International Journal of Security and Its Application
Vol.11, No.3 (2017), pp.33-40
http://dx.doi.org/10.14257/ijsia.2017.11.2.04

Diversified Caesar Cipher for Impeccable Security

[1]Priya Verma, [2]Gurjot Singh Gaba, [3]Rajan Miglani*

[1,2,3]Discipline of Electronics and Communication Engineering
Lovely Professional University, Phagwara, Punjab, India - 144411
[1]priyaverma1740@gmail.com, [2]er.gurjotgaba@gmail.com
**Corresponding Author – [3]rajan.16957@lpu.co.in*

Abstract

In the communication systems, two parties are involved in the communication i.e. sender and receiver. Both the parties share the information after encryption with secret key. It is very dangerous to transmit the information over internet without encryption because of various potential attacks. Attackers always try to capture the information that is sent between sender and receiver. Various techniques are emerged to provide information security. Caesar cipher is one of the encryption techniques which encrypt message in the form of alphabets only. In this paper, a new improved technique of Caesar cipher is proposed in which encryption is not restricted only to alphabets. The diversified Caesar cipher has capability to encrypt symbols, characters as well as digits. A new character value table is also proposed which specifies the positions of symbols, characters and digits in the table. Moreover, matrix concept is used to make the Caesar cipher more complex which creates difficulty for brute force attacker to determine the key value.

Keywords*: cryptography; plaintext; cipher text; encryption; decryption; brute force attack.*

1. Introduction

In our day to day transactions, for example, using debit and credit cards, checking emails, etc. has made information security, a very necessary component for applications using Internet. Different cryptography methods are suggested by the researchers to encrypt the data in the past. But the attackers are always trying to hack the information and retrieving secret keys by various means. Many organizations are working hard to secure themselves from the growing threats of message hacking through various trends in cryptography. In cryptography [10], the message is encrypted with encryption algorithm [1] and the secret key as depicted in figure 1. At the receiver side, decryption is done with the decryption algorithm and the same secret key sent by the sender. The most widely known encryption technique in cryptography is Caesar Cipher [2, 9]. In Caesar cipher, characters of plaintext are replaced with fixed number of locations down the alphabet. It is also called 'shift cipher'. This method is used by Julius Caesar to communicate with his generals. It is more prone to attacks because the key ranges between 1 to 26. Brute force attacker tries all the possible combinations of keys and gets the message in a very easy way [5]. So the key should be more and more complex to create hindrance in brute force attack [11].

Symmetric Encryption is carried out in this way:

$$c = E(k, p) = (p + k) \bmod 26 \quad (1)$$

The decryption process is inverse of Encryption:

* Corresponding Author

ISSN: 1738-9976 IJSIA

$$p = D(k, c) = (c - k) \bmod 26 \quad (2)$$

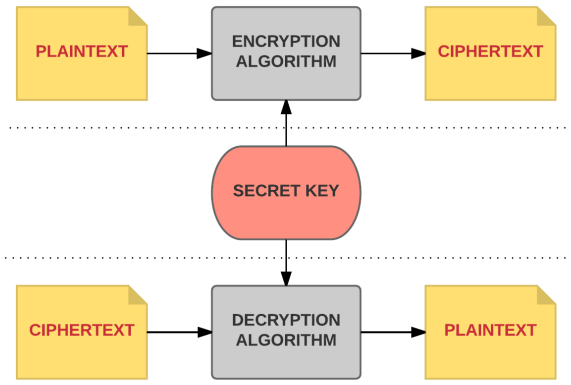

Figure 1. Encryption/Decryption Model

The basic and the traditional Caesar cipher works only on shifting of characters based on the key value [4]. The Caesar cipher with key value of 3 would behave in this way:

Plaintext	ARE YOU READY
Cipher text	DUH BRX UHDGB

2. Related Work

Pranab Garg (2014), et al. in paper entitled *"A Review Paper on Cryptography and Significance of Key Length"* states that for the secure communication of data over networks, cryptography is mandate. The authors suggested various cryptography algorithms which are currently used for encryption. These algorithms are Public Key Algorithm, Symmetric Key Algorithm, and Hash Function. In public key cryptography, constant key is employed by sender and receiver to encipher and decipher the message. In asymmetric key cryptography, two different keys are used i.e. personal key and public key. Personal key's held by the receiver. Public key's disclosed to the general public. RSA, Diffie-Hellman, Digital Signature algorithmic program (DSA), are the general public key algorithms. Hash functions are those algorithms that use no key for its operation.

