Review Article | Impact Factor: 0.621 | ISSN: 2319-507X
Sandip Raut, IJPRET, 2014; Volume 2 (9): 1180-1189 | IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

LIGHTWEIGHT ENCRYPTION- DECRYPTION TECHNIQUE

SANDIP S. RAUT[1], PROF. DHANANJAY M. DAKHANE[2], PROF. RAVINDRA L. PARDHI[2]

1. 2 nd Sem M. E, Computer Engineering, Sipna C.O.E.T, Amaravati, India.
2. Dept. Computer Science and Engineering, Sipna C.O.E.T, Amaravati, India.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: In cryptosystem there are set of rule for how to encrypt the plaintext and how to decrypt the cipher text. Encryption is the conversion of data into a form called cipher text, that cannot be easily understood by unauthorized people. Decryption is the process of converting data into its original form so it can be understood. 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, we modified the traditional Caesar cipher. Another thing alphabet index is checked and divide the alphabet index by two and collect the quotient if the index value of plaintext is even then replace the alphabet otherwise replace special symbol. Encryption and scrambling of the letters in the Cipher Text.

Keywords: Caesar Cipher; Cryptography; Encryption; Decryption

PAPER-QR CODE

Corresponding Author: MR. SANDIP S. RAUT

Access Online On:

www.ijpret.com

How to Cite This Article:

Sandip Raut, IJPRET, 2014; Volume 2 (9): 1180-1189

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 very crucial part to transfer data and to keep confidential is a big concern and 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. While transferring a data there is a no privilege to intruder to access authorized data or the confidential data. 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. Cryptography is a technique to transfer a data without understanding to third party, convert the plain text into non readable form at sender side and then only the receiver knows how to get original plain text. 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].

II. CRYPTOGRAPHY

Cryptography is the science of data security. 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].

Modern cryptography concerns itself with the following four objectives:
1) Confidentiality: the information cannot be understood by anyone for whom it was unintended

2) Integrity: the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected

3) Non-repudiation: the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information

4) Authentication: the sender and receiver can confirm each others identity and the origin/destination of the information

2.1 Symmetric Encryption

Symmetric cryptography is cryptography in which a single or secret key is used to encrypt and decrypt a message so that it arrives securely. 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].

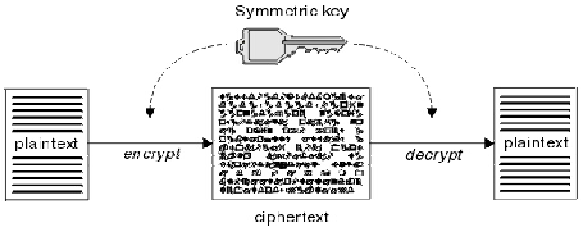

Fig 1: Shows the working of symmetric encryption.

2.2 Asymmetric Encryption

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. This also allows for the exchanging of securely signed and one-to-one messages, as follows. The sender encrypts the message using the common algorithm and his own secret key. They then sign the result, encrypt it again using the recipient's public key, and send it. The recipient decrypts the received message using their own secret key, identifies the sender from their now-clear text signature, and then decrypt the result using the sender's public key.

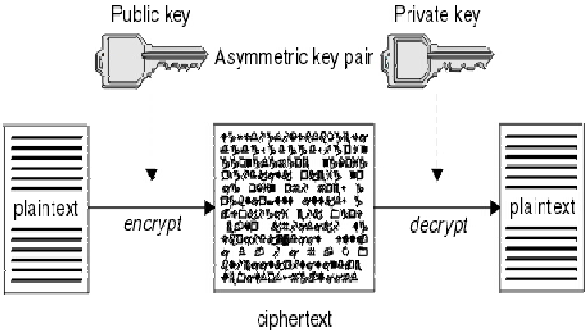

Fig 2: Public Key Cryptography Process

II. RELATED WORK

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.

III. PROPOSED 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. Author of [14] proposed a 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.

In this paper we proposed new method, a alphabet index is checked and divide the alphabet index by two and collect the quotient if the index value of plaintext is even then replace the alphabet otherwise replace special symbol.

Encryption Algorithm

Step 1:Take a plain text as input.

Step 2:check alphabet or numeric value.

Step 3: if (Alphabet)

Check index value

If (Even)

Collect the quotient and replace alphabet

Else (odd)

Collect quotient and replace symbol

Step 4: For numeric value

If (Even)

Increase value by one

Else (odd)

Decrease value by one

Step5: Get the encrypted text.

