IMPACT: International Journal of Research in Engineering and Technology
ISSN (P): 2347–4599; ISSN (E): 2321–8843
Vol. 10, Issue 3, Mar 2022, 1–10

A NEW VARYING CIPHER FOR SYMMETRIC KEY CRYPTOSYSTEMS

U. Thirupalu[1], E. Spandhana[2] & Dr. E. Kesavulu Reddy[3]

[1]Research Scholar (PT), Department of Computer Science, S.V.U. College of CM & CS, Tirupati, A.P, India

[2]Business Analyst, ADECCO India Pvt Ltd Bangalore, India

[3]Assistant Professor, Department of Computer Science, S.V.U. College of CM&CS, Tirupati, A.P, India

Received: 21 Mar 2022 **Accepted:** 23 Mar 2022 **Published:** 24 Mar 2022

ABSTRACT

Data encryption is one of the widely used methodologies to ensure the data confidentiality in cloud environment. Most of the proposed methods which generate cryptographic algorithms are weak, and slow. Another important problem in the proposed methods is to replace bits which lead to improvement in the performance of cryptographic algorithms. Chosen-plaintext, chosen- cipher text attacks on symmetric-key encryption schemes giving adversary actions to predict the original message or the key. We proposed new Varying Cipher to reduced or increased the plain text before producing the cipher text. The same way the key size is increased or decreased according to the size of both plain text and varying text size. The block size is also increased or decreased the size of only varying text. In this paper we explain the proposed cryptosystem processing data as plaintext and produce the cipher text with duplicate text symbols. The expectation is the diagonal process enforce generation of highly complex, immunized, and resistant cipher text which is infeasible to break or cryptanalysis.

KEYWORDS: *Varying Cipher, Symmetric Key Cryptography, Oscillation, Key Generation*

INTRODUCTION

A model is a three-dimensional representation of a person or thing or a proposed structure. In cryptography, it is a method of protecting information and communications through the use of codes. So that only those for whom the information is intended can send or receive and process it. In earlier days, where the word cryptography was not entered into the words of dictionary. For example, the sender would like to send a message to a particular receiver, they may select any one of the media which are existing in the world. While sending unprotected areas or normal paths, there may be a chance to hack the information by the third party usually hackers.

Varying Cipher is a cipher which is newly designed by us. The primary motto of VC is to generate the variable length cipher. Varying Cipher is a new concept to generate the cipher test as variable length. This is the concept to increase or decrease the plain text. It uses six transformation functions.

RELATED WORK

Asymmetric key cryptography is almost 1000 times slower than Symmetric key cryptography, because they require more computational power. She mainly focuses on symmetric key cryptography [1] due to the assumption that symmetric cryptography has higher effectiveness and require less energy consumption, in contrast to asymmetric key cryptography.

The symmetric key [2] computational power is a small than the asymmetric key algorithms. Finally, they concluded the symmetric key algorithm consumes the least encryption time and memory usage than other existing symmetric key algorithms. The rapid growth of web-based services great amount of data has become more open and accessible.

In the encryption process, the 9's complement is performed on the equivalent Unicode value of given plaintext to produce final ciphertext. The result of 9's complement is XOR with the random public keys and followed by a shuffling process [3].They address various issues on combination cipher methods like substitution, stream cipher and vigenere cipher. To overcome the limitations, the authors proposed analgorithm by combining vigenere cipher with a stream cipher. It aimed to hide the relationship between the ciphertext and plaintext by handling the repetitive patterns in the plaintext [4].They proposed an algorithm which supports for user desired security level and processing level. The algorithm provides security levels and their corresponding processing levels by generating random keys for the encryption/decryption process by using fuzzy logic [5].

They proposed pseudorandom number generator based on the logistic pseudorandom image algorithm. In this method, authors use a dynamic block & white images with a grayscalesize of $2^k * 2^k$ pixels for key generation [6][7].They explains new symmetric key cryptographic method called Bit Level generalized modified vernam cipher method with feedback which is extension of standard vernam cipher. In this approach random key generator is used to construct a bit level modified vernam cipher [8].

