Modified Caesar Cipher for Better Security Enhancement

Kashish Goyal
M.Tech Research Scholar, Department of Computer Science and Engineering
Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India.

Supriya Kinger
Assistant Professor, Department of Computer Science and Engineering
Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India.

ABSTRACT
Encryption is the process of scrambling a message so that only the intended recipient can read it. With the fast progression of digital data exchange in electronic way, Information Security is becoming much more important in data storage and transmission. Caesar cipher is a mono alphabetic cipher. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter. In this paper, author modified the traditional Caesar cipher and fixed the key size as one. Another thing alphabet index is checked if the alphabet index is even then increase the value by one else alphabet index is odd decrease the key value by one. Encryption and scrambling of the letters in the Cipher Text.

General Terms
Security, Encryption

Keywords
Decryption, Symmetric Encryption, Plaintext, Cipher Text.

1. INTRODUCTION
Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted [1]. Security is a big concern and securing crucial data is very essential, so that the data cannot be change or misused for any illegal purposes. For example in Internet Banking system, e-reservation system the security of data is a very important issue. Under no circumstances the intruder should be able to get into the server database or the confidential data. In any type of service sectors the confidentiality of data is a very important issue. The primary goal of any system is that the data cannot be modified by any external user or intruder [2]. To avoid such a type of situation. Convert data into a non readable form at sender side and convert that data in readable form again at receiver side. The technique and science of creating non readable data or cipher so that only authorized person is only able to read the data is called Cryptography [9]. In Cryptography, Caesar cipher is one of the most widely known encryption decryption algorithm. Caesar cipher is a type of substitution type cipher in this kind of cipher each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. The encryption is represented using modular arithmetic [3].

With the increasing trend of internet technologies, numerous security issues are arising. Cloud users are also victim of the security issues. In cloud computing security issues are faced by the Cloud providers as well customers. In most cases, provider must ensure that their infrastructure is secure and that their client's personal data and applications are protected while the customer must ensure that the Cloud provider has taken the proper security measures to protect their information So security issues are everywhere [4].

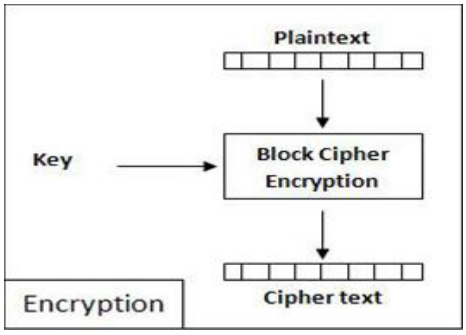

Fig 1: Plaintext to Cipher Text

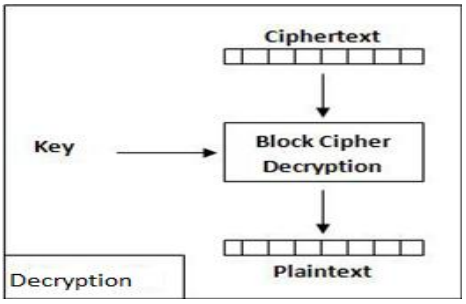

Fig 2: Cipher Text to Plaintext

2. CRYPTOGRAPHY
Cryptology is not a new; it has existed for more than 2000 years. The word cryptology is derived from two Greek words: kryptos, which means "hidden or secret and graphein" (to write), is the art and science of making communication unintelligible to all except the intended recipients [5]. In the language of cryptography, the message one intends to send is called the plaintext while the message that is actually sent is called the cipher text. Ciphers make textual communication a mystery to anyone who might unduly intercept it. Hence, a cipher is a method used to encode characters to hide their values. Cipher is employed in design of cryptosystem. A cryptosystem is a system, method, or process that is used to provide encryption and decryption [6]. There are two main categories of cryptography depending on the type of security keys used to encrypt/decrypt the data. These two categories are: Asymmetric and Symmetric encryption techniques.

