IMPROVED CAESAR CIPHER WITH RANDOM NUMBER GENERATION TECHNIQUE AND MULTISTAGE ENCRYPTION

S G Srikantaswamy[1] and Dr. H D Phaneendra[2]

[1]Research scholar, National Institute of Engineering, Mysore
sg_srikantaswamy@yahoo.com
[2]Professor and Research Guide, National Institute of Engineering, Mysore
hdphanee@yahoo.com

ABSTRACT :

Secured Communication involves Encryption process at the sending end and Decryption process at the receiving end of the communication system. Many Ciphers have been developed to provide data security . The efficiency of the Ciphers that are being used depends mainly on their throughput and memory requirement. Using of large key spaces with huge number of rounds with multiple complex operations may provide security but at the same time affects speed of operation. Hence in this paper we have proposed a method to improve Caesar cipher with random number generation technique for key generation operations. The Caesar cipher has been expanded so as to include alphabets, numbers and symbols. The 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 . In this paper, we 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! Combinations of keys, for Caesar encryption.

KEYWORDS:

Encryption, Decryption, Substitution, Cipher, Random Number, Recursive, Primitive root, Plaintext, Ciphertext

1. INTRODUCTION :

In Cryptography, the Caesar cipher is one of the most widely known encryption technique. Caesar cipher 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. The encryption is represented using modular arithmetic

c by first transforming the letters into numbers, according to the scheme A=0,B=1…..Z=25.

Encryption of a letter x by a shift n can be described mathematically as $E_n(x)=(x+n) \bmod 26$. Decryption is performed as $D_n(x)=(x-n) \bmod 26$ (Wikipedia, Caesar_cipher).

If it is known that a given ciphertext is Caesar cipher, then brute-force cryptanalysis is easily performed (William stallings, 2004, Cryptography and Network security, 3rd edition, Pearson Education)

Hybrid approach of Caesar cipher and Columnar transposition , the combination of the two have been discussed . (Dharmendra Kumar Gupta et al, 2012). This approach is intended to propose Cipher with good features , But the key generation technique should be strengthened to thwart the efforts of cryptanalysis and also key space adapted is not sufficient.

Classical techniques and modern techniques can be combined to produce better results. Avalanche effect has been compared by changing the key value for DES, Playfair and Vigenere (Fauzan saeed and Mustafa Rashid, 2010). The Comparative study of both classical and modern techniques have been discussed by considering playfair, Vigenere cipher, Caesar cipher , DES and Blowfish.(Sriram Ramanujam and Mrimuthu Karuppiah, 2011).But the desirable requirement is to use wider key-space with high degree of security. This can be achieved by using a key-length of 128-bit or more. The data encryption technique using compression technique has been proposed in (Monodeep Banerjee et al, 2012). Thus the combination of encryption and compression provides appreciable security but the key length and efficient compression techniques are required for appreciable security.

Design of robust cipher for non-invertible matrices based on hill cipher has been discussed in (Rushdi A.Hamamreh and Mousa Farajallah, 2009). The proposed method suggests the idea of converting a given plaintext characters into two ciphertext characters. The method also suggested the use of RSA algorithm for encrypting the key used for encryption and decryption. Cryptographic techniques using graceful codes has been proposed (Prof.K.Govinda and Dr.E.Sathiyamoorth", Multilevel Cryptography Technique using Graceful Codes "- JGRCS, Volume 2, N0.7, July 2011). This method is useful for small amount of data.

The hill cipher can be improved with the combination of Affine cipher. Affine hill cipher mixes the hill cipher with a nonlinear affine transformation. The extended system proposed a method in which matrix inverse computation has been eliminated (A.F.A.Abidin et al, 2011). Vigenere cipher is able to be cracked, because of the lack of diffusion property. The Vigenere cipher can be made Secure by using padding bits and one can diffuse the statistical properties of the messages (Phillip I Wilson and Mario Garcia, 2006). Effective key length should be adopted . The algorithm works for alphabets . Play fair cipher can be made more effective with the use of linear feedback shift register (Packirisamy Murali and Gandhi doss Senthil kumar, 2008). The desired properties of a random number generator functions are: It should be efficiently computable, the period should be large and successive values should be independent and uniformly distributed (Raj Jain , " the Computer Systems Performance analysis ", John Wiley & sons Inc.) .

2.ENCRYPTION ALGORITHM :

1) Read the Plaintext Message
2) Replace the Plaintext characters by their numerical value
3) Generate a Secret key using random number generation technique

$X_n = K X_{n-1} + 1 \bmod n$, where K is the Seed value and n is an integer representing modulus.

