Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 9 No. 1, March, 2018 - www.cisdijournal.org

Sieve Cipher: Development of Substitution Cipher by Modification of the Sieve-of-Eratosthenes

Valentine I. Anene, Afolayan A. Obiniyi & Barroon I. Ahmed
Department of Computer Science
Faculty of Physical Sciences
Ahmadu Bello University
Zaria, Nigeria.
Email: vallee.neutral@gmail.com, aaobiniyi@gmail.com, barroonia@yahoo.co.uk

ABSTRACT

Security of data over unsecured channel is a global issue. With the fast progression of digital data exchange in electronic way, Information Security is becoming much more important in data storage and transmission. Many Ciphers have been developed to provide data security over unsecured channel. Substitution cipher is a method of enciphering in which units of plaintext are replaced with ciphertext. This paper presents a substitution cipher, which modifies the sieve of Eratosthenes. The sieve of Eratosthenes is a simple, ancient mathematical approach for finding all prime numbers up to any given limit, by iteratively marking as composite the multiples of each prime. The proposed system generates shuffled cipher characters for transmission by getting the multiples of a key.

Keywords*:* Substitution Cipher, Encipher/Encrypt, Decipher/Decrypt, Plaintext, Ciphertext, Key.

CISDI Journal Reference Format
Valentine I. Anene, Afolayan A. Obiniyi & Barroon I. Ahmed (2018): Sieve Cipher: Development of Substitution Cipher by Modification of the Sieve-of-Eratosthenes. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 8 No 1. Pp 41-46. 4Available online at www.cisdijournal.org

1. INTRODUCTION

Security of information results from the need for private transmission of both military and diplomatic messages [1]. In the discussion of security of information, data security cannot be overlooked. Data over Internet may be stolen, intercepted, illegally modified or even destroyed by an adversary resulting in intellectual property rights infringement, data loss, data leakage and data damage [2]. Cryptography is the practice and study of hiding information. Cryptography is the science of using mathematics to encrypt and decrypt data [3]. Secured communication involves encryption process at the sending end and decryption process at the receiving end of the communication system [4]. Cryptography is a technique used to avoid unauthorized access of data [5]. Cryptography is divided into two main categories depending on the type of security keys used to encrypt/decrypt the plaintext. These two categories are: Asymmetric and Symmetric encryption techniques [5].

1.1 Symmetric Encryption

In symmetric key cryptography same secret key is used for encryption and decryption. The encryption algorithm produces the key and then sends it to receiver section where decryption takes place. It is much effective and faster than asymmetrical key cryptography [5].

1.2 Asymmetric Encryption

Asymmetric key cryptography is also known as public key cryptography. It uses two keys: public key and private key. Public key is known to the public and is used for encryption. Private key is known only to the user of that key and is used for decryption. The public and the private keys are correlated to each other by any mathematical means [5].

1.3 Terminologies Used in Cryptography

Terminology used in cryptography are:

- ❖ *Plain Text*: It is the original message or the actual confidential message which person wishes to send to other party.
- ❖ *Cipher Text*: It is the output of encryption algorithm. Cipher text message cannot be understood by anyone or intruder because of its non-readable format.
- ❖ *Encryption Algorithm*: It is the process of converting plaintext message into cipher text with a use of key.
- ❖ *Key*: This is also given as an input to encryption algorithm. It may be numeric or alpha numeric
- ❖ text or may be a special symbol.
- ❖ *Decryption Algorithm*: It is a reverse method of encryption algorithm. In this the original message is retrieved from the cipher text [6].

