

Rectangular Generalized Vigenere Cipher

YumnamKirani Singh

C-DAC Silchar, Ground Floor, IIPC Building, NIT Silchar Campus, India

Abstract

Proposed here is a new form of symmetric key cipher entitled Rectangular Generalized Vigenere Cipher in which the encryption and decryption tables are not necessarily square but rectangular matrices. The main advantage of using rectangular cipher is the reduction of memory requirement for storing the encryption and decryption tables. At the same time, it does not compromise the security of the cipher much although the search space is reduced as the key search space in generalized Vigenere cipher is infinitely large. The encryption and decryption process are as faster than the generalized Vigenere cipher. Such a cipher can be conveniently used as lightweight cipher for memory and power constrained IoT devices.

Keywords: Vigenere Cipher, Generalized Vigenere Cipher, Rectangular Generalized Vigenere Cipher, Meitei Lock Sequence, Symmetric Key Encryption, Lightweight Cryptography.

Date of Submission: 13-09-2021

Date of acceptance: 28-09-2021

I. INTRODUCTION

Vigenere Cipher is symmetric key a poly-alphabetic cypher. It was considered as secure cipher until it was cryptanalyzed by Kaisiki Test. There are three main drawbacks in the Vigenere cipher. The first drawback is the use encryption table formed by regular shifting of 26 letters of Roman alphabet. The second drawback is the use of keystream formed by repetition of a chosen password. The third drawback is that decryption is not based on table by searching and matching and hence takes much longer time as compared to decryption [2, 3, 11]. All these drawbacks have been taken care of in Generalized Vigenere Cipher (GVC) [7]. In generalized Vigenere cipher, encryption table is formed from rows or columns of unique random numbers of certain range. As a result, the encrypted text i.e., cipher text becomes random in nature. Moreover, it uses a key stream which is a random like sequence known as Meitei Lock Sequence (MLS) generated from a chosen password array[5,6]. The MLS keystream can also be generated using any of the standard hash functions. This is because standard hash functions has a desirable property that can be used to generate a secure keystream. In a hash function, when there is a slight change in the input there is untraceable change in the output, which has been utilized in generating a MLS key stream [8]. The use of random-like sequence as keystream in generalized Vigenere cipher makes it more secure. The decryption process is also made much faster in GVC by using decryption table instead of searching and matching method in the Vigenere Cipher. In other words, the GVC is much faster and more secure than the original cipher proposed by Vigenere. Moreover, the encryption and decryption tables can be of any size for use in encryption of any data types such as text, image, or sound data. The generalized Vigenere cipher has been successfully used in the encryption of image and sound data in [8,9].

The original Vigenere Cipher or the generalized Vigenere Cipher use a square cipher table. In the original Vigenere Cipher, the cipher table also known as Vigenere Square is a table of 26x26 formed by shifting the 26 capital letters of the Roman alphabet. In the generalized Vigenere cipher, the cipher table is a random square table of 26x26 or 256x256 or 512x512 depending on range of input data to be encrypted. In these cipher, it is assumed that key stream also has the same range as the input data. It is found that the key stream range need not be the same as the input data range in Vigenere or generalized Vigenere cipher. If these two ranges are different, then we need to use rectangular cipher tables i.e., encryption and decryption tables. In this paper, we propose the use of rectangular cipher tables for developing a fast and secure encryption scheme. The main advantage of using rectangular cipher table is that we can save significant amount of memory in storing the cipher tables. For example, instead of using 256x256 cipher table for encrypting an image which requires 64 Kilobytes, if we can perform image encryption using 256x8 cipher table which requires only 2 Kilobytes, it will save significant amount of memory. Moreover, it will be faster during the encryption and decryption process. A secure cipher with low memory requirement is desired feature in lightweight cryptography for use IoT devices [1, 4,10]. The memory requirement can be significantly reduced further if we use rectangular cipher tables which can be generated by left or right shifting operations.

We have successfully tested the use of rectangular generalized VigenereCipher for different sizes of tables for encryption of text and image data. It is found that cipher table of 256x8 is sufficient for secure

encryption of uncorrelated data like text, sensor data. For highly correlated data like images, the cipher table must be at least 256x32 for secure encryption.

