Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Caesar Cipher with Complement Approach

Sailakshimi.S
Research Scholar
Department of Computer Science
Adhiparasakthi College of Arts and Science,
Kalavai, Tamil Nadu, India

Sasikala.G
Assistant Professor
Department of Computer Science
Adhiparasakthi College of Arts and Science,
Kalavai, Tamil Nadu, India

Abstract— Cryptography is of knowledge and talent to transmit message towards sender and receiver with more security. It converts message into non-readable form and protect communication from illegal user. Cryptography has two types of text one is ordinary text or plain text and another is cipher text. Ordinary text is message of sender or receiver. Cipher text is message in the form of unreadable. Cryptography contains two major processes encryption and decryption. Encryption is the process of converting ordinary text into cipher text. Decryption is the process of converting cipher text into ordinary text. There are several techniques in cryptography to encrypt and decrypt the text. In this paper we propose Caesar cipher with a new technique by using two levels XOR with complement approach. Sometimes messages can be easily identified by the hackers and unauthorized users. To avoid this problem we are using complement approach and two levels XOR operations that to make cipher text protected and it's very difficult to break message by unauthorized users. So this technique is useful to send and receive message with in personal, reliability and authorization.

***Keywords— cryptograph y, encryption, decryption, XOR, cipher*.**

I. INTRODUCTION

Cryptography is an area focus on hiding message from unauthorized user. While message is intend to send as original text but message actually received as cipher text. Unless we don't know secret code for cipher text we cannot identify original text. A Cryptographic is a technique that used to afford encryption and decryption. Encryption is a method of converting user message in to non-readable form that is cipher text. Decryption is a method of converting cipher text into readable form that is original text. Transposition and substitution are two techniques for the encryption. In transposition technique we are converting ordinary text to cipher text by using the any kind of permutation method on the message. Example for transposition methods are Rail fence and columnar method. In substitution technique we are converting message into cipher text by replacing any alphabet, symbol or number. Example for substitution methods are caesar cipher, monoalphabetic , playfair and hillcipher. In normal Caesar cipher method we are replacing the message into cipher text by adding same number to all the text. Due to modern technology we can easily split and identify the cipher text by non permitted user. To avoid this problem we should develop more security to cipher text. So in this paper we develop two-level of XOR and complement approach to make a cipher text more secure and it's very difficult to identify by illegal user.

II. RELATED WORK

Sharad patali et.el[1] describes the major complexity of one time pad is key distribution. To solve this problem they use performance for one time pad with binary addition via 2's complement approach. In this paper they proved that one time pad is unbreakable hypothetically, for this reason the scheme is practical for things similar to communicating with high values of security. To make attacker life difficult they use a complement approach for the cipher text. So that attacker cannot identify text easily. They also given idea for future research we can design algorithm in modular arithmetic with 2's complement binary addition, multiplication and division concepts.

Ochoche Abraham et.el[2] describes some new techniques to the traditional Caesar cipher algorithm, which entirely eliminates primary weak point. First they avoid spaces from cipher text and second they creating cipher text to the improved caesar cipher(ICC). They provide two steps encryption and scuttle the letters in the cipher text. So even if it's decrypted the result would be rubbish. To complete the fortification spaces in between words were avoided and encrypted were jumbled to from a permanent stream's of character

Ch .santhosh reddy et.el[3] describes various types of cryptography and different keys in cryptography. They given a brief explanation about symmetric key algorithm and they proposed new algorithm in symmetric key cryptography. In proposed algorithm they use two levels XOR Operation for encryption and decryption algorithm and therefore hackers cannot identify message easily. They proved that algorithm that contains similar type text in to dissimilar type of cipher text. It works efficiently for huge amount of data.

Prachi patni[4] describes some variation in caesar cipher. In classical cipher we are using mono alphabetic and stable key length during text file to be encrypted. Once attacker identify key of Caesar cipher we can easily broken text. To overcome in this problem they use variable key for each character in proposed algorithm. Plain text can be encrypt in such a way so it very difficult to be decrypt. we use poly-alphabetic cipher technique in modified caesar cipher when plain text is encrypted. The encryption made using variable length key which depends on time of the file, place of character and string length. Receiver end time and file name given to the receiver if they knows decryption key they can easily identify original message.