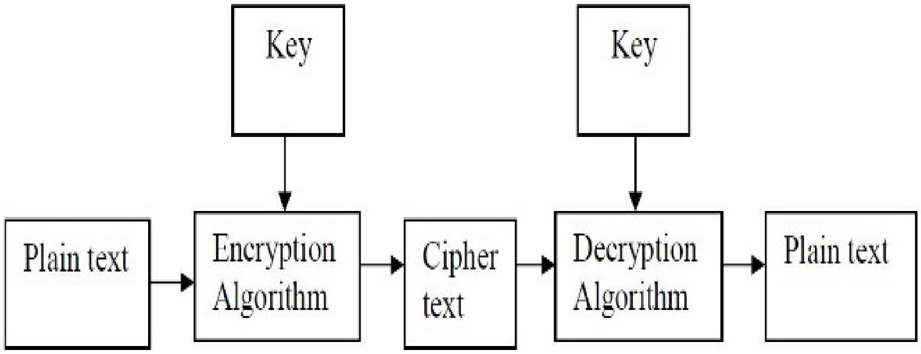

Fig 1: Encryption/Decryption process [3]

2. LITERATURE REVIEW

Information or data is the wealth of any organization therefore security issues are top priority to an organization dealing with confidential data [7]. An information system (IS) is more than just computer hardware; it comprises of software, hardware, data, people, procedures, and networks that make possible the use of information resources in the organization [8]. Information security is defined as the measures to safeguard attack on data (stored and transmitted data) [9]. Information security in an enterprise is a well-informed sense of assurance that the information risk and controls are in balance. In general, security is “the quality or state of being secure, to be free from danger” [8]. Recently with the rapid use of information in modern technology, information hiding methods received much attention from the research community in information security. This growth of information encourages researchers to develop security techniques and to keep data transmission between sender and receiver safer from attackers [10]. With increasing rate in the usage of computer as a means of secure communication, computer security cannot be overlooked. The different layers of security according to the type of content intended to be secured is summarized by: Physical security, Personal security, Operational security, Communication security, Network security [11].

Computer security is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (such as hardware, software, firmware, information/data, and telecommunications) [12]. Cryptography is a technique used to avoid unauthorized access of data [13]. Cryptography is the art of storing and transmitting data in a mangled form so that only authenticated users are able to read and process it [6]. Cryptography is the study of encryption principles and methods. The two basic building blocks of all encryption techniques are substitution technique and transposition technique [6]. Substitution technique is a method of encoding by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing the inverse substitution [7].

2.1 Substitution ciphers include Caesar cipher, Vigenere cipher, Playfair cipher.

Substitution ciphers include Caesar cipher, Vigenere cipher, Playfair cipher.

Caesar Cipher: One of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter of some fixed number of positions down the alphabet. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet [14].

Vigenere cipher: Vigenere cipher is a polyalphabetic substitution cipher which constitutes a matrix of 26 by 26 Caesar cipher shifts. It consists of a set of monoalphabetic substitution rules of Caesar ciphers with shifts of 0 through 25 [9].

Playfair Cipher: Playfair is classical cipher that has a square of matrix of 5 × 5 alphabetic letters arranged in an appropriate manner [15]. When a key is selected and place it in the matrix, the remaining letters of English alphabet are then one by one placed in the matrix of playfair cipher. The plain text is broken into pairs and if a pair has same alphabet then they are separated by introducing a filler letter like ‘x’, otherwise if the pair are different alphabetic letters and reside in the same row of matrix then each letter is replaced by the letter ahead of it.

3. RELATED WORKS

In this section, a review on works done in the area of substitution ciphers will be carried out.

Omolara *et al.,* [3] proposed a modified hybrid Caesar cipher and vigenere cipher for secure data communication. A lettered key and a numbered key were used for the encryption process. A Caesar cipher was performed on the lettered key using the shift of the numbered key. Vigenere cipher is then performed on the plaintext using the new key. The binary equivalent of the text generated is then exclusive-ored (XORed) with the binary of the numbered key to generate the final ciphertext.

Nishith and Kishore, [16] proposed improving security of vigenere cipher by double columnar transposition. This involves applying the vigenere cipher on a plaintext, before subsequently applying columnar transposition twice to further scramble the text.

Kester [17] proposed a hybrid cryptosystem based on vigenere cipher and columnar transposition cipher. He suggested the use of transposition cipher to scramble a plaintext, which is then used as the key for the vigenere cipher encryption process. This increased the security of the vigenere cipher.

