ISSN 2250-3153

Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers

Ch. Santhosh Reddy, Ch. Sowjanya, P. Praveena, Prof Shalini L

School of Computing Science and Engineering
VIT University, Vellore, Tamilnadu – 632 014, India

Abstract- Cryptography is an art and science. It is a playing major role in information and security division. The main aim of the cryptography is protecting the data from unauthorized users or hackers. "Cryptography is subject contains two parts one is encryption and another one decryption. Encryption is a process converting the plain text to cipher text using some keys. Decryption is a process of converting the cipher text to plain text using the keys". There are several algorithms in cryptography to encode and decode the data based on the key.
This paper discusses types of cryptography and different keys in cryptography. The paper can give brief description about symmetric key algorithms and we are proposing new algorithm in symmetric key cryptography. The proposed algorithm contains two levels of Exclusive OR (XOR) operation. This algorithm is useful in transmission of messages and data between one user and another.

Index Terms- Cryptography, Encryption, Decryption, Symmetric Key.

I. INTRODUCTION

Cryptography is a subject concentrate on hiding the text or information secretly. Cryptography is branch of Mathematics and Computer Science. The modern Cryptography is providing the platform to store the important data secretly or publicly, for example Digital Signatures, Online authentication and mainly in Communications. In telecommunication cryptography is necessary when communicating over any unauthorized medium, which includes just about any network, particularly the Internet and online communication [1]. From 1900 B.C onwards Egyptians were introduced this concept.
Cryptography not only protects the data from theft or alteration, but also be used for user authentication [1]. Cryptography is combination of encryption and decryption. Encryption is a process of converting the plain text to cipher text using with some keys, whereas decryption is process of converting the cipher text to plain text using with same key or other key.
Cryptography algorithms mainly broadcasted into two ways based on the key distribution. They are Symmetric Key algorithm (Private Key algorithm), Asymmetric key algorithm (Public Key algorithm).

A. Asymmetric Key algorithms

Asymmetric key algorithms also called public key algorithms. In public key algorithm both parties (sender and receiver) having their own different keys. At the sender encrypt the data with his own key, and receiver decrypt the data with his own key. In some situation the both parties use the additional key, which is common to both parties. First they will do the encryption or decryption with the same key, and again do the encryption or decryption with their own key. Example for public key algorithms is RSA, Diffie Hellman key exchange protocol.

B. Symmetric key algorithms

Symmetric algorithms is also called as secrete key algorithms. In secrete key algorithms both parties (Sender, Receiver) will use the same key to encrypt or decrypt the data. Example for symmetric key algorithms is DES, AES, Triple DES, and Blowfish.

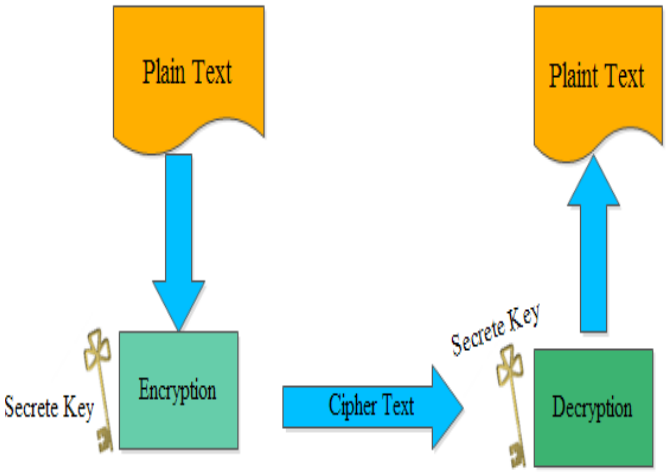


Fig 1: Secrete key algorithm

II. EXISTED SYSTEM

In existed system many of the algorithms encrypting the plain text to cipher text. But the algorithms applying same encryption process to entire plain text. So if the same type of characters repeated in plain text, that all characters converting into the same type of cipher text. The cryptanalysis for this type of cipher texts is becoming easy process. For example if the plain text is "BANANA". In this plain text 'A' is repeated 3 times and 'N' is repeated 2 times. In the present existed algorithms 3A's and 2N's will be encrypted in to same characters. In decryption 3 characters is enough to get this plain text. For those texts cryptanalysis will become easy for these type plain texts.

III. PROPOSED ALGORITHM

Encryption:

P=plain Text

1. Add the randomized characters in between the plain text. For every 3 characters add one duplicate character.
2. Get the ASCII codes for the characters in plain text.
3. Convert the ASCII codes into Binary format.
4. Do the complement of the plain text.
5. Select any series of prime numbers and convert into Binary format.
6. Do the first level Exclusive OR (XOR) between characters of plain text and selected series of prime numbers.
7. Select any Randomized number (key). Get the keythprime number from the prime numbers table.
8. Do the Second level of XOR operation between result of step5 and Randomized prime number.
9. Convert the result of step7 into decimal values. Now you will get the cipher text.