2.1 Symmetric Encryption
When same key is used to encrypt and decrypt the message then it is known as symmetrical key cryptography. It is also known as private key cryptography; users have the provision to update the keys and use them to derive the sub keys. It is much effective and fast approach as compared to asymmetrical key cryptography. In symmetrical key cryptography; key has been generated by the encryption algorithm and then send it to the receiver section and decryption takes place [7, 8]. There are few challenges in the

technique; i) the key should be transmitted over the secure channel from sender to receiver. The point is that if the secure channel already exits then transmit the data over the same channel, what is the need of encryption in such case. Practically no secured channel exits therefore key has been transmitted along the data which increases the overheads and effective bandwidth gets reduced. Secondly, the channel noise put harm to the key and data during the transmission [9].

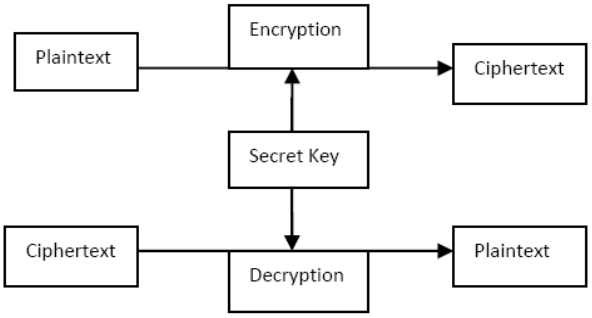

Fig 3: Shows the working of symmetric encryption.

2.2 Asymmetric Encryption

It is also called as public key cryptography. It uses two keys: public key, which is known to the public, used for encryption and private key, which is known only to the user of that key, used for decryption. The public and the private keys are related to each other by any mathematical means. In other words, data encrypted by one public key can be encrypted only by its corresponding private key [10]. Encryption and decryption procedure as shown below in figure 4:

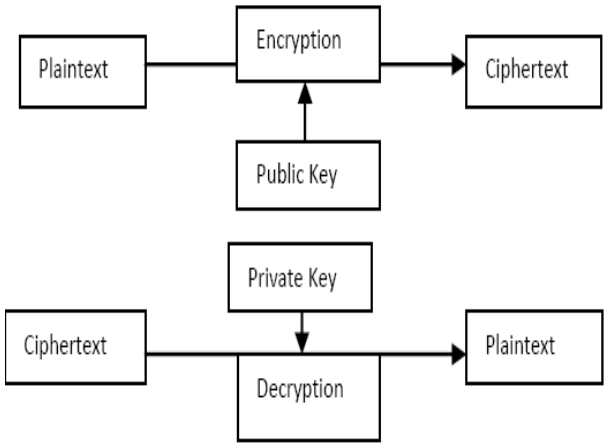

Fig 4: Public Key Cryptography Process

This capability surmounts the symmetric encryption problem of managing secret keys. But on the other hand, this unique feature of public key encryption makes it mathematically more prone to attacks. Moreover, asymmetric encryption techniques are almost 1000 times slower than symmetric techniques, because they require more computational processing power [11].

Cryptography is an art and science of converting original message into non readable form. 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 [12].

It is said to have been used by Julius Caesar to communicate with his army. Caesar is considered to be one of the first persons to have ever employed encryption for the sake of securing messages. Caesar decided that shifting each letter three places down the alphabet in the message would be his standard algorithm, and so he informed all of his generals of his decision, and was then able to send them secured messages. 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.

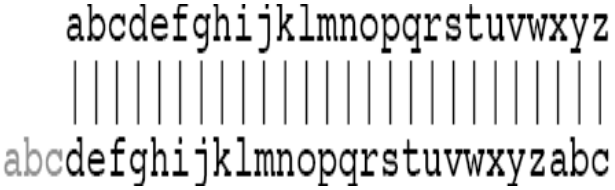

Fig 5 : Caesar cipher working

Further enhancement to original three places shifting of character in Caesar cipher uses modulo twenty six arithmetic for encryption key that is greater than twenty six.

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

Where x is value of plaintext n is number of shift. The most pressing weakness of this cipher is simplicity of its encryption and decryption algorithms; the system can be deciphered without knowing the encryption key. It is easily broken by reversing encryption process with simple shift of alphabet ordering [8].