Goyal *et al.,* [18] proposed a modified Caesar cipher algorithm which 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 complements the encryption key, so that reverse character substitution can be achieved.

4. SIEVE OF ERATHOSTHENES

Each natural number (i.e. each positive integer) '*n*' has the "trivial" divisors 1 and '*n*' itself. Therefore, each natural number different from 1 has at least two divisors. Natural numbers having exactly these two divisors are called *prime numbers*. According to this definition, the number 1 is not considered a prime number. There are good reasons for this; one of them is that otherwise the fundamental theorem of number theory on the prime factor decomposition of the integers would not be true, [19]. Prime numbers constitute one of the oldest and most interesting fields of research in mathematics. They are the building blocks from which all natural numbers are constructed by multiplication.

Eratosthenes was a Greek mathematician who is famous for his work on prime numbers and for measuring the diameter of the earth. The sieve of Eratosthenes is one the major accomplishments of Eratosthenes who was born in Cyrene, Greece, which is now known as Libya, in North Africa, in 276 B.**C.E.** The sieve of Eratosthenes is a simple, ancient algorithm for finding all prime numbers up to any given limit, and is still important today in number research theory. It does so by iteratively marking as composite (i.e., not prime) the multiples of each prime, starting with the multiples of two [20]. Eratosthenes figured out that if you were to write down all the natural numbers from 2 to infinity and "sieve out" every second number after two (or multiples of two), then move to the next available number (3) and continue to "sieve out" every multiple of 3 and so on, one would end up with a list of prime numbers.

4.1 Demonstration of the Sieve of Eratosthenes

The sieve of Eratosthenes procedure is demonstrated using an example 1 to n = 20.

1. List all natural numbers from 1 to 20:
   1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
2. Cross out the number 1 (it is not considered a prime number)
   ~~1~~ 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
3. 2 is selected; all proper multiples of 2 are Crossed out
   ~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~
4. In the remaining numbers, the first "free" number (i.e. the first number which has not been selected nor crossed out) chosen; in this case 3 is selected; all proper multiples of 3 are Crossed out
5. ~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~
6. 5, being the next free number is selected; all proper multiples of 5 are Crossed out
   ~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~
7. The procedure is continued accordingly until each of the numbers is either selected or crossed out.
8. ~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~
9. End of the procedure. The underscored numbers (i.e. 2, 3, 5, 7, 11, 13, 17, and 19) are the prime numbers within 1 to 20.

5. PROPOSED CIPHER

5.1 Modification of the Sieve of Eratosthenes

To encrypt a message using the proposed cipher, the proposed cipher requires plaintext and encryption key. The encryption key is an integer value and it determines alphabet index where generation of the ciphertext begins. The encryption key is based on modulo twenty-five (25) arithmetic to ensure that integer value wraps round, in case encryption key supplied is more than twenty-five. Decryption follows reverse operations performed during the process of encryption. It requires decryption key, and encrypted text. The decryption key will be same as the encryption key so that reverse character substitution can be achieved.
As stated earlier, the sieve of Eratosthenes is a simple, ancient algorithm for finding all prime numbers by iteratively marking as composite (i.e. not prime) the multiples of each prime, starting with the multiples of two. In this paper, a new cipher is proposed, which uses the sieve of Eratosthenes approach. Enciphering begins with the alphabet corresponding to index of the key and enciphering continues by marking multiples of the key and concatenating to previous cipher character till the first loop is done. All characters already used for enciphering process are marked and ignored during the second loop. Multiples of the key are continually marked during the second loop and concatenated to the cipher characters already generated. The process is continued until characters existing in a loop is less than the size of the key, then the key is reduced by one and the process is continued until key is reduced to zero.