4) Arrange the Secret key generated in step 3 , in the matrix form of the order I X J
5) Obtain the Trace of the Matrix
   Secret Key Value=(Trace of the Key matrix) mod 94
6) Perform the Caesar substitution encryption using the secret key value generated in step 5
7) Arrange the Ciphertext sequence in the order I X J

8) Obtain the transpose of the matrix I X J
9) Exclusive-or the results of step 7 and step 8
10) Perform Columnar transposition
11) Perform Permutation transposition
12) Transmit the Ciphertext .

3.DECRYPTION ALGORITHM :

1) Read the Ciphertext Message
2) Arrange them in the matrix form of order I X J
3) Obtain the transpose of the Matrix I X J
4) Exclusive-or the results of step 2 and step 3
5) Perform reverse Caesar Substitution
6) Process the Plaintext

4.ALGORITHM DESCRIPTION AND ILLUSTRATION :

The Proposed method can be applied to encrypt Plaintext messages composed of alphabets , numbers and symbols. The above characters have been assigned the numerical values as shown below.

Character Value Table :

Character	Value
!	0
‘’	1
#	2
$	3
%	4
&	5
‘	6
(	7
)	8
*	9
+	10
’	11
-	12

.	13
/	14
0	15
1	16
2	17
3	18
4	19
5	20
6	21
7	22
8	23
9	24
:	25
;	26
<	27
=	28
>	29
?	30
@	31
A	32
B	33
C	34
D	35
E	36
F	37
G	38
H	39
I	40

J	41
K	42
L	43
M	44
N	45
O	46
P	47
Q	48
R	49
S	50
T	51
U	52
V	53
W	54
X	55
Y	56
Z	57
[	58
\	59
]	60
^	61
_	62
`	63
A	64
B	65
C	66
D	67
E	68
F	69
G	70
H	71
I	72
J	73
K	74
L	75

M	76
N	77
O	78
P	79
Q	80
R	81
S	82
T	83
u	84
v	85
w	86
x	87
y	88
z	89
{	90
|	91
}	92
~	93

Encryption operation is expressed as :

C=E(P)=(P+K) mod 94

“K” can take any Value in the range 0 to 93.

Decryption operation is expressed as :

P=D(C) =(C-K) mod 94

“K” can take any Value in the range 0 to 93.

Algorithm Illustration

Consider a plaintext Message which is to be encrypted using the proposed algorithm.

“This Message is very Secret OK”.

Now replace each character of the Plaintext message by its numerical value and arranging them in 5 X 5 Matrix form, we get the following set of values.

T=51	h=71	i=72	s=82	M=44	e=68	s=82	s=82	a=64	g=70	e=68	i=72
	s=82										
V=85	e=68	r=85	y=88	S=50	e=68	c=66	r=85	e=68	t=83	O=46	K=42

51	71	72	82	44
68	82	82	64	70
68	72	82	85	68
85	88	50	68	66
85	68	83	46	42

Now to encrypt the Plaintext ,generate the key using random number generation technique using recursive equation.

Consider Multiplicative Linear Congruential Generators (LCGs) for random generation.
$X_n = a\ X_{n-1} \bmod m$.

Multiplicative LCG will be a full-period generator if and only if the multiplier "a" is a primitive root of the modulus m.

Let m= 31, a prime number

a= 3 (a primitive root of m)

$\therefore \quad X_n = 3\ X_{n-1} \quad \bmod 31$

This is the equation for key generation using random number generation technique.

Let the Seed Value be $X_0 = 1$

Then $X_1 = 3\ X_0 \bmod 31$

$X_1 = 3 .1 \bmod 31 = 3$,

$X_2 = 3.3 \bmod 31 = 9$, $X_3 = 3.9 \bmod 31 = 27$ and Similarly $X_4 = 19$, $X_5 = 26$, $X_6 = 16$, $X_7 = 17$, $X_8 = 20$, $X_9 = 29$, $X_{10} = 25$, $X_{11} = 13$, $X_{12} = 8$, $X_{13} = 24$, $X_{14} = 10$, $X_{15} = 30$, $X_{16} = 28$, $X_{17} = 22$, $X_{18} = 4$, $X_{19} = 12$

$X_{20} = 5$, $X_{21} = 15$, $X_{22} = 14$, $X_{23} = 11$, $X_{24} = 2$

Considering the 25 random Numbers and arranging them in 5 X 5 matrix form, We get

01	03	09	27	19
26	16	17	20	29
25	13	08	24	10
30	28	22	04	12
05	15	14	11	02

The Key required to Perform Caesar Encryption is derived from the Random Number Matrix as :

Key= [Trace of random number Matrix 5X5] Mod 94

Trace of the Above Matrix = [01+16+08+04+02]=31

Key=[TRACE Mod 94]=41 Mod 94=41

So the Key required to Perform Caesar Encryption is 41.

The Caesar Encryption is described by the equation C=(P+K) Mod 94

The Plaintext Message Considered for Encryption is " **This Message is Very Secret OK"**.