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

Another security concern is that, if how one letter should be deciphered is already known, then the shift can be determine and decipher the entire message. A better approach would be to make use of statistical data about English letter frequencies. Correcting these weaknesses of the Caesar cipher so it becomes unbreakable using existing methods [6].

3. RELATED WORKS

To give more prospective about the performance of the encryption algorithms, this section describes and examines previous work done in field of data encryption.

Srikantaswamy et al. [3] have proposed a method to improve Caesar cipher with random number generation technique for key generation operations. Here Caesar cipher has been expanded so as to include alphanumeric and a symbols. Original Caesar cipher was restricted only for alphabets. The key used for Caesar Substitution has been derived using a key Matrix Trace value restricted to Modulo 94. The Matrix elements are generated using recursive random number generation equation, the output of which solely depends on the value of seed selected. author made an effort to incorporate modern cipher properties to classical cipher. The second stage of encryption has been performed using columnar transposition with arbitrary random order column selection. Thus the proposed Scheme is a hybrid version of classical and modern cipher properties. The proposed method provides appreciable Security with high throughput and occupies minimum memory space. The method is resistant against brute-force attack with 93! Combination of keys, for Caesar.

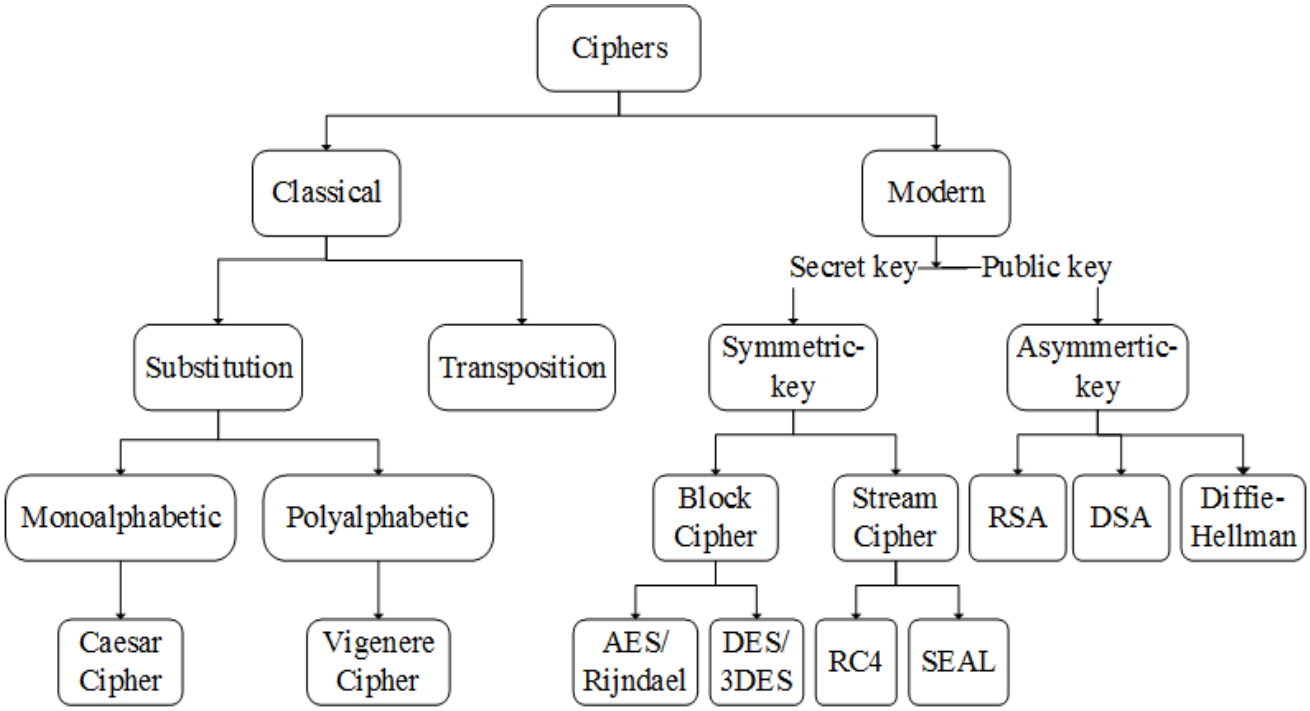

Fig 6: Classification of Encryption methods

Goyal et al. [4] describe Cloud Computing security issues. Security is the biggest challenge for Cloud Computing currently. Trust has proved to be one of the most important and effective alternative means to construct security in distributed systems. Obviously putting everything into a single box i.e. into the Cloud will only make it easier for hacker. In this paper author discuss security issues like Confidentiality, web security, Email Security etc.

Mathur [14] 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 operates when the length of input and the length of key are same.

Saroha et al. [12] 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 presents a perspective on combination of techniques substitution and transposition. A double columnar transposition method can be applied on Caesar cipher in order to overcome all limitation of Caesar cipher and provide much more secure and strong cipher.

Singh et al. [15] have proposed a method of Caesar cipher substitution and Rail fence transposition techniques are used individually, cipher text obtained is easy to crack. These papers present a perspective on combination of techniques substitution and transposition. Combining Caesar cipher with Rail fence technique can eliminate their fundamental weakness and produce a cipher text that is hard to crack.

