

Character-Based Symmetric Key Algorithm using Randomized Prime Numbers

K. Purushotam Naidu¹, V. Lakshmana Rao², A. Uday Kumar³

¹Gayatri Vidya Parishad College of Engineering for Women, Visakhapatnam, Andhra Pradesh

²Gayatri Vidya Parishad College of Engineering for Women, Visakhapatnam, Andhra Pradesh

³Gayatri Vidya Parishad College of Engineering for Women, Visakhapatnam, Andhra Pradesh

Abstract- This paper deals with the types of cryptography and different keys in cryptography. It gives a brief description about symmetric key algorithms. In the existing system many of the algorithms encrypt the plain text to cipher text. But the algorithms apply the same encryption process to the entire plain text. So if the same type of characters are repeated in plain text then all the characters are converted into the same type of cipher text. The cryptanalysis for this type of cipher text is becoming an easy process for the hacker. So we are proposing a new algorithm in symmetric key cryptography. The proposed algorithm contains two levels of Exclusive OR (XOR) operations. This algorithm produces different cipher text to the same plain text. Here we also use a series of prime numbers in order to increase the complexity for unauthorized users.

I. INTRODUCTION

Cryptography is a practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence the adversaries and which are

and diplomats. In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs and secure computation, among others.

The modern field of cryptography can be divided into several areas of study.

[A] Asymmetric Key Algorithms

Asymmetric key algorithms are also called public key algorithms. In public key algorithms both parties (sender and receiver) have their own different keys. The Sender will encrypt the data with his own key and the receiver will decrypt the data with his own key. In some situations both parties use an additional key which is common to both the 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 algorithm is RSA, Diffie Hellman key exchange protocol.

related to various aspects of information security such as data confidentiality, data integrity, authentication, and non-repudiation. Applications of cryptography include ATM cards, computer passwords and electronic commerce.

Modern cryptography is heavily based on mathematical theory and computer science practice. Cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure, theoretical advances and faster computing technology requires these solutions to be continually adapted.

Before the modern era, cryptography was concerned solely with message confidentiality (i.e. encryption) – conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret. Encryption is used to ensure secrecy in communications, such as those of spies, military leaders,

[B] Symmetric Key Algorithms

Symmetric algorithms are also called secret key algorithms. In secret key algorithms both the parties (sender and receiver) will use the same key to encrypt or decrypt the data. Example for symmetric key algorithms are DES, AES, TDES and Blowfish.



Fig 1: Secret key algorithm

II. EXISTING SYSTEM

In the existing system many of the algorithms encrypt the plain text to cipher text but they produce same cipher text for the characters repeated in the plain text. The

cryptanalysis for this type of cipher text is becoming an easy process. For example if the plain text is "TOMATO". In this plain text "T" is repeated twice and "O" is repeated twice. In the present existing algorithms 2T's and 2O's will be encrypted in to the same characters. In decryption 4 characters is enough to get this plain text.

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.

DECRYPTION:

1. Convert the cipher text into binary format. Get the Keyth prime number from the prime numbers table and convert into binary format.
2. Do the first level XOR operation between cipher text and Key.
3. Select the series of prime numbers and convert into binary format (the series must be same in both encryption and decryption).
4. Do the second level XOR between result of step-2 and the selected series of prime numbers.
5. Get the compliment of the result of step-4.
6. Convert the result from binary format to decimal format
7. Remove the randomized stuffed characters.
8. Now you can get the plain text.

IV. EXAMPLE

Consider a sample plain text: TOMATO

3. Convert the ASCII codes into binary format.
4. Do the compliment of the pain 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 Keyth prime number from the prime numbers table.
8. Do the second level Exclusive OR (XOR) operation between the result of step-5 and the Key.
9. Convert the result of step-7 into decimal values. Now you will get the cipher text.

ENCRYPTION

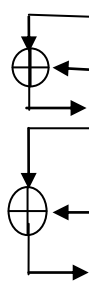
- In the below table X and S are randomly added characters.
- The used prime numbers for level1 encryption are: 29,31,37,41,43,47,53 and 59.
- The key is 50th prime number that i.e., 229.

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 level2 XOR are 29, 31, 37, 41, 43, 47, 53 and 59
- In the decryption table 88(X) and 83(S) are randomly added characters.
- After removing the stuffed characters the plain text P=TOMXATO

1 Plaintext	T	O	M	X	A	T	O	S
ASCII	84	79	77	88	65	84	79	83
Binary number	01010100	01001111	01001101	01011000	01000001	01010100	01001111	01010011
Complement	10101011	10110000	10110010	10100111	10111110	10101011	10110000	10101100
Prime numbers	00011101	00011111	00100101	00101001	00101011	00101111	00110101	00111011
Level1 result	10110110	10101111	10010111	10001110	10010101	10000100	10000101	10010111
KEY	11100101	11100101	11100101	11100101	11100101	11100101	11100101	11100101
Level2 result	01010011	01001010	01110010	01101011	01110000	01100001	01100000	01110010
Cipher text	19	74	114	107	112	97	96	114

Encryption Table



Cipher text	19	74	114	107	112	97	96	114
Binary format	01010011	01001010	01110010	01101011	01110000	01100001	01100000	01110010
KEY	11100101	11100101	11100101	11100101	11100101	11100101	11100101	11100101
Level1 result	10110110	10101111	10010111	10001110	10010101	10000100	10000101	10010111
Prime numbers	00011101	00011111	00100101	00101001	00101011	00101111	00110101	00111011
Level2 result	10101011	10110000	10110010	10100111	10111110	10101011	10110000	10101100
Complement	01010100	01001111	01001101	01011000	01000001	01010100	01001111	01010011
ASCII	84	79	77	88	65	84	79	83
Plain text	T	O	M	-	A	T	O	-

Decryption Table

V. ADVANTAGES OF THE PROPOSED ALGORITHM

- 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 work very smoothly.

VI. CONCLUSION

Large number of cryptography algorithms exist 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. The present symmetric key algorithms are taking huge amount of cost. The proposed algorithm in this paper is given as a solution for the existing problem. This algorithm converts same type of text into different types of cipher text and works very smoothly for large amount of data.

The future enhancement is that this algorithm can also be implemented for providing security for image, audio and video files.

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. Shafiu 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>