The Matrix form of the numerical Values of the above Plaintext Message is represented below.

51	71	72	82	44
68	82	82	64	70
68	72	82	85	68
85	88	50	68	66
85	68	83	46	42

Adding the Key Value K to each Plaintext Character and taking Modulus 94 , we get

$$\begin{matrix} 51+41 & 71+41 & 72+41 & 82+41 & 44+41 \\ 68+41 & 82+41 & 82+41 & 64+41 & 70+41 \\ 68+41 & 72+41 & 82+41 & 85+41 & 68+41 \\ 85+41 & 88+41 & 50+41 & 68+41 & 66+41 \\ 85+41 & 68+41 & 83+41 & 46+41 & 42+41 \end{matrix} \quad \text{MOD } 94$$

The resultant Ciphertext Matrix is :

$$C = \begin{matrix} 92 & 18 & 19 & 29 & 85 \\ 15 & 29 & 29 & 11 & 17 \\ 15 & 19 & 29 & 32 & 15 \\ 32 & 35 & 91 & 15 & 13 \\ 32 & 16 & 30 & 87 & 83 \end{matrix}$$

The Transpose of the above Matrix is :

$$CT = \begin{matrix} 92 & 15 & 15 & 32 & 32 \\ 18 & 29 & 19 & 35 & 16 \\ 19 & 29 & 29 & 91 & 30 \\ 29 & 11 & 32 & 15 & 87 \\ 85 & 17 & 15 & 13 & 83 \end{matrix}$$

Exclusive-Or the Matrices C and CT we get :

$$C \square CT = \begin{matrix} 0 & 29 & 28 & 61 & 23 \\ 29 & 0 & 14 & 40 & 1 \\ 28 & 14 & 0 & 29 & 17 \\ 61 & 40 & 29 & 0 & 90 \\ 23 & 1 & 17 & 90 & 0 \end{matrix}$$

Now Performing Columnar Transposition on the above Matrix in a random order Column selection : C4, C1, C3, C1, C0.

Reading the Above Matrix in the above Order and making a single row we get :
C = 23 1 17 90 0 29 0 14 40 1 61 40 29 0 90 29 0 14 40 1 0 29 28 61 23

Now replacing each numerical value by its character representation from the table, the Ciphertext sequence would be as follows.

Ciphetext = 8 " 2 { ! > ! / I " ^ I > ! { > ! / I " ! > = ^ 8

The Next step is to perform the Transposition Technique on the above ciphertext sequence by performing Permutation as C=C3

C8	C23	C17	C0	C6	C24	C9
C14	C2	C13	C7	C1	C16	C10
C15	C21	C17	C20	C19	C18	C12
C11	C4	C5				

The Final Ciphertext Message is :

Ciphertext C = **{ I ^ / 8 ! 8 " { 2 ! / " ! ^> > / ! " I > I ! >**

The Decryption is performed in the reverse Order.

The input to the decryption algorithm is the above ciphertext sequence. Performing the reverse Permutation , we get C=C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16 C17 C18 C19 C20 C21 C22 C23 C24.

Representing ciphetext in the Matrix form and performing C ▫ CT, we get Partial Plaintext. Using the Secret Key and decrypting , the resultant Plaintext would be " **This Message is Very Secret OK ".**

5. FEATURES OF THE PROPOSED ALGORITHM:

- Key length of the Algorithm is 100-bits
- Brute force attack requires 93! Attempts , which makes the algorithm more robust
- The proposed algorithm includes rich character set compare to Caesar cipher
- The algorithm occupies memory approximately equal to 5 Kb
- The algorithm works very fast with 1 µS / byte