Lim Chong Han (2014), et al. in paper entitled "*An Implementation of Caesar Cipher and XOR Encryption Technique in a Secure Wireless Communication*" proposed a technique for the secure transmission of data over the networks, which includes three stages i.e. Encryption design technique, serial port communication program and encoding pattern design. In their work, XOR technique is integrated with Caesar Cipher to extend complexity [6].

Rajan (2014), et al. in paper entitled "*Advancement in Caesar cipher by randomization and delta formation*" proposed a technique in which Caesar cipher is extended using randomization and delta formation. In this method, encryption process is divided into three parts i.e. Randomization, Encryption and Delta formation. A random key table is generated in this technique to confuse the hacker. This technique generates potential combinations of 26!*9. Here, the life time of the new algorithm: $(1.4346 \times 10^{32}) / (348 \times 10^{8}) = 4.20 \times 10^{21}$ seconds, that is around 1.334×10^{13}years [7].

3. Diversified Caesar Cipher (DCC)

Due to only 26 possible set of keys, Caesar cipher is considered to be less secure. Brute force attacker captures the message by trying all the possible set of keys [8]. To overcome the limitations of traditional Caesar ciphers, a new methodology is proposed in this paper which is coined as DCC.

3.1 Encryption Process

The encryption process is divided into three steps:

a) Formation of character value table

During the encryption process, a random character value table is formed (refer Table I) to enhance complexity of the algorithm by including symbols, digits, upper case and lower case characters so that Caesar cipher does not get easily susceptible to attacks. After that the complete message is divided into two parts. One part is termed as L.H.S and other one as R.H.S. Convert the message into decimal numbers after referring the Table I and then segregates the numbers based on their locations. Even location numbers and odd location numbers are segregated to achieve the principle of encryption/decryption.

b) Key generation

After selecting an initial key value, following steps were performed:-

i. Find the addition of even location numbers and then divide it by 2.
ii. Find the addition of odd location numbers and then divide it by 2.
iii. Then take the difference of step (i) and step (ii) and simply multiply it with the selected initial key value.

c) Encryption Methodology

i. Add the even and odd locations numbers with the key value and solve it by taking *mod 82* separately.
ii. Combine both the even and odd locations numbers and convert the decimal numbers into the characters/special characters through character value table.
iii. The resulting characters/numeric is Cipher text.

3.2 Decryption Process

It is the reverse of the encryption method. Firstly, convert the ciphertext into decimal form through Table I. Then fragment the total decimal numbers into two parts and subtract the key value from the numbers individually followed by mod 82 calculation. Resulting values of both fragments are combined according to the even and odd location of numbers. The numbers are then decrypted using Table 1. Thus, plaintext is obtained.

Table 1. Character Table

0	"	12	+	24	K	36	W	48	i	60	u	72	7
1	~	13	=	25	L	37	X	49	j	61	v	73	8
2	!	14	A	26	M	38	Y	50	k	62	w	74	9
3	@	15	B	27	N	39	Z	51	l	63	x	75	10
4	$	16	C	28	O	40	a	52	m	64	y	76	{
5	%	17	D	29	P	41	b	53	n	65	z	77	}
6	^	18	E	30	Q	42	c	54	o	66	1	78	:
7	&	19	F	31	R	43	d	55	p	67	2	79	;
8	*	20	G	32	S	44	e	56	q	68	3	80	/
9	(	21	H	33	T	45	f	57	r	69	4	81	\
10	)	22	I	34	U	46	g	58	s	70	5	82	|
11	_	23	J	35	V	47	h	59	t	71	6		

