Nearest Prime Cipher for Data Confidentiality and Integrity

Dr. S. Kiran
Assistant Professor, Dept of CSE, YSREC of YV University, Proddatur, India
Email: rkirans125@gmail.com
N. Subramanyan
Teaching Assistant, Dept of CSE, YSREC of YV University, Proddatur, India
Email: subramanyam.neelam@gmail.com
Y. Suma
Student, III B.Tech CSE, YSREC of YV University, Proddatur, India
Email: sumachinni097@gmail.com
K. Haripriya
Student, III B.Tech CSE, YSREC of YV University, Proddatur, India
Email: haripriyakancherla7@gmail.com

ABSTRACT

Communication is the process of transmitting information from source to destination. The information exchanged between sender and receiver through the proper channel. The information should not be stolen by unauthorized parties like hackers while sending or receiving via channel. To avoid this stealing of the information cryptography techniques are used. The key is playing prominent role in cryptography. This paper proposes a novel method for key generation by using nearest primes. Further 2's complement and logical operations are used in encryption and decryption process. The final cipher text is generated by representing the intermediate cipher in matrix form and then read by column wise.

Keywords - **2's complement, Ciphertext, Cryptography, Nearest prime number, Plaintext, XOR operation.**

Date of Submission: May 08, 2016 Date of Acceptance: May 25, 2016

I. INTRODUCTION

Cryptography[1] is used to constrain the potential sender and/or receiver of a message. Cryptography is based on secret key. The sender can encode its message so that it can only decode with suitable key.

Cipher[1] is the algorithm that is used to transform plaintext into cipher text, this method is called encryption, in other words, it's a mechanism of converting readable and understandable data into "meaningless" data, and it is done as follows:

$$C = E_{(k)}(P) \qquad (1)$$

Where $E_{(k)}$ is the encryption algorithm using key k, C is a cipher text and P is a plain text. Symmetric and asymmetric are two types of encryption algorithms.

The opposite of cipher mechanism is called decipher that is the algorithm which recovers the plain text from cipher text, this is called decryption, in other words, it's a mechanism of converting "meaningless" data into readable data, and it is done as follows:

$$P = D_{(k^{-1})}(C) \qquad (2)$$

Where $D_{(k^{-1})}$is the decryption algorithm using key k.

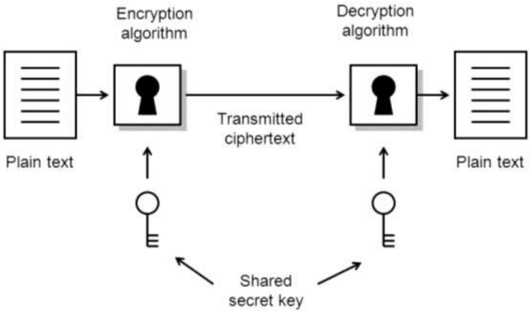

Fig 1. Conventional Encryption Model

Security services: Here are some of the services that are provided by the security[2].

- Confidentiality(privacy)
- Authentication(who created or sent the data)
- Data integrity(has not been altered)
- Non-repudiation(the order is final)
- Access control(prevent misuse of resources)
- Availability (permanence, non-erasure).

If we are protecting confidential information then cryptography is provide high level of privacy of individuals and group.

There are a number of cryptographic primitives-basic building blocks, such as block ciphers, stream ciphers and hash functions. Cryptography has being used for millennia to safeguard military and diplomatic communications. Data encryption standard adopted by the National institute of standards is the most commonly used symmetric encryption algorithm. Black-box transformations are some of the transformations that are hidden in the algorithm. The proposed work/algorithm follows symmetric cryptographic system.

II. HISTORY

The word cryptography[1] comes from the Greek Word 'Kryptos' and 'Graphein'. For the past 20 years, the most commonly used symmetric encryption algorithm in United States for civilian applications. In 2001, NTST adopted a new application algorithm called the advanced encryption standard (AES) to replace DES. AES is another symmetric block cipher which uses key lengths of 128,192 and 356 bits and works on 128 bit blocks. Generally, the algorithm is compact and efficient. There are several symmetric block encryption algorithms in use today. One is Twofish algorithm and the other is RC5.The Twofish algorithm is fast, compact and easy to implement. RC5 can vary in key length, number of transformations and block size. In 1970, one "Crypto group" was developed by IBM named as Horst-Festal. RC4 is the most common stream cipher which is designed to encrypt and decrypt a stream of bytes or bits rather than a block. RC4 as used in WEP (IEEE standard 802.11) has been found to be breakable in amount of computer time which itself has vulnerabilities.