II. RECTANGULAR GENERALIZED VIGENERE CIPHER

Vigenere Cipher uses a cipher table, which is basically a square matrix generated by left circular shift of the first row. Such a cipher table has the same elements in all diagonal lines. This can be considered as weak feature for a secure cipher. In generalized Vigenere, the elements in the square cipher table are random in nature in the sense that no row or column in the table can be derived from any row or column by any means. Such a random cipher table cannot be generated twice and makes the generalized Vigenere cipher a very secure cipher. The size of cipher table is determined by two factors. The first factor is the range of the input data values to be encrypted and the second factor is the range of values in the key stream. In the Vigenere cipher, the input data range and the key stream range are considered to have the same range. This is the reason, why cipher table in these ciphers are square. In this section, we show that the key stream range need not be the same as the input data range. In other words, we can use rectangular cipher tables to perform encryption and decryption operations.

Let $R = \{r_1, r_2, r_3, \dots, r_m\}$ be the m different random positive integers and $K = \{k_1, k_2, k_3, \dots, k_n\}$ be n different random positive integers, then the table E of size $m \times n$ formed by random permutation of R in n different ways is a generalized rectangular Vigenere cipher. That, is E is rectangular encryption table which can be used in encrypt plain text message M formed by combinations of m different symbols or characters using key stream K formed by n different symbols. For simplicity, let us consider the following random matrix E of size 4×8 . The matrix consists of 8 different numbers in random positions. It may be noted that each row is unique. So, the message having 8 different numbers or symbols can be encrypted using this table. The key stream that can be used for this encryption table will have for different values corresponding to the number of rows.

Table-1: Encryption table E

3	1	7	2	8	4	5	6
5	8	3	1	6	7	4	2
6	3	4	7	5	1	8	2
1	5	8	4	3	2	6	7

Once an encryption table is formed, the decryption table of the corresponding size must be created. We can easily obtain the decryption table D having the same size as E as $D(i, E(i, j)) = j$, for all $i = 1$ to 4 and $j = 1$ to 8.

Following is the decryption table D for the encryption table E .

Table-2: Decryption Table D

2	4	1	6	7	8	3	5
4	8	3	7	1	5	6	2
6	8	2	3	5	1	4	7
1	6	5	4	2	7	8	3

After obtaining the encryption and decryption tables, we can perform the encryption and decryption operations. If M is a message string, and K is the key string having the same length as M . Then the encrypted text, i.e., cipher text C is given by

$$C = E(K, M)$$

The original message M can be obtained by decrypting C using D as

$$M = D(K, C)$$

It may be noted that key stream is taken as the first input index because the row index corresponds values of elements of key stream. If the encryption table has unique columns corresponding to the message input range, then the key stream would be the second parameter during the encryption and decryption process.

To understand the encryption and decryption process, let us consider a numerical array of 8 different values as message string, and another random array of four different values as key stream and then perform the encryption and decryption operation.

$$\text{Message } M = \{4, 6, 2, 1, 4, 8, 3, 7, 4, 5, 2\}$$

$$\text{Key string } K = \{3, 1, 4, 2, 2, 3, 4, 2, 1, 3, 2\}$$

Then, cipher text $C = E(K, M)$ is obtained as

i.e., $C=\{7, 4, 5, 5, 1, 2, 8, 4, 2, 5, 8\}$

The elements in the cipher text are obtained from the elements of the encryption table E of size 4x8. The first element of C is the element of E in the 3rd row and the 4th column, the second element of C is the element of E in the 1st row and the 6th column. Similarly, other elements of C are obtained from the encryption table E using the elements of K as the row indices and corresponding elements of M as column indices. If we compare the message M and cipher text C, we see that the cipher text is totally different from the plan text.

The original message M can be retrieved from C using decryption table D and K as

$$M=D(K,C)$$

$$M=\{4, 6, 2, 1, 4, 8, 3, 7, 4, 5, 2\}$$

The first element M is the element of D in the 3rd row and 7th column of D, the second element is the element of D in the 1st row and the 4th column and so on. We see that we can exactly get the original message back from the cipher text. In other words, we can perform encryption and decryption operation using the rectangular cipher tables (E and D) in the same way as we do in Vigenere or generalized Vigenere Cipher.