4. Results and Discussion

Let us suppose the message that we want to encrypt is:

"Message Encryption is done with his Intelligence"

Message →	**Left Hand Side**	**Right Hand Side**
	'Message Encryption is Do'	***'ne with his Intelligence'***
Numbers	26,44,58,58,40,46,44,18,53,42,57, 46,55,59,48,54,53,48,58,43,54	53,43,62,48,59,47,47,48,58,22,5 3,59,44,51,51,48,46,44,53,42,44

The numbers present in *Odd* Location in L.H.S are:

26, 58, 40, 44, 53, 57, 55, 48, 53, 58, 54

The numbers present in *Even* Location in L.H.S are:

44, 58, 46, 18, 42, 46, 59, 54, 48, 43

Key generation method:

Firstly, take key value from the user (K). Then, in order to secure the key, perform the following operations:

i. Addition of L.H.S. numbers is 476, when divided by 2, resulted in 238.
ii. Addition of R.H.S. numbers is 546, when divided by 2, resulted in 273.

N = |Difference of (i) and (ii)| = |238-273|= |35|

Key value generation	N × K
Let us suppose key value as 3	K = 3
Key Obtained	35 × 3 = 105

By performing the addition of key value in the even location of L.H.S. numbers, we get

A = [44+105, 58+105, 46+105, 42+105, 46+105, 59+105, 54+105, 48+105, 43+105] mod 82 (5)

After solving the above matrix, we get,

A= [67, 81, 69, 41, 65, 69, 82, 77, 71, 66] (6)

Similarly, for odd location numbers in L.H.S,

B = [26+105, 58+105, 40+105, 44+105, 53+105, 57+105, 55+105, 48+105, 53+105, 58+105, 54+105] mod 82 (7)

After solving the matrix, we get,

B = [49, 81, 63, 67, 76, 80, 78, 71, 76, 81, 77] (8)

Now, arrange the value of A and B in increasing order,

67, 81, 69, 41, 65, 69, 82, 77, 71, 66, 49, 81, 63, 67, 76, 80, 78, 71, 76, 81, 77

Convert these decimal numbers into the corresponding characters or special characters after referring character value table.

Final Cipher text obtained is:

2\4bz4|}61j\x2{/:6{|}

Similarly, R.H.S part of the message can be encrypted.

Analysis of Decryption Process

In case of decryption, perform all the steps in reverse order.

Obtained Ciphertext is

2\4bz4|}61j\x2{/:6{|}

The decimal value of ciphertext is

67, 81, 69, 41, 65, 69, 82, 77, 71, 66, 49, 81, 63, 67, 76, 80, 78, 71, 76, 81, 77

Now, divide the decimal values into two parts:

A = [67, 81, 69, 41, 65, 69, 82, 77, 71, 66] (9)

B = [49, 81, 63, 67, 76, 80, 78, 71, 76, 81, 77] (10)

Key value is *'105'*

Perform the operation of subtracting the Key from A and B,

A = [105-67, 105-81, 105-69, 105-41, 105-65, 105-69, 105-82, 105-77, 105-71, 105-66] mod 82 (11)

B = [105-49, 105-81, 105-63, 105-67, 105-76, 105-80, 105-78, 105-71, 105-76, 105-81, 105-77] mod 82 (12)

Final Result is:

A = [44, 58, 46, 18, 42, 46, 59, 54, 48, 43] (13)

B = [26, 58, 40, 44, 53, 57, 55, 48, 53, 58, 54] (14)

Then combine both A and B according to even and odd number

26, 44, 58, 58, 40, 46, 44, 18, 53, 42, 57, 46, 55, 59, 48, 54, 53, 48, 58, 43, 54

Final decrypted message is:

"Message Encryption is Do"

Similarly, R.H.S of the message is decrypted.

Table 2. Comparison of Existing and Proposed Technique of caesar Cipher

PARAMETERS	EXISTING CAESAR CIPHER [4]	DIVERSIFIED CAESAR CIPHER
Complexity	Less	Severe
Operations Performed	Less	More
Key Size	Small	Large
Brute Force Attack	Easily Carried out	Difficult to conduct
Security	Inferior	Decent

Table 2 shows the comparison of the existing Caesar cipher and proposed technique (DCC) on the basis of various parameters. It is analyzed from the table that existing Caesar cipher provides less security and is more prone to brute force attack.