Decryption Algorithm

Step 1:Insert cipher text.

Step 2:check it is alphabet, symbol or numeric value.

Step 3:If (Alphabet)

2*index value

Else (symbol)

2*Assign value of symbol

Step 4:Numeric value.

If (Even)

Decrease value by one

Else (odd)

Increase value by one

Step 5: Get the plain text.

Table 1. Mapping table for uppercase alphabets

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

Table 2. Mapping table for Lowercase alphabets

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

Table 3. Key for odd number

D	F	H	J	L	N	P	R	T	V	X	Z
D*	F*	H*	J*	L*	N*	P*	R*	T*	V*	X*	Z*

Table 4. 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

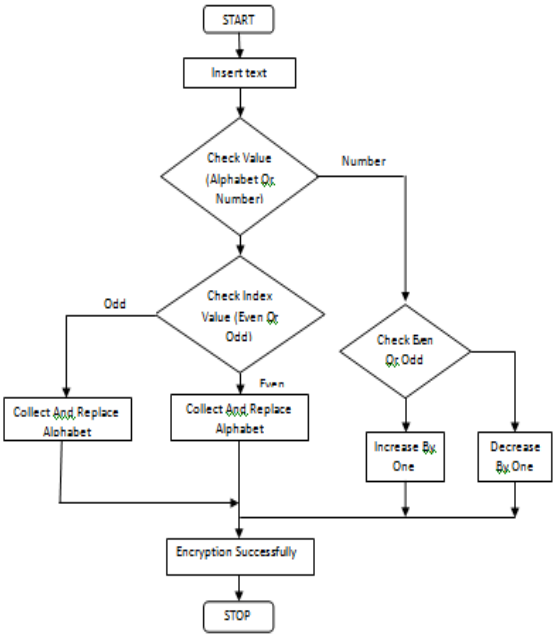

Fig 3: Encryption Process

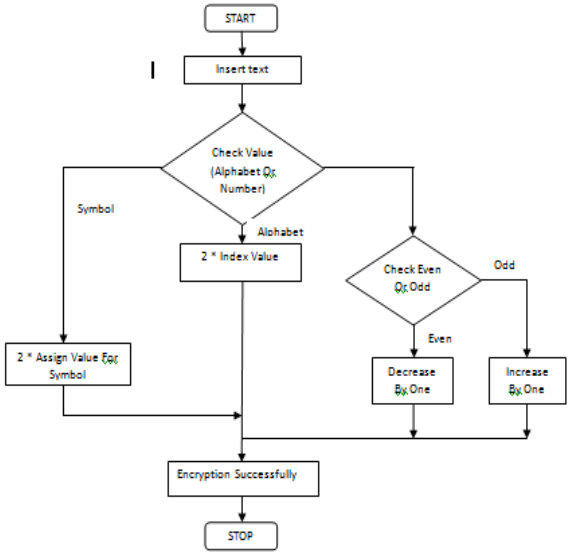

Fig 4: Decryption Process

IV. EXPERIMENTAL RESULTS

Step 1: Suppose original message is Computer123

Step 2: Now apply Caesar cipher to encrypt the plain text.

Index is checked and divide the alphabet index by two and collect the quotient if the index value of plaintext is even then replace the alphabet otherwise replace special symbol.

Experimental Example

2 14 12 15 20 19 4 17

C O M P U T E R

2/2 14/2 12/2 15/2 20/2 19/2 4/2 17/2

=1 =7 =6 =7.5 =10 =9.5 =2 =8.5

b h g p* k t* c r*

1*2 7*2 6*2 7.5*2 10*2 9.5*2 2*2 8.5*2

=2 =14 =12 =15 =20 =19 =4 =17

C O M P U T E R

We get 'bhgp*kt*cr*' as cipher text because the index value of C is 2 while dividing 2/2 we get 1 as quotient. The alphabet at position 1 is b (as shown in table 2). If the index of original plaintext is odd then we replace special symbol.

V. CONCLUSION

In this paper we design algorithm of security i.e. modified version of Caesar cipher. Cryptography are used which makes it difficult to detect the presence of hidden message. But in some cases if the eavesdropper has attacked the carrier of message then he will not be able to get the original message as all the relevant data here is in encrypted form. 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.

VI. 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. Kashish Goyal, Supriya Kinger "Modified Caesar Cipher for Better Security Enhancement" International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013.