2, No.4. pp. 39-49, December 2012.

[10] Ajit Singh, Aarti Nandal and Swati Malik, "*Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security*", International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 2, Issue 12. Pp. 78-82, December 2012.

[11]Kashish Goyal and Supriya Kinger"*Modified Caesar Cipher for Better Security Enhancement*" published in International Journal of Computer Applications (0975 – 8887)(IJCA)" Volume 73– No.3, July 2013.

[12] Sinkov A., *Elementary Cryptoanalysis – A mathematical Approach*, Mathematical Association of America, 1966.

[13] William Stallings, "Cryptography and Network Security", Fourth Edition, Prentice-Hall -pp.80-81.

[14] http://www.cs.trincoll.edu /~crypto/historical/caesar.html (Savarese, C and Hart, B, The Caesar Cipher, Last updated: 04/26/2010 03:46:57).

[15] http://www.garykesseler.net/library/crypto.html(An overview of cryptography by Gary C. Kessler last updated 3/10/13)

[16] "CRYPTOGRAPHY", https://en//.wikipedia.org/wiki/cryptography

[17] http://www.nku.edu (Fall 2006 Chris Christensen)

[18] www.giac.org/cissp-papers/57.pdf