2.1 Generation of Random Encryption and Decryption Tables

Random Encryption tables are the tables generated randomly at sequence of key strokes or manually. These random tables are unique either column-wise or row-wise for it to be used as an encryption table. Uniqueness either in columns or rows ensures generation of decryption table. The size of the encryption or decryption table depends on the ranges of the values in the input data to be encrypted and the range of the key streams to be used for encryption. In the original Vigenere Cipher or the generalized Vigenere cipher, the range of the key stream is assumed to be equal to the range of the input data. As a result, the cipher table is always square. If the ranges of input data and the range of key streams are different the encryption and decryption tables would rectangular in shape. The range of input data can be considered fixed. However, the range of key streams can be varied so that smaller rectangular encryption tables can be used for encrypting the input data.

2.2 Generation of MLS Key Streams

MLS (Meitei Lock Sequence) is a random like sequence generated from an arbitrarily chosen non-negative array of any length. It can also be generated from any of the standard Hash functions such as SHA, SHA256, MD5 etc. The algorithm for generating MLS sequence from any of these standard hash functions is given in [8,9]. The useful or desirable property of MLS key stream is that the generated key streams are significantly different when there is any slight difference in any part of the input array or password from which the key streams will be generated.

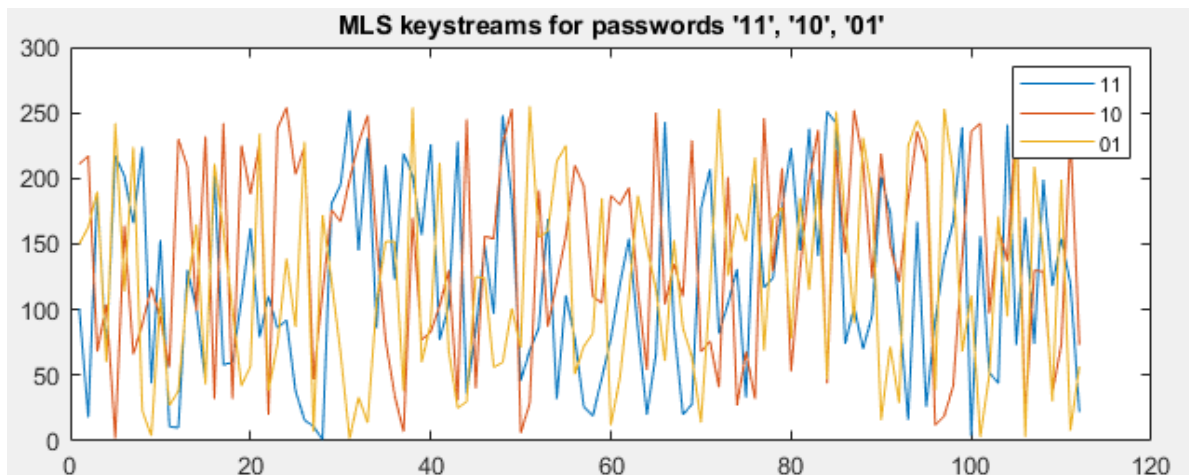


Figure-1: MLS Key streams generated using MD5 from the passwords '11', '10', and '01'.

The input for generating MLS key stream can be as long as we like but the minimum length should be 2. The output of the MLS key stream can be fixed to a particular length or as long as we desire. Because these properties, MLS key streams can be used for generating message digests like any other hash function for message authentication.




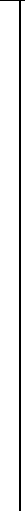




By default, the range of a MLS key stream generated from any standard hash function is 1 to 256. However, for use it in any encryption or decryption based on rectangular cipher tables, the range of the key streams should be changed to specific range as required by the rectangular tables.

III. EXPERIMENTAL RESULTS

To test the tightness of security of the proposed rectangular Vigenere cipher, we use rectangular encryption and decryption tables of size 256x8, 256x16, 256x32, 256x64 and used them for the encryption text and image data. The number of rows in these tables corresponds to the possible range of values in the data to be encrypted. The ASCII value of the text data is much below the range of 256, for 8-bit image data, the range of 256 is sufficient. So, a rectangular encryption table having 256 rows is sufficient for use in the encryption of both text and image data. The number of columns in these tables corresponds to the range of the values in the keystreams. For example, for using the encryption table of 256x8 for encryption of text or image data, the elements in the keystream must have a value 1 to 8. Similarly, for using the encryption or decryption table size 256x64, the elements of the keystream must be in the range 1 to 64. The smaller the encryption table, less memory is required to store it. However, performance is poor as compared to larger size encryption table especially for highly correlated data like images.

Table-3 shows the rectangular encryption and decryption tables (matrices) used in conducting the experiments on text and image data. These rectangular tables are shown as gray images in the Table-1. The E means the encryption table and DEC means the decryption table.