Kothari et al. [13] proposed that if a cipher is computationally secure then it means that the probability of cracking the encryption key using current computational technology and algorithms within a reasonable time is supposedly extremely small, yet not impossible. In theory, every cryptographic algorithm except the Vernam Cipher can be broken given enough cipher text and time. This is where COMCRYPT comes into picture. COMCRYPT is an encryption algorithm, which has been formulated on the lines of Vernam cipher. When a passphrase is taken from the user, a scrambling algorithm is implemented on it, which generates two more random keys. These keys are superimposed on each other and then XOR to the text to produce the cipher text. This algorithm was monitored on different plaintexts, and it was found that this method was almost unbreakable. This method supports multiple encryptions and multiple decryptions. A minor change in the text key will change the cipher text quite a lot.

4. PROPOSED ALGORITHM

4.1 Modified Caesar Cipher Algorithm

To encrypt a message proposed algorithm requires plaintext and encryption key. The encryption key is an integer value and it determines alphabet to be used for substitution. It is based on modulo twenty six arithmetic to ensure that integer value wraps round in case encryption key supplied is more than twenty six. Decryption follows reverse operations performed during the process of encryption. It requires decryption key, and encrypted text. The decryption key should be complement to the encryption key so that reverse character substitution can be achieved. As stated earlier, Caesar cipher simply shifts encrypted character by number of positions. In this paper author proposed a new method, where key size is fixed as one. In this method firstly alphabet index is checked if the alphabet index is even then increase the value by one else the index is odd decrease the key value by one. Furthermore, the characters of the encrypted text are

scrambled in such a way that if an attempt is made to decrypt the cipher text it would not be easy to decrypt the text.

Encryption Algorithm
Step1: Take the plain text as input.
Step2: Firstly alphabet index is checked if the alphabet index is even then increase the value by one else decrease the key value by one.
Step3: Get the encrypted text.

Decryption Algorithm
Step 1: Insert cipher text.
Step2: Check alphabet index if the alphabet index is even then increase the value by one else decrease the key value by one.
Step 3: Get the plain text.

Table 1. Key for uppercase alphabets

TEXT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
KEY	B	A	D	C	F	E	H	G	J	I	L	K	N	M	P	O	R	Q	T	S	V	U	X	W	Z	Y

Table 2. Key for Lowercase alphabets

text	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
key	b	a	d	c	f	e	h	g	j	i	l	k	n	m	p	o	r	q	t	s	v	u	x	w	z	y

Table 3. Key for Numeric values

Number	1	2	3	4	5	6	7	8	9	0
Key	2	1	4	3	6	5	8	7	0	9

Table 4. Mapping table for uppercase alphabets

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 5. Mapping table for Lowercase alphabets