III. EXISTING WORK

The existing method[3] generates a 64 bit random sequence for key generation. Key generation consists of two parts. One is raster scan method and the other is store and forward method. The existing method has various stages of encryption and decryption. In the first stage, caeser cipher[4] substitution method is used, which is computed by using the key, generated from raster scan method. In the second stage, using lookup table, the decimal equivalent of intermediate ciphertext is taken and then XOR operation is performed between intermediate cipher binary value and the key generated from store and forward method. In the third stage, column wise retrieval and nibble grouping is applied.

Limitations:

1. It is applicable only for 94 characters. It is not providing full support for ASCII characters.
2. Look up table is necessary.
3. Only column wise retrieval process is proposed.

IV. PROPOSED WORK

The proposed work generates a 8-bit random sequence for key generation. Key is obtained by performing subtraction between plain text values and its nearest prime values. Several stages are involved in encryption and decryption uses arithmetic and logical operations[5][6].

A. *Key Generation*

Each character of plain text converted into ASCII value. Further, find nearest prime of it. For key generation find the difference between nearest prime and plain text ASCII. Consider the difference value as key, it is continued for each character of plain text.

Key generation algorithm steps:-

Step1: Initially, the given plain text is converted into its equivalent ASCII values.

Step2: Find nearest prime values for ASCII values.

Step3: The key values are obtained from finding difference between ASCII and nearest prime values.

Step4: Perform 2's complement for generated value.

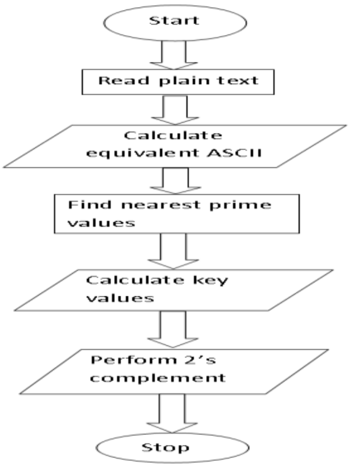

Fig 2. Flow chart showing key generation process

Example for key generation:

Plain text is: NETWORKSECURITY

ASCII values are: 78 69 84 87 79 82 75 83 69 67 85 82 73 84 89

Nearest primes values are: 79 71 89 89 83 83 79 89 71 71 89 83 79 89 97

Key values are: 1 2 5 2 4 1 4 6 2 4 4 1 6 5 8

Table 1. Key generation process

Key Value	Binary code	2's complement
1	00000001	11111111
2	00000010	11111110
5	00000101	11111011
2	00000010	11111110
4	00000100	11111100
1	00000001	11111111
4	00000100	11111100
6	00000110	11111010
2	00000010	11111110
4	00000100	11111100
4	00000100	11111100
1	00000001	11111111
6	00000110	11111010
5	00000101	11111011
8	00001000	11111000

B. Encryption algorithm

Round1: perform XOR operation between nearest prime and key.
Round2: reverse the result of round1.
Round3: store it in matrix form(column wise).
Round4: retrieve values from two rows of each n*4 matrix. Find equivalent ASCII and consider to be as final cipher text.

Round 1:

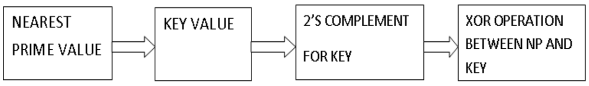

Fig 3. Steps involved in round 1

Round 2:

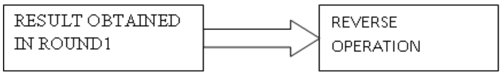

Fig 4. Steps involved in round 2

Round 3:

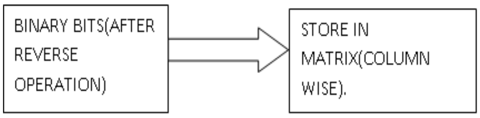
BINARY BITS(AFTER REVERSE OPERATION)
STORE IN MATRIX(COLUMN WISE).