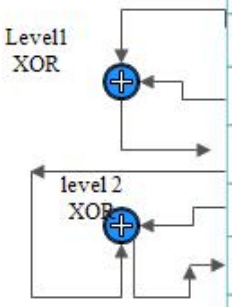
Decryption:

1. Convert the cipher text into Binary format. Get the Keythprime number from the prime numbers table. And convert it into binary format.
2. Do the first level of Exclusive OR (XOR) operation between cipher text and Keyth primary key.
3. Select the series of prime numbers and convert it into the binary format (the series must be same in both encryption side and decryption side).
4. Do second level of XOR operation between result of step2 and selected series of prime numbers.
5. Get complement of the result of step4.
6. Convert the result from binary to decimal format.
7. Remove the randomized stuffed numbers.
8. Now you can get the plaintext.

IV. EXAMPLE

Let's sample plain text is: BANANA

Encryption



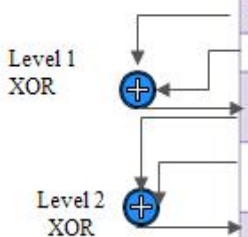
plaintext	B	A	N	X	A	N	A	S
ASCII	66	65	78	88	65	78	65	83
Binary number	01000010	01000001	01001110	1011000	01000001	01001110	01000001	1010011
Complement	10111101	10111110	10110001	10100111	10111110	10110001	10111110	10101100
Prime numbers	00011101	00011111	00100101	00101001	00101011	00101111	00110101	00111011
Level 1 Result	10100000	10100001	10010100	10001110	10010101	10011110	10001011	10010111
KEY	11100101	11100101	11100101	11100101	11100101	11100101	11100101	11100101
Level 2 Result	01000101	01000100	01110001	01101011	01110000	01111011	01101110	01110010
Cipher Text	69	68	113	107	112	123	110	114

Fig. 2 Encryption Table

- In the above table X and S randomly added characters.
- The used prime numbers for level1 encryption is: 29,31,37,41,43,47,51 and 53.
- The key is 50th prime numbers that is 229.

Decryption

- The Cipher text is 69, 68, 113, 107, 112, 123, 110, and 114.
- The Key K=50th prime number 229.
- The prime numbers for level 2XOR is 29,31,37,41,43,47,51 and 53.
- In the decryption table 88(X) and 83(S) is randomly added characters.
- After removing the stuffed characters the plain text P=BANANA.



Cipher text	69	68	113	107	112	123	110	114
Binary code	01000101	01000100	01110001	01101011	01110000	01111011	01101110	01110010
Key	11100101	11100101	11100101	11100101	11100101	11100101	11100101	11100101
Level 1 Result	10100000	10100001	10010100	10001110	10010101	10011110	10001011	10010111
Prime Number	00011101	00011111	00100101	00101001	00101011	00101111	00110101	00111011
Level 2 Result	10111101	10111110	10110001	10100111	10111110	10110001	10111110	10101100
Complement	01000010	01000001	01001110	01011000	01000001	01001110	01000001	01010011
P (ASCII)	66	65	78	88	65	78	65	83
Plain Text	**B**	**A**	**N**	-	**A**	**N**	**A**	-

Fig. 3Decryption table

V. ADVANTAGES OF PROPOSED SYSTEM

- Algorithm is very simple to implement.
- There are 2 levels of XOR operations in the algorithm. It makes very secure cipher text.
- The same repeated characters in plain text will be decoded into different cipher characters.
- For large amount of data this algorithm will works very smoothly.

VI. CONCLUSION

Large number of cryptography algorithms exists in the present scenario. Those algorithms work efficiently but the same type of plain text is converted into cipher text. This is the major drawback of the existing system. And the present symmetric key algorithms are taking huge amount of cost. The proposed algorithm in this paper is given as solution for the existing problem. This algorithm converts the same type text into different type of cipher text and works very smoothly for large amount of data.

REFERENCES

[1] Gary C. Kessler, "An overview of Cryptography", 1998, an article available at www.garykessler.net/library/crypto.htm

[2] S. William, "Cryptography and Network Security: Principles and Practice", 4th edition, Prentice-Hall, Inc., 2010.

[3] B. Forouzan, "Cryptography and Network Security" 4th edition, Mc Graw Hill, Inc 2007.

[4] Zakir H Sarker, Md. Shafiul Parvez, "A Cost Effective Symmetric Key cryptographic Algorithm for Small Amount of Data", IEEE, 1995.

[5] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, 2010.

[6] Sheetal Saigal, Saloni and Akshat Sharma, "A Secret Key Cryptographic Algorithm", Journal of computing, Volume 3, issue 8, August 2011.

[7] Atul kahate,"Computer and Network security", Tata Mc Graw Hill, 2nd edition 2008.

[8] S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html.

[9] M. Thogla "History of Cryptography", http://www.answers.com/topic/history-of-cryptography, written on 2007.

AUTHORS

First Author – Ch. Santhosh Reddy, M.Sc(Computer Science), School of Computing Science and Engineering, VIT University. Chsanthosh23@gmail.com.

Second Author – Ch. Sowjanya ,M.Sc(Computer Science), School of Computing Science and Engineering, VIT University.

Third Author – P. Praveena ,M.Sc(Computer Science), School of Computing Science and Engineering, VIT University.

Fourth Author – L. Shalini, asst. professor, School of Computing Science and Engineering, VIT University.