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Encryption

C=E (P) = (P+1) if P is even or zero than add one

Else

E (P) = (P-1) (mod 26) if p is odd than subtract one

Decryption

P=D(C) =(C-1) if C is odd than Subtract one

Else

D(C) = (C+1) if P is even or zero than add one

4.2 Comparison with Caesar cipher

Existing Technique of Caesar cipher using the key as three where each character is shifted by three character for example A become D and key is most of time in incremental order Caesar cipher is a mono alphabetic cipher. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter but in this Modified Caesar cipher algorithm to encrypt a message proposed algorithm requires plaintext and encryption key. It is based on modulo twenty six arithmetic. Here key size of Caesar cipher fixed as one. Another thing alphabet index is checked if the alphabet index is even then increase the value by one else alphabet index is odd than decrease the key value by one. In this way this method is better than existing one.

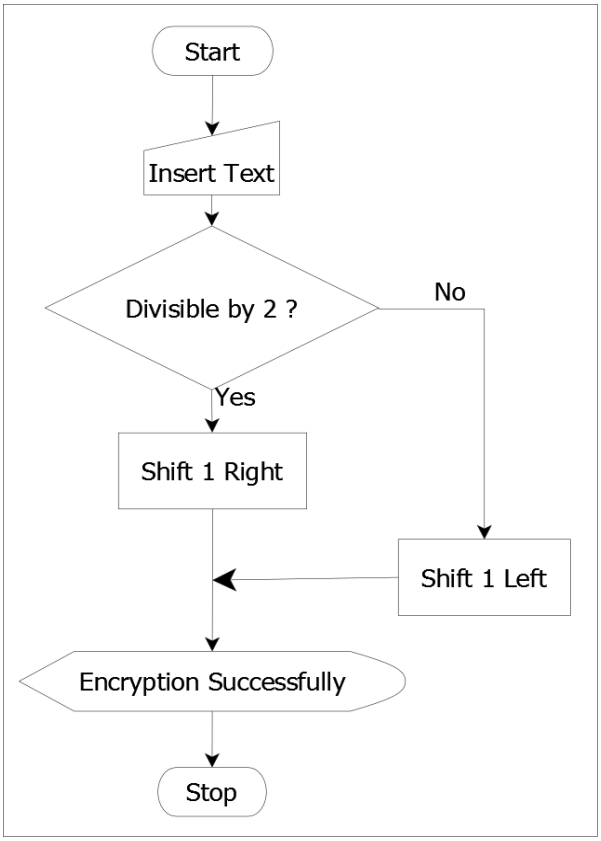

Fig 7: Encryption Process

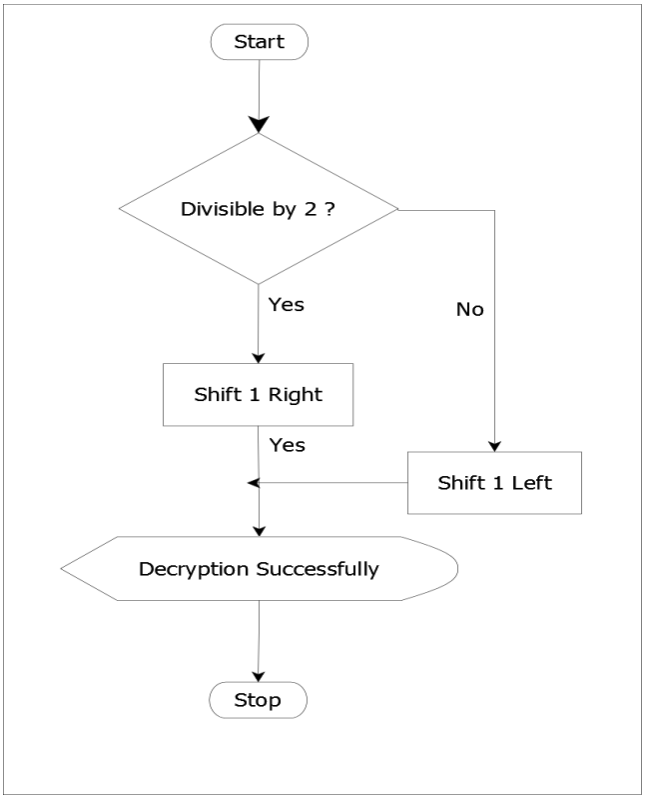

Fig 8: Decryption Process

5. EXPERIMENTAL RESULTS

A. Encryption

Step 1: Suppose original message is Computer123

Step 2: Now apply Caesar cipher to encrypt the plain text. Shifting the key as one.