III. METHODOLOGY

In this paper when sender gives an ordinary text each character in the text, gets ASCII number and it converts equivalent eight bit binary number format. Then we are giving eight bit binary format prime number as random key. We performing first level XOR operation for ordinary text and prime number so we get first level result then we convert in to 1's complement number called as complement number. Then perform second level XOR operation for complement number along with same prime number and we will get eight bit binary number. Now we convert binary into decimal value . We take decimal value as an ASCII value and mark corresponding character for that ASCII number. Character acts as cipher text. It provides more secure for the information.

IV. ALGORITHM

A. ENCRYPTION ALGORITHM

STEP1: Consider the ordinary text (message). Mark the ASCII value of each character from the chart.
STEP2: Change decimal value into eight bit binary number.
STEP3: Choose any prime number and convert into eight bit binary number as a random key.
STEP4: Do first level XOR for random key and ordinary text. We get first level result.
STEP5: Then convert first level result into one's complement. This number is called complement number.
STEP6: Perform second level XOR for same random key and complement number. Now we obtain eight bit binary result.
STEP7: Convert eight bit binary result into decimal value.
STEP8: Take decimal value result as a ASCII value.
STEP9: Get corresponding symbol for that ASCII value.
STEP10: At this instant we get cipher text.

B. DECRYPTION ALGORITHM

STEP1: Convert cipher text corresponding ASCII value.
STEP2: Convert decimal value into eight bit binary number.
STEP3: Use same prime number as random key.
STEP4: Do first level XOR for random key and cipher text. We get first level result.
STEP5: Then convert first level result into one's complement. This number is called complement number.
STEP6: Perform second level XOR for same random key and complement number. Now obtain eight bit binary result.
STEP7: Convert eight bit binary result into decimal value.
STEP8: Take decimal value result as a ASCII value.
STEP9: Get corresponding symbol for that ASCII value.
STEP10: At this instant we get original message.

V. IMPLEMENTATION

ENCRYPTION MESSAGE: BEST

TABLE I.ENCRYPTION TABLE

ORIGINAL MESSAGE	B	E	S	T
ASCII VALUE	66	69	83	84
BINARY VALUE	01000010	01000101	01010011	01010100
PRIME NUMBER	00000011	00000011	00000011	00000011
XOR RESULT 1	01000001	01000110	01010000	01010111
COMPLEMENT NUMBER	10111110	10111001	10101111	10101000
PRIME NUMBER	00000011	00000011	00000011	00000011
XOR RESULT 2	10111101	10111010	10101100	10101011
DECIMAL VALUE	189	186	172	171
CIPHER TEXT	╜	║	¼	½

CIPHER TEXT: ╜ ║ ¼ ½
DECRYPTION MESSAGE: ╜ ║ ¼ ½

TABLE II. DECRYPTION TABLE

CIPHER TEXT	╝	║	¼	½
ASCII VALUE	**189**	**186**	**172**	**171**
BINARY VALUE	**10111101**	**10111010**	**10101100**	**10101011**
PRIME NUMBER	**00000011**	**00000011**	**00000011**	**00000011**
XOR RESULT1	**10111110**	**10111001**	**10101111**	**10101000**
COMPLEMENT NUMBER	**01000001**	**01000110**	**01010000**	**01010111**
PRIME NUMBER	**00000011**	**00000011**	**00000011**	**00000011**
XOR RESULT2	**01000010**	**01000101**	**01010011**	**01010100**
DECIMAL VALUE	**66**	**69**	**83**	**84**
ORIGINAL MESSAGE	**B**	**E**	**S**	**T**

ORIGINAL MESSAGE: BEST

VI. CONCLUSION

In this paper we proposed caesar cipher through a new technique by using two levels XOR with complement approach .This algorithm make a cipher text very complicated and it cannot break by unauthorized user. It works very smoothly for large amount of data. So sender and receiver can send and receive message with more security and personal.

REFERENCES

[1] Sharad patali ,"*Effective secure encryption scheme using complement approach*".

[2] Ochoche Abraham, "*An improved Caesar cipher algorithm*" international journal of engineering and advanced technology , volume -2,issue -5, 1198-1202.

[3] Ch .santhosh reddy "*Poly-alphabetic symmetric key algorithm using randomized prime numbers*" international journal of scientific and research publications volume-2, issue-9, September 2012, ISSN 2250-3153.

[4] Prachi patni "*A poly-alphabetic approach to Caesar cipher algorithm*" international journal of computer science and information technologies, volume-4 (6), 2013, ISSN 0975-9646.