6. COMPARISION OF THE PROPOSED METHOD WITH OTHER METHODS :

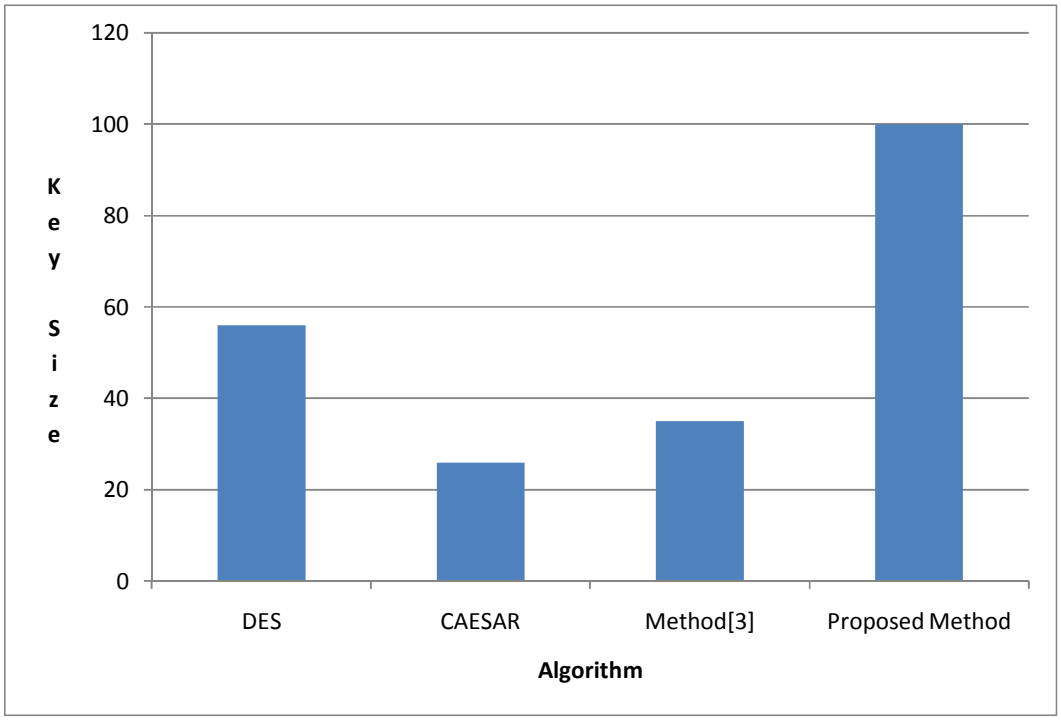

Figure1 : Comparison of Algorithms with respect to Key Length

From the above graph, it is clear that the proposed method is highly resistant to cryptanalytic attacks. The proposed method involves 93! key combinations. The method used to generate key is based on Random number generation principle. Hence key generation is purely based on Seed input to random number generator. Thus by selecting different seed values , different random number series can be generated which can be effectively used as key values after suitable manipulations. Thus the proposed method is a very effective cryptographic method.

6. RESISTANCE OF THE ALGORITHM :

Brute force Attack : Caesar cipher requires 25 different key Values to obtain the Plaintext. Method[3] involves 9 digits key which approximately equal to 2^{36} alternate keys . The proposed method involves 100 bit key value. The modern DES algorithm involves 56 bit key value. Thus the proposed method exhibits more resistance against cryptanalytic attacks.

7. CONCLUSION :

Data Security is a very important aspect. The throughput and memory requirements are the two important factors to be considered while designing ciphers. Classical ciphers can be made effective and used for providing security by adding the properties possessed by the modern ciphers. The key generation play a crucial role in designing the ciphers. The key should be truly random to increase confusion property of the cipher. The present paper has been designed with

Caesar cipher concept and transposition techniques to provide effective security. The system can be further improved by using modular arithmetic and exponential mathematical operations. The proposed method provides high throughput and occupies less memory.

8. REFERENCES :

[1] A.F.A.Abidin, O.Y. Chuan and M.R.K. ariffin-" A Novel enhancement Technique of the Hill Cipher for effective Cryptographic Purposes '- Journal of Computer science , 7(5): 785-789, 2011

[2] Dharmendra Kumar Gupta , Sumit Kumar Srivastava, Vedpal Singh- " New Concept of encryption algorithm A hybrid approach of Caesar Cipher and Columnar transposition in multi stages " – Journal of Global Research in Computer Science, Volume 3 , No. 1 , January 2012 , P. No. 60-66

[3] Fauzan Saeed , Mustafa Rashid- " Integrating Classical Encryption with Modern Technique " – IJCSNS, Volume 10, No. 5, May 2010

[4] Prof.K.Govinda , Dr.E. sathiyamoorth-"Multilevel Cryptography Technique Using Graceful Codes "- JGRCS, Volume 2, No.7, July 2011

[5] Monodeep Banerjee , Saptarshi Naskar , krishnendu Basuli , Samar Sen Sarma- " A Novel scheme for Text data encryption "- JGRCS, Volume 3, No.1, January 2012

[6] Phillip I Wilson and Mario Garcia – " A Modified Version of the Vigenere Algorithm "- IJCSNS, Vol. 6, No.3B, march 2006

[7] Packirisamy Murali and Gandhi doss Senthil Kumar – " Modified Version of Playfair cipher using Linear feedback Shift Register " – IJCSNS, Vol.8, No.12, December 2008

[8] Raj jain-"The art of Computer Systems Performance Analys is"-John Wiley & sons Inc.

[9] Rushdi. A. Hamamreh, Mousa Farajallah – " Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher "- IJCsNS, Volume 9, No.5, May 2009

[10] Sriram Ramanujam , Mrimuthu Karuppiah – " Designing an algorithm with high Avalanche effect "- International Journal of Computer Science and Network Security ", - Volume 11, No.1 , January 2011

[11] http://en.wikipedia.org/wiki/Caesar_cipher

[12] William Stallings- " Cryptography and Network security, Second Edition

*****