A novel method for encryption is proposed by considering basic theory of one-time-pad (OTP) [9]. This approach is used to confirm the implementation of one-time security encryption scheme as simple and effective in user concern, where the method is more complicated in nature of attacker point of view. They implement number of encryption schemes using 1's complements, 2's complements and 9's complements with binary addition, subtraction with reversible approach with XOR properties. They propose a novel technique to produce a key which can substitute OTP which takes Gas (Genetic Algorithms) as base for generating the key [10].

They attempt to hides the statistical relationship betweenthe ciphertext and plaintext by using different keys in encryption process. Different keys are generates using a seed and XOR with the plaintext after a performing left shift by one position on each key and followed by 10's complement and modulo 127 arithmetic operations [11][12].He presented a new data encryption scheme named as Ordeal Random Data Encryption Scheme (ORDES) [13] which emphasis on secrecy of the key. The authors proposed to generate a secure cryptographic key by considering multiple biometric modalities of human being. Especially, it presents generation of secure cryptographic key based Iris and fingerprint [14].This work addressed the importance of passing statistical randomness tests for block ciphers. The authors introduced a cryptographic randomness testing method. A package of statistical and cryptographic randomness tests is mentioned bellow [15].

- Strict Avalanche Criterion Text.
- Liner Span Test.
- Collision Text.
- Coverage Text.

In this publication the authors considered the basic fact of OTP scheme with conjunction of 9's complement of decimal value which will be XOR with a random number key [16].

EXISTING SYSTEM

In cryptography the symmetric encryption schemes use a common shared secret key directly in cryptographic processes like encrypt or decrypt and authenticate the data. Here are a few recent research works and their inherited problems which helped to formulate the problem identifications.

Encryption algorithm converts the data into scrambled form by using the '**key'** and only the intended user has the key to decrypt the data. Security is the most challenging issue in the world, related to cyber security and to give more confidentiality to the users to enable high integrity and availability of the data. Encryption can be implemented by using some substitution technique, shifting technique, or mathematical operations at a great level. Cloud computing is one of the fastest growing internet-based technologies. Data encryption is one of the widely used methodologies to ensure the data confidentiality in cloud environment. Moreover, most of the proposed methods which generate cryptographic algorithms are weak, and slow. Another important problem in the proposed methods is to replace bits which lead to improvement in the performance of cryptographic algorithms.

In addition to these Diagonal Transposition, Bit Substitution, and Oscillation Fetching process on varying text with the key positions. For the first time, in this research work, we propose a construction method to generate variable length keys with maximum possible immunity to break.

We also aim a kind of symmetric key encryption system which provides confidentiality, authentication, especially for large sequences of data for communication or for data store. Here, our intention is to propose a cryptosystem for processing data as plaintext and produce the cipher text with duplicate text symbols. The expectation is the diagonal process enforce generation of highly complex, immunized, and resistant cipher text which is infeasible to break or cryptanalysis.

PROPOSED SYSTEM

In this research, we introduced a cryptosystem for ciphers that is '**Varying Cipher**' (VC). It is a kind of symmetric key encryption scheme. It aims to provide confidentiality, authentication to the data, especially for long sequences of communication with the use of a symmetric-key.

Here our new VC produce the cipher text as a variable length. Variable length means that the length of the cipher text is greater the plaintext or lesser the plaintext. It performs the operations at five level. Further chosen-plaintext, chosen-cipher text attacks on symmetric-key encryption schemes giving adversary actions to predict the original message or the key. **Varying Cipher (VC),** varying key, varying block etc. It is one of the challenging processes to design these things as a single task. The technique varying cipher is reduced or increased the plain text before producing the cipher text. In the same way the key size is increased or decreased according to the size of both plain text and varying text size. The block size is also increased or decreased the size of only varying text.