4. Conclusion

It is found that the previous Caesar cipher is less secure because of its simplicity in operation of encryption. But the ciphertext result we obtained in proposed technique contains symbols, digits, upper case and lower case characters which enhance the performance of Caesar cipher. In the proposed technique, the key size is 82. So brute force attacker has to try 82! possible combinations to decrypt the message which could create trouble for him. The proposed technique has prolonged lifetime of the cryptography algorithm than the existing algorithm. Hence this technique is found to be more secure!!

References

[1] R. Mane, "A Review on Cryptography Algorithms, Attacks and Encryption Tools," International Journal of Innovative Research in Computer and Communication Engineering., vol. 3, no. 9, **(2015)**, pp.8509-8514.

[2] G. Gupta, R. Chawla, "Review on Encryption Ciphers of Cryptography in Network Security," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 7, **(2012)**, pp.1-26.

[3] S. Chandra, "A comparative survey of Symmetric and Asymmetric Key Cryptography," International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, **(2014)**, pp. 83–93.
[4] S. Shakti, "Encryption using different techniques," International Journal in Multidisciplinary and Academic Research (SSIJMAR)., vol. 2, no.1, **(2013),** pp. 1-9.
[5] P. Garg, "A Review Paper on Cryptography and Significance of Key Length," International Journal of computer science and communication engineering, vol. 2, **(2012)**, pp.88-91.
[6] L.C. Han, N.M. Mahyuddin, "An Implementation of Caesar Cipher and XOR Encryption Technique in a Secure Wireless Communication," 2nd International conference on Electronic Design (ICED), Penang, **(2014),** pp.111-116.
[7] A.Rajan and D. Balakumaran, "Advancement in Caesar cipher by randomization and delta formation," International conference on Information communication and Embedded systems (ICICES), Chennai, **(2014)**, pp.1-4.
[8] K. Goyal, S. Kinger, "Modified Caesar Cipher for Better Security Enhancement," International Journal of Computer Applications, vol. 73, no.3, **(2013)**, pp. 27-31.
[9] S.B. Dar, "Enhancing the Security of Caesar Cipher Using Double Substitution Method," International Journal of Computer Science & Engineering Technology, vol. 5, no. 7,**(2014)**, pp.772-774.
[10] William Stallings, "Cryptography and Network Security: Principles & Practices", New York, NY: Pearson Education, **(2006).**
[11] Y. S. Rajput, "An Improved Cryptographic Technique to Encrypt Text using Double Encryption," International journal of Computer Science & Engineering Technology, vol.8, no. 11,**(2014)**, pp. 886-892.

Authors

Gurjot Singh Gaba, is currently pursuing Ph.D. in Electronics & Electrical Engineering with Spl. in *Cryptography and Network Security of WSN and IoT's*. He is working as an Asst. Prof. in Lovely Professional University, India since 2011. His research interest includes Wireless Sensor Networks, Computer Networks, Optical Communications and Cryptography. He is a reviewer of SCIE and Scopus Indexed Journals. He has recently been appointed as Editor of IJEEE journal. He is a member of many technical bodies including ISCA, IAENG, IACSIT, CSI, and ISTE. He is an author of six International books and more than two dozen research papers.

Priya Verma, has completed her M.Tech in Electronics and Communication Engineering with Spl. in Wireless Communication Systems at Lovely Professional University, India. Her research interests include Wireless Sensor Networks, Cryptography and Network Security.

Rajan Miglani, is currently pursuing Ph.D. *in Optical Communications*. He is associated with Lovely Professional University, India since 2012 as an Asst Prof in department of Communication systems. His research interests include Optical and Wireless Networks, Optical computing and processing, Cryptography and Wireless Sensor Networks. He has authored and guided numerous research papers, published in various reputed journals around the world.