Table-3: Rectangular Encryption and Decryption tables of different sizes

Size: 256x8		Size: 256x16		Size: 256x32		Size: 256x64	
E8	D8	E16	D16	E32	D32	E64	D64
							

For encryption purpose, we use key streams of generated from the password ‘1111’ for different ranges, namely 1 to 8, 1 to 16, 1 to 32 and 1 to 64. If we use the same key streams for decryption, the cipher text or data will be decrypted without any error. To test the how much error is introduced during the decryption, we use key streams generated from slightly different password ‘1110’. The key streams used for encryption is shown in Figure-2. In the plot, only the first 500 values of the key streams are plotted. The blue plot corresponds to key stream having range 1-to 8, the red plot corresponds to the key stream having range 1 to 16, the yellow plot corresponds to the key stream having 1 to 32 values and the violet plot corresponds to the key stream having range 1 to 64. It may be seen that even though the key streams are generated from the same password ‘1111’, the key streams are different. Similarly, the MLS key streams of different values generated from the password ‘1110’ is shown in Figure-3. It may be noted that the MLS key streams in both figures are generated using MD5 hash function.

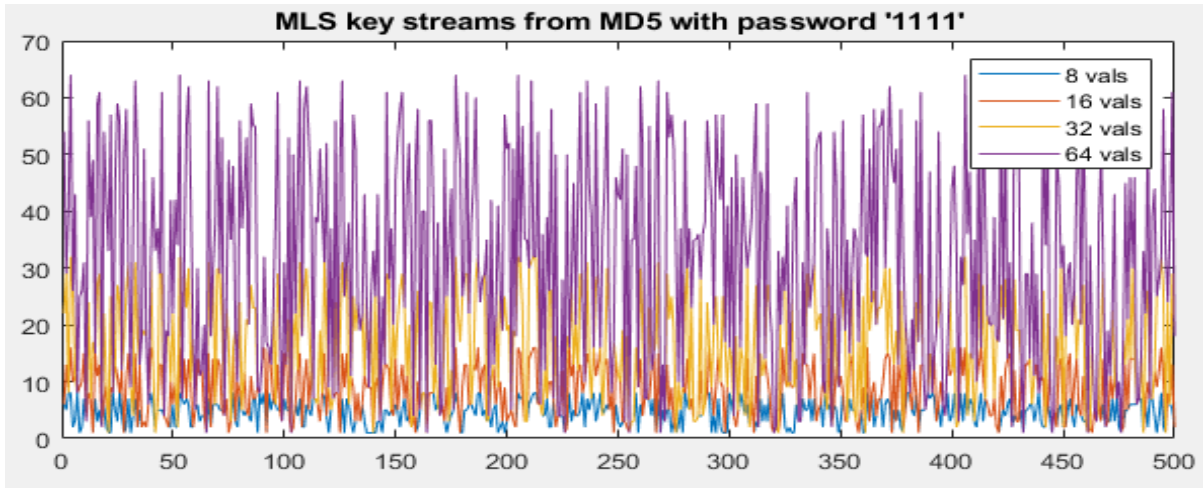


Figure-2: MLS key streams of different ranges generated from the password '1111'