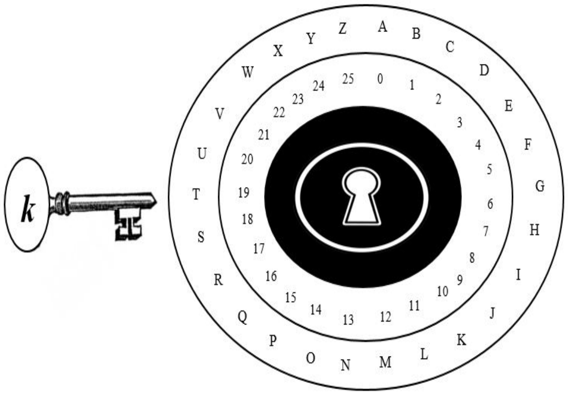

Fig 2: Proposed System

5.2 Illustration

For illustration purpose, an assumed key of three (3) will be used to illustrate how the proposed system generates ciphertext for encryption. First, the generation begins with the character mapped to the index of the key, and character mapped to the multiples of the key are used for the ciphertext generation during the first loop.

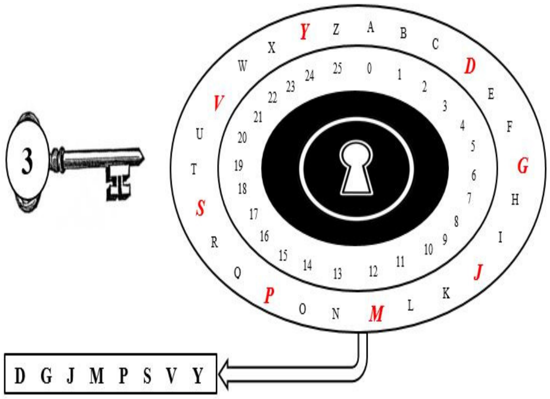

Fig 3: Ciphertext generated after first loop

The process continues into the second loop. Characters already used for enciphering process are ignored and character mapped to the multiples of the key are continually marked during the second loop and concatenated to the cipher characters already generated.

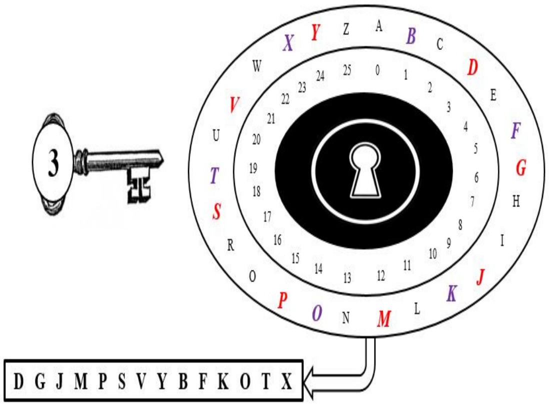
3
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
D G J M P S V Y B F K O T X

Fig 4: Ciphertext generated after second loop

The process continue loop wise in a clockwise manner until the amount of character left is less than the key, in this case three. The key is then reduced by one continuously after a character is marked until the value of the key becomes zero.

D G J M P S V Y B F K O T X C I Q W E N Z L A U

Fig 5: Ciphertext generated before amount of character left is less than the key

D G J M P S V Y B F K O T X C I Q W E N Z L A U R H

Fig 6: Ciphertext generated

6. EXPERIMENTAL RESULT

6.1 Encryption

Suppose we have a message "CRYPTOGRAPHY" to encrypt, using the key and ciphertext generated in the illustration of section 5, the mapping table below is used

Table 1: Mapping table

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	D	G	J	M	P	S	V	Y	B	F	K	O	T	X	C	I	Q	W	E	N	Z	L	A	U	R	H

Taking the ciphertext letter mapped to each the letter in "CRYPTOGRAPHY" we have "JWRINCVWDIYR". "JWRINCVWDIYR" becomes the encrypted message.

6.2 Decryption

Decrypting the encrypted message in section A, above, "JWRINCVWDIYR", we use the mapping table of table1. Taking the plaintext letter mapped to each the letter in "JWRINCVWDIYR" we have "CRYPTOGRAPHY" the original message.