Here our new VC produce the cipher text as a variable length. Variable length means that the length of the cipher text is greater the plaintext or lesser the plaintext. It performs the operations at five level.

- Sorting Out the Plaintext (SOP)
- Drop Dupe Chars (DDC).
- Diagonal Transpositions (DT).
- Key Generation (KG).
- Bit Substitution (BS).
- Oscillation Fetching (OF).

Sorting Out the Plaintext (SOP)

Sorting is a process of arranging the plaintext elements into an order. Here we use one of the sorting techniques i.e. Selection sort.

Drop Dupe Chars (DDC)

Drop Dupe Chars method drops the duplicates characters in the plain text. Textual data may contain duplicate data that data is dropped. It counts the number for the character. Then add the number with the character to form a new string. The new string is act as intermediate string between actual plaintext and cipher text. So that, our Varying Cipher (VC) is the robust cipher than existing ciphers.

Diagonal Transpositions (DT)

Diagonal transposition is one of the transpositions techniques where we place the actual plaintext in to the suitable Block (matrix) which is designed by our own after taken the DDC plaintext length.

Key Generation (KG)

The proposed algorithm VC is a Symmetric Key algorithm. Proposed algorithm use two keys: primary key and ind Key. These two are made as single key as Main Key. The primary key performs all primary operation on DDCPT. The primary key is entered by the sender (Pal) as a kind oftext.

Bit Substitution (BS)

Bit Substitution manipulates the bits of the byte with the key values. It is the process of manipulation of a byte i.e. 1 is replaced with 0and 0 is replaced with 1 vice-versa. This operation is performed from right to left. If the key value is 1, it changes every nd – rd bit of byte like the above. If the key value is 2, it changes every 2 – bit of the byte. If the key value is it changes every 3 – bit of the byte vice-versa. If the key value is greater than 8 the bit manipulation is started at 1onwards by performing modulo operation of the given key value.

Oscillation Fetching (OF)

Oscillation is the repetitive variation, typically in time of some measure about a central value or between two or more different states. It is motion of an Object that regularly repents itself, back and forth, over the same path.

- If the key values are odd then the fetching process is: Aij
- If the key values are even then the fetching process is: Aji

RESEARCH METHODOLOGY

The generated cipher text should not give any clues to cryptanalysts to find out the machining of plain text. The cryptanalysts spend more time to break the cipher. This algorithm should generate large key size, so that is more confusion for the cryptanalysts. It occupies tiny storage space for the cipher text. Both cipher text and key size not at all matched to break the cipher at any movement.

Designed Parameters

The parameters which are considered for VC designs as follows,

- Symbolic Characters
- Simplify Plaintext
- Block Size
- Key Size
- Complexity
- Speed

IMPLEMENTATION OF VARYING CIPHER

The new cryptosystem for ciphers is '**Varying Cipher**' (VC). It is a kind of symmetric key encryption scheme. It aims to provide confidentiality, authentication to the data, especially for long sequences of communication with the use of asymmetric-key. Generally, most of the data contains general characters than the numbers. Besides, the general characters include repeated characters. The proposed cipher technique reduces the text by hiding the repeated characters with represented numbers and it became a tiny text and the produced cipher text is also tiny cipher.

The tiny cipher occupies less memory space in storage medium especially in cloud storage. It is the most useful technology for the cloud computing designers. Moreover, the rate of transmission of this tiny cipher is very high while transmitting the cipher between sender and receiver over the Internet. Whereas other existing symmetric key algorithm cipher text occupies more memory space and also transmitting rate is low. In key generation point-of-view, our VC generated key is very large than other existing algorithms.