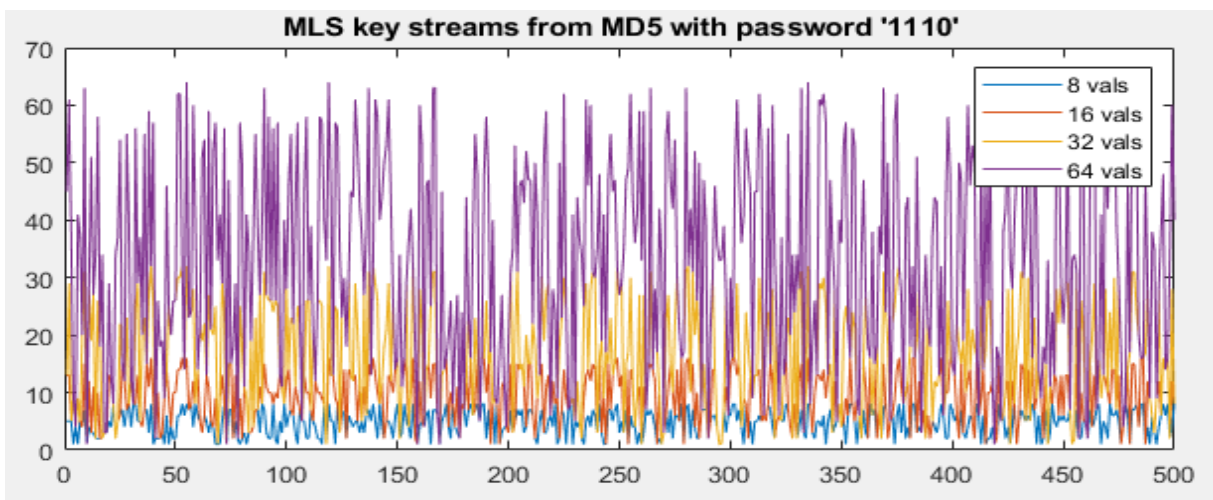


Figure-3: MLS key streams generated from the password '1110'.

3.1 Text Encryption Results

For encryption of text, we consider the string “The quick brown fox jumps over the lazy dog” as plain text. The plain text is encrypted with the rectangular encryption tables given in Table-3 with the corresponding key streams of appropriate ranges given Figure-2. The encrypted texts are then decrypted with key streams of appropriate ranges from the corresponding rectangular decryption tables. The encrypted text and decrypted texts are given Table-4.

Table-4: Encryption and decryption of plain text with key streams of different ranges

Plain text	'The quick brown fox jumps over a lazy dog'	Key Stream Range
Encrypted Text	'G÷Ö^!Î·A>”!ÿzøE*IVç°ÿÖÊuk^¼÷=¬^Ð”ç0°5°*5, '	8
Decrypted Text	'2hø Kmî JùK:© í&%\$ ÷'x pápo7& · -¼Ém'	
Encrypted Text	'G Ö y ·\EY!ÿzøc _Vç×ÿÖÊP¼^Q÷ÖøØBYç\°5°* !'	16
Decrypted Text	'#høñ ¼i{tÄ·:· /h \$ CjÄ W{Eo7x C·< { i”¼Ä'	
Encrypted Text	'æ¯ÖGÖ ·#Ec!Öz ca.V ×ÿ ÊP”Q f øÐca\°cÄ**!'	32
Decrypted Text	'\$høbq*îVW - Û~È1 \$ÄÖj W° o ý%C î”°nøø9Ä'	
Cipher text	'&¯ïöÖ ·#Ec!hi°cüBV eÊuÊ qwQ ø >î\° Ä** '	64
Decrypted text	'°î° qîCV -Kô -8b\$?xÈ/zøümoP«%Cu\$×*PD o '	