Fig 5. Steps involved in round 3

Round 4:

ROW WISE RETRIEVING
EQUIVALENT ACSII
FIND CIPHER TEXT

Fig 6. Steps involved in round 4

Example:-

Table 2. Encryption process

Nearest Prime	Key	XOR	Reverse
01001111	11111111	10110000	00001101
01000111	11111110	10111001	10011101
01011001	11111011	10100010	01000101
01011001	11111110	10100111	11100101
01010011	11111100	10101111	11110101
01010011	11111111	10101100	00110101
01001111	11111100	10110011	11001101
01011001	11111010	10100011	11000101
01000111	11111110	10111001	10011101
01000111	11111100	10111011	11011101
01011001	11111100	10100101	10100101
01010011	11111111	10101100	00110101
01001111	11111010	10110101	10101101
01011001	11111111	10100010	01000101
01100001	11111000	10011001	10011001

Matrix form:-

Arranging the reverse values in row wise in the matrix.

Table 3.after placing reverse values row wise

0	0	0	0	1	1	0	1
1	0	0	1	1	1	0	1
0	1	0	0	0	1	0	1
1	1	1	0	0	1	0	1
1	1	1	1	0	1	0	1
0	0	1	1	0	1	0	1
1	1	0	0	1	1	0	1
1	1	0	0	0	1	0	1
1	0	0	1	1	1	0	1
1	1	0	1	1	1	0	1
1	0	1	0	0	1	0	1
0	0	1	1	0	1	0	1
1	0	1	0	1	1	0	1
0	1	0	0	0	1	0	1
1	0	0	1	1	0	0	1
0	0	0	0	0	0	0	0

Cipher text is:91 59 28 76 194 255 0 255 234 68 56 210 202 252 0 254

C. Decryption algorithm

Round 1: Rearrange the cipher text information in the form of matrix by finding their binary equivalents.
Round 2: Retrieve row wise binary values and reverse them.
Round 3: Reversed values are XOR with key to find nearest prime values.
Round 4: Find the original value by subtracting with key value from nearest prime value.

Round 1:

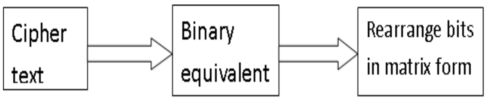

Fig 7. Steps involved in round 1

Round 2:

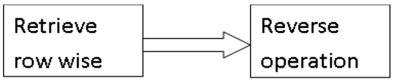

Fig 8. Steps involved in round 2

Round 3:

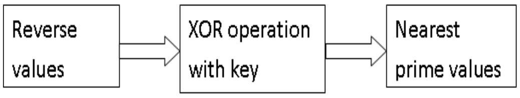

Fig 9. Steps involved in round 3

Round 4:

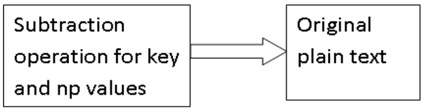

Fig 10. Steps involved in round 4

Example:-

Table 4. Cipher text to binary equivalents form

Cipher text	Binary
91	01011011
59	00111011
28	00011100
76	01001100
194	11000010
255	11111111
0	00000000
255	11111111
234	11101010
68	01000100
56	00111000
210	11010010
202	11001010
252	11111101
0	00000000
254	11111110

Matrix form:-

After rewriting the Table 4 binary value columns as rows

Table 5. After rewriting binary value columns as rows

0	0	0	0	1	1	0	1
1	0	0	1	1	1	0	**1**
0	1	0	0	0	1	0	1
1	1	1	0	0	1	0	1
1	1	1	1	0	1	0	1
0	0	1	1	0	1	0	1
1	1	0	0	1	1	0	1
1	1	0	0	0	1	0	1
1	0	0	1	1	1	0	1
1	1	0	1	1	1	0	1
1	0	1	0	0	1	0	1
0	0	1	1	0	1	0	1
1	0	1	0	1	1	0	1
0	1	0	0	0	1	0	1
1	0	0	1	1	0	0	1
0	0	0	0	0	0	0	0

Row wise retrieval:

After row wise retrieval of Table 5.