Varying Cipher Algorithm: Encryption Algorithm Sender(A)

- Enter Plain text
- Send the Text to S.O.P Method
- The S.O.P method process step by step in the following
    - Order the elements of the plain text
    - Return the index of the Plain Text as Ind key

- Start DDC step by step in the given below
    - Count the duplicate characters
    - Drop the duplicate characters only and count number
    - Add the character (and number of Duplicates) to form the new DDCPT(Drop Dupe chars Plain text).
- Design the matrix which is suited to DDCPT.
- Process the Diagonal Transposition method (DT) for DDCPT
- Read the key related to size of the matrix (as Primary key)
- Merge the Primary key and Index key(Ind key) as a main key
- Send the main key to the Receiver
- Perform Bit Substitution in the following
    - Fetch each character related to key get the binary form of the character
    - Permutate the bit operation related to key
- Perform the Oscillation Fetching in the following
    - Get the characters related to key
    - Add Characters to cipher Text.
- Send Cipher text to Receiver

Varying Cipher Algorithm: Decryption Algorithm

- Receive the key from sender
- Split the key into parts
    - Primary key
    - Index key (Ind Key)
- Perform Decryption operation from Oscillation fetching in the following.
    - Create matrix related to Primary key (Key Size)
    - Fill the cipher character into matrix using key.
- Perform Decryption Bit Substitution operation in the following.
    - Fetch each character related to the key.
    - Get the binary form of the cipher characters
    - Permutate the bit operation related to key.

- Get the character in the reverse manner of DT to new Text.
- Repeat the following to perform Pick Dropped Chars (PDC) operation.
    - Fetch the character
    - If the character is not followed number, just add it to new string.
    - If the character is followed number fill the character(s) related to the number to the new string
- Perform Unsort (US) method using Ind key to get Plaintext.

JAVA PROGRAM TEST RESULTS

For implementing the proposed cipher, VC encryption/decryption process techniques with explanation along with sample outputs. We used JDK1.6.0 to design and develop the new cryptosystem for ciphers, under Windows 10 Pro operating system with Intel Core i3 processor 2.0GHz and 4.00GB RAM. The Block which is designed to perform Diagonal Transpositions, Bit Substitution, and Oscillation Fetching of DDC plain text. The key size is also designed by the DDC plain test (primary key). The Indexed key (Ind Key) is derived from Sorting Out the Plaintext (SOP) method.

Encryption

Encryption is one of the processes, which convert the message (plaintext) into scramble (cipher) text. The method BitSubs() of VC is used to convert the plaintext into ciphertext. It takes the message as input form the source node usually sender Pal, then process and produce the required output to the destination node usually receiver Milky as cipher text.

Figure 1

Figure 2

Figure 3

Figure 4

Decryption

Decryption is the process of converting the ciphertext into plaintext. It is similar to encryption, simply it is the reverse process of encryption. Here, the ciphertext is placed into the block (matrix) in a diagonal position and performs OscillationDes, bitSubs, getElements, pickDroppedChars, and unSort methods of VC to get plaintext by passing different key to the related algorithms.

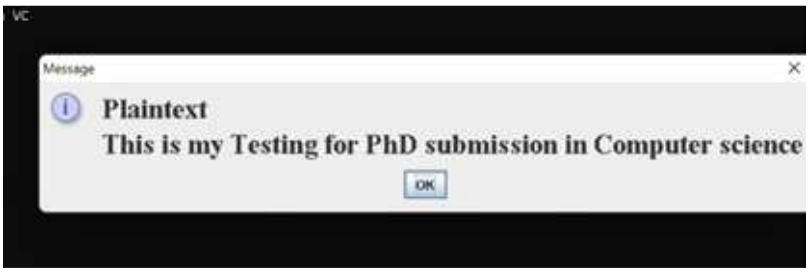

Figure 5

CONCLUSION AND FUTURE WORK

The varying cipher proved that reduced or increased the plain text before producing the cipher text. Also, the key size is increased or decreased according to the size of both plain text and varying text size. The block size is also increased or decreased the size of only varying text. The Varying Cipher is more secure than the symmetric ciphers also it is implemented in java programming and tested successfully.