Example 1

Table 6. Encryption process

Plaintext	**: Computer123**
Cipher Text:	**Dpnovsfq214**

We get Dpnovsfq214 as cipher text because as per as algorithm the value C that is 2 is even (Refer to table 4) and we have to add one as per algorithm and we get D as cipher text of C. same way o is even and we add one and then p became cipher text of o.

Example 2

Table 7. Encryption process

Plain Text	**Cryptography**
Cipher Text	**Dqzosphqbogz**

B. Decryption

Example 1

Table 8. Decryption Process

Cipher Text	**: Dpnovsfq214**
Plaintext	**: Computer123**

We get Computer123 as Plain Text because according to algorithm D is odd (Refer to table 4) and we have to Subtract one as per algorithm and we get C as Plain Text of D. Same way p is odd and we subtract one and then o became plaintext of p.

Example 2

Table 9. Decryption Process

Cipher Text	**: Dqzosphqbogz**
Plaintext	**: Cryptography**

6. CONCLUSION AND SCOPE OF FUTURE WORK

Data Security is a very important aspect. The key generations play a crucial role in designing the ciphers. This paper presents Modified Caesar cipher. It is a substitution cipher. The use of internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used. In this paper Caesar cipher technique is used for security. it is unique in its own way. Security provided by this algorithm can be enhanced further, if more than one algorithm is applied to data. Future work will explore this concept and a combination of algorithms will be applied over data to setup a more secure environment for data storage and retrieval.

7. REFERENCES

[1] Hamdan.O.Alanazi, B.B.Zaidan and A.A.Zaidan, New Comparative Study between DES, 3DES and AES within Nine Factors, Journal Of Computing. Vol. 2 , Issue 3. Pp.152-157, 2010.

[2] Somdip Dey, Joyshree Nath and Ashoke Nath, "An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation, Bit Reversal, Modified Caesar Cipher (SD-REE), DJSA method, TTJSA method: SJA-I Algorithm", International Journal of Computer Applications (IJCA). Vol. 46, No. 20. Pp. 46-53, May 2012.

[3] 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.

[4] Kashish Goyal, Supriya, "Security Concerns In the World of Cloud Computing", IJARCS International Journal of Advanced Research in Computer Science, Vol. 4, No. 4, pp. 230-234, March 2013.

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

[6] Ochoche Abraham, Ganiyu O. Shefiu, "AN IMPROVED CAESAR CIPHER (ICC) ALGORITHM", International Journal Of Engineering Science & Advanced Technology (IJESAT). Vol. 2, Issue -5. pp .1198 – 1202, October 2012.

[7] Jason Crampton, "Time-Storage Trade-Offs for Cryptographically-Enforced Access Control", Lecture Notes in Computer Science, Springer, 2011, Vol. 6879/2011, pp. 245-261.

[8] Jiannong Cao, Lin Liao, Guojun Wang, "Scalable key management for Secure Multicast Communication in the Mobile Environment" Pervasive and Mobile Computing Vol. 2, pp.187–203, 2006.

[9] Gaurav Sharma, Ajay Kakkar, "Cryptography Algorithms and approaches used for data security", International Journal of Scientific & Engineering Research Vol. 3, Issue 6, 2012.

[10] Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering,Vol. 1, Issue 2, pp. 6-12, 2011.

[11] "ENCRYPTION"http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.htm

[12] 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.

[13] Maulik Kothari, Manthan Shah, and Meet Malde, "Comcrypt: An Encryption Algorithm based on Vernam cipher", International Journal on Computer Science and Technology (IJCST). Vol. 3, Issue 4.pp .364-367, Oct – Dec 2012.

[14] 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.

[15] 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.