7. CONCLUSION AND SCOPE OF FUTURE WORK

The use of Internet is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different techniques. Data Security is a very important aspect. To provide the security to the network and data, different encryption methods are used. This paper presents a substitution cipher developed by modifying sieve of Eratosthenes. This cipher generates ciphertext by taking the multiples of a key provided. Security provided in this paper can be further enhanced, if other ciphers are applied to the cipher in this paper, bringing about a hybrid or more than one algorithm is applied to data.

REFERENCES

[1] Seberry, J. and Pierprzyk, J. (1989). An Introduction to Computer Security. Prentice Hall Advances in Computer Science Series, pp 123 - 134.

[2] Ratnakirti, R., Anirban, S., & Suvamoy, C. (2013). Chaos based Edge Adaptive Image Steganography. ScienceDirect and International Conference on Computational Intelligence: Modeling Techniques and Applications, 138-146.

[3] Omolara, O. E., Oludare, A. I., & Abdullahi, S. E. (2014). Developing a modified Hybrid Caesar cipher and Vigenere cipher for secure Data Communication. IISTE, 34-46.

[4] Srikantaswamy S and Phaneendra H. (2012). Improved Caesar cipher with random number generation technique and multistage encryption. Published by International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.4, December 2012.

[5] Kakkar A, Singh M., Bansal P. (2012). Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network. International Journal of Engineering and Technology Volume 2 No. 1.

[6] Sharma R, Sharma R and Singh R (2012). Classical Encryption Techniques. published in International Journal of Computers & Technology. Volume 3. No. 1.

[7] Michael, W. E., & Herbert, M. J. (2011). Principles of Information Security, 4th Ed. Kennsaw University: Cengage Learning.

[8] Whitman, E. M., and Mattord, J.H. (2011). Principle of Information Security (4th ed.). Course Technology: Boston, pp 3-82.

[9] Stallings, W. (2011). Cryptography and Network Security: Principles and Practice (5th ed.). Prentice Hall: New York, pp. 25-54.

[10] Al-Shatanawi, O. M., & El-Emam, N. N. (2015). A New Image Steganography Algorithm Based on MLSB Method with Random Pixels Selection. International Journal of Network Security and Its Applications, 7(2), 37-53.

[11] A. Kakkar, M. L. Singh, P.K. Bansal. (2012). Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network. International Journal of Engineering and Technology Volume 2 No. 1.

[12] Deepesh, R. and Bhandari, V. (2013). A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image. International Journal of Computer Applications 64(20), 15 - 19.

[13] Kester Quist-Aphetsi. (2012). A Cryptosystem based on Vigenere cipher with varying key. International Journal of Advanced Research in Computer Engineering and Technology, 108-112.

[14] Sastry, Shankar, N., and Bhavani. S. D. (2009). A Modified Playfair Cipher Involving Interweaving and Iteration. International Journal of Computer Theory and Engineering, 1(5), 1793-8201.

[15] National Institute of Standards and Technology (1995) An Introduction to Computer Security: The Computer Security Handbook. publication, pp. 800 – 812, London.

[16] Nishith, S., and Kishore, B. (2014). Improving Security of Vigenere Cipher by Double Columnar Transposition. International Journal of Computer Applications, Vol 100 (No. 14). Pp 6-10.

[17] Kester Q-A. (2013). A hybrid cryptosystem based in Vigenere cipher and Columnar Transposition cipher. ISSN No: 2250-3536 Volume 3, Issue 1.

[18] Goyal K. and Kinger S. (2013). Modified Caesar Cipher for Better Security Enhancement. Published in International Journal of Computer Applications (0975 – 8887)(IJCA)" Volume 73– No.3.

[19] Jochen Ziegenbalg. The Sieve of Eratosthenes (Eratosthenes of Cyrene ca 276-194 BC)".
Retrieved from:
http://www.ziegenbalg.ph-Karlsruhe.de/materialien-homepage-jzbg/materials-in-English/sieve-of-Eratosthenes/The-Sieve-of-EratosthenesSimulation.htm.

[20] Horsley Samuel (1772). Κόσκινον Ερατοσθένους or, The Sieve of Eratosthenes. Being an account of his method of finding all the Prime Numbers. Vol. 62. pp. 327–347.