Varying Cipher and applies to a data exchanging scenario especially for large mount data transformation. In further research work the algorithm will be experimented for secure, store, and retrieval of large data to and from could technology with the emphasis on keeping the security in the hand of client not in the hand of cloud service providers.

- Cloud storage.
- Key exchanging.
- Web applications & Client / Server communication applications.

REFERENCES

1. *Madhumita Panda, "Performance Analysis of Symmetric Cryptographic Algorithms", IJARSE, Vol. No.06, Special Issue No (01), Dec-2017.*
2. *OKOLIE, Samuel. O and ADETOBA, Bolaji. T, "Comparative Analysis of Performance Characteristic of well-known Symmetric Key Encryption Algorithms", IJSRNSC, Vol-4, Issue-3, June 2016*

3. *Abhas Tandon, Rahul Sharma, Sankalp Sodhiya and P. M. Durai Raj Vincent, "Universal Encryption Algorithm using Logical Operations and Bits Shuffling for Unicode" ,Indian Journal of Science and Technology , Vol. 8(15), pp.1-5, July 2015.*
4. *Fairouz Mushtaq Sher Ali and Falah Hassan Sarhan, "Enhancing Security of Vigenere Cipher by Stream Cipher", International Journal of Computer Applications, Volume 100 – No.1, August 2014.*
5. *Gamil R. S. Qaid and Sanjay N. Talbar, "Encrypting Image By Using Fuzzy Logic Algorithm", International Journalof Image Processing and Vision Sciences, vol. 2, no. 1, 2013.*
6. *Sodeif Ahadpour, Yaser Sadra, and Zahra Arasteh Fard, "A novel chaotic Encryption scheme based on Pseudorandombit padding", International Journal of Computer Science Issues, vol. 9, no. 1, January 2012.*
7. *Sodeif Ahadpour, Yaser Sadra and Zahra Arasteh Fard, "A novel chaotic image Encryption using generalized threshold function", International Journal of Computer Applications, vol. 42, no. 18, pp. 25–31, March 2012.*
8. *Prabal Banerjee and Asoke Nath, "Bit Level Generalized Modified Vernam Cipher Method with Feedback", International Journal of Advanced Computer Research, Vol.2 No.4 Issue-6, December 2012.*
9. *Sharad Patil, Ashok Patil, and Ajay Kumar, "Implemented Encryption Scheme Using Even(10's And 2's) Complement With Binary Addition Approach", International Journal of Information Technology and Knowledge Management, vol. 5, no. 1, pp. 65–67, 2012.*
10. *Farhat Ullah Khan and Surbhi Bhatia, "A novel approach to genetic algorithm-based Cryptography", International Journal of Research in Computer Science, vol. 2, no. 3, pp. 7–10, 2012.*
11. *S. G. Srikantaswamy and Dr. H. D. Phaneendra, "Enhanced One Time Pad Cipher with More Arithmetic and Logical Operations with Flexible Key Generation Algorithm"' International Journal of Network Security & Its Applications, vol. 3, no. 6, pp.243–248, November 2011.*
12. *S. G. Srikantaswamy and Prof. 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, vol. 29, pp. 34-36, 2011.*
13. *RAMVEER SINGH and DEO BRAT OJHA, "An Ordeal Random Data Encryption Scheme (ORDES)", International Journal of Engineering Science and Technology, vol. 10, pp. 6349–6360, 2010.*
14. *A. Jagadeesan and Dr. K. Duraiswamy, "Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris", International Journal of Computer Science and Information Security, vol. 7,no.2, February 2010.*
15. *Ali Doganaksoy, Barıs¸ Ege, Onur Kocak and Fatih Sulak, "Cryptographic Randomness Testing of Block Ciphers and Hash Functions", International Association for Cryptologic Research, 2010.*
16. *Srinivasan Nagaraj , Kishore Bhamidipati and M Ramachandra, "Formal Method of Encryption Using 9'S Complement", International Journal of Computer Applications, vol 8, no.5, pp. 23-25, October 2010.*