Table 6. Row wise retrieval process

00001101
10011101
01000101
11100101
11110101
00110101
11001101
11000101
10011101
11011101
10100101
00110101
10101101
01000101
10011001

Decryption:-

Table 7. Decryprtion process

Reverse	Key	Nearest prime
10110000	11111111	01001111
10111001	11111110	01000111
10100010	11111011	01011001
10100111	11111110	01011001
10101111	11111100	01010011
10101100	11111111	01010011
10110011	11111100	01001111
10100011	11111010	01011001
10111001	11111110	01000111
10111011	11111100	01000111
10100101	11111100	01011001
10101100	11111111	01010011
10110101	11111010	01001111
10100010	11111011	01011001
10011001	11111000	01100001

Nearest prime values:
79 71 89 89 83 83 79 89 71 71 89 83 79 89 97

Key values: 1 2 5 2 4 1 4 6 2 4 4 1 6 5 8

ASCII values(subtraction b/w key & np):
78 69 84 87 79 82 75 83 69 67 85 82 73 84 89

Plaintext(original message): NETWORKSECURITY

Advantages:-

- Nearest prime values technique is used for the key generation.
- Mixed column and row wise retrieval process is extended. Which is one of the flavor added in this paper.
- It is applicable for 256 characters.

V. CONCLUSION

A passive attack attempts to learn or make use of information from the system. Data confidentiality is a measure of ability of the system to protect its data from a kind of passive attacks. Data integrity refers to maintain accuracy and consistency of data. The proposed algorithm nearest primes cipher provides data confidentiality and integrity to the system. The cipher text is generated using a step by step encryption algorithm based on nearest primes and logical operations. The result of the above operations is stored in a matrix row wise and retrieves in column wise to obtain more security.

The future work can be extended to implementation of secure key exchange mechanism, reducing the time complexity in key generation using data structures, the size of data to be encrypted can be increased by increasing key length. Supplementing authentication security service to the nearest prime encryption algorithm.

REFERENCES

[1] William Stallings, "Cryptography and Network Security: Principles and Practices", 4th Edition, Prentice Hall, 2006, page numbers 30-39.

[2] Hans Delfs and Helmut Knebl, "Introduction to Cryptography: Principles and Applications", Springer, first edition, 2002, page numbers 11- 14.

[3] S. Kiran, R. Pradeep Kumar Reddy, “Multi-Stage encryption using Seeded SDES” International Journal of Advanced Networking and Applications Volume: 07 Issue: 02 Pages: 2694-2699 (2015) ISSN: 0975-0290.

[4] B.Bazith Mohammed, “automatic key generation of Caesar cipher”, international journal of engineering trends and technology (IJETT), vol.6,no.6,pp.337-339,dec.2013.

[5] S.G.Srikantaswamy and Dr.H.D.phaneendra,“A cipher design using the combined effect of arithmetic and logic operations with substitutions and transposition techniques“, International Journal of Computer Applications (0975-8887),vol.29,no.8,pp.34-36.

Author’s profile

Dr.S.Kiran is assistant Professor in the department of Computer Science and Engineering at Yogivemana University, Proddatur. He acquired M.Tech Degree from Nagarjuna University, Guntur. He completed Ph.D in computer Science in Computer Science from S. K. University. He has been continuously imparting his knowledge to several students in research activities. He published many articles National and International journals. His research areas are image processing, Cryptography and Network Security, Software Engineering and Data mining and Data ware house.

N.Subramanyan received his B.Tech degree in Computer Science and Engineering from Annamacharya Institute of Technology & Sciences ,Rajampeta. M.Tech. degree in Information Technology from RGM College of Engineering and Technology, Nandyal. Currently he is working as Academic Consultant in the Department of CSE at YSR Engineering College of Yogi Vemana University,Proddatur. He has got 6 years of teaching experience. He has attended 2 workshops.

Y. Suma is a student in the department of Computer Science and Engineering at Y.S.R Engineering college of Yogivemana University, Proddatur. She is studying 3rd B.Tech in CSE. She attended many workshops ,seminars and published papers in national and International journals.

K. Hari priya is a student in the department of Computer Science and Engineering at Y.S.R Engineering college of Yogivemana University, Proddatur. She is studying 3rd B.Tech in CSE. She attended many workshops,seminars and published papers in national and International journals.