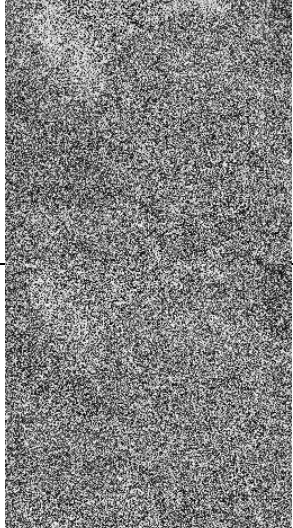
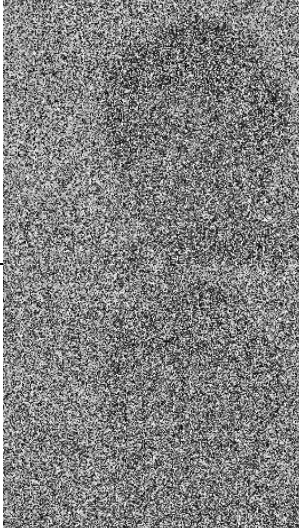
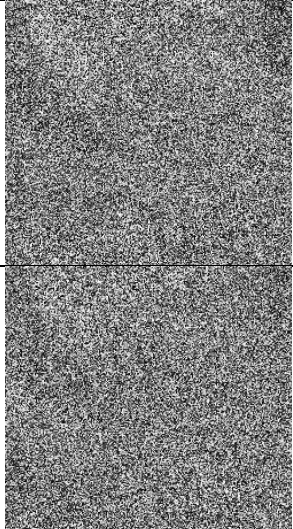
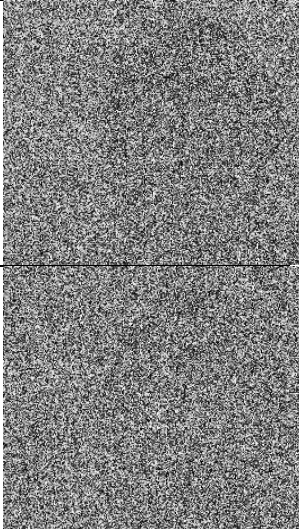
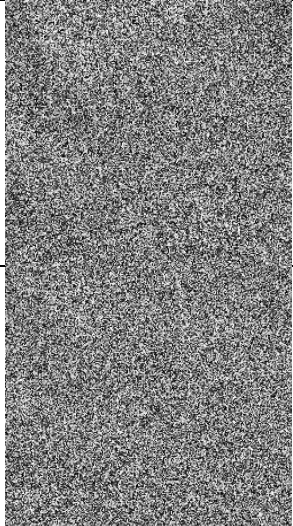
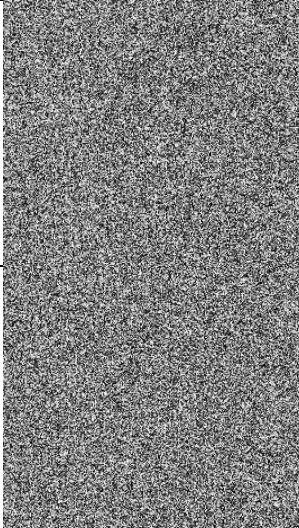
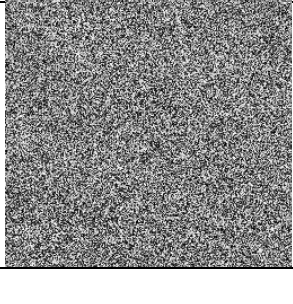
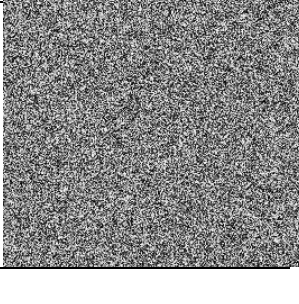
From Table-4, it can be seen that the decrypted text contains no useful information that can trace any word in the original plain text regardless of the ranges of key streams. It means that the rectangular cipher table

of size 256x8 is as effective as other larger tables. No trace of information can be found from either of the cipher text or decrypted text with wrong password. This is because text data is uncorrelated. So, for uncorrelated data smaller rectangular table is sufficiently secure.

3.2 Image Encryption Results

To test the strength of encryption schemes based on rectangular Vigenere cipher tables given in Table-3, we use the image 38-12.jpg of FEI database. The image is converted into gray and the perform encryption using rectangular cipher tables and corresponding key streams of appropriate ranges generated from password ‘1111’. The encrypted images are then decrypted using corresponding rectangular decryption tables and key streams of appropriate ranges generated from the password ‘1110’. The encrypted images and the decrypted images are given in Table-5.

Table-5: Encryption and Decryption of image using key streams of different ranges

				
Key Stream Range	‘1111’	Encrypted Images with	‘1110’	Decrypted Images with
8				
16				
32				
64				

From the images in the table it could be seen that the encrypted images do not reveal any information of the any part of the image irrespective of the ranges of key stream values. However, when the decryption key is generated from a password which close to the original password, the decrypted image begins to show some discernable patterns in the decrypted image for low range key stream as shown decrypted image with 8 and 16 key values. Such discernable patterns disappear for higher range key streams. From this, it may be concluded that for encrypting highly correlated data like images, the MLS keystream range should be at least 1 -32. In other words, the rectangular encryption table for encrypting images should be at least 256x32.

IV. CONCLUSION

A new encryption secure scheme based on rectangular cipher table has been proposed. The use of rectangular cipher tables can reduce the requirement of memory space in developing cryptographic applications. Saving memory space is important for low constraint IoT devices. It has been found that smaller cipher tables can be securely used for encryption of uncorrelated data. For highly correlated data, the random cipher table must be at least 256x32 for developing a secure cryptographic application.

REFERENCES

- [1]. Muhammad Usman et al, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things", International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017
- [2]. David Salomon. 2003. Data Privacy and Security. Springer.
- [3]. Bruce Schneier. 2001. Applied Cryptography. John Wiley and Sons.
- [4]. Daniel A. F. Saraiva, et al., "PRISEC: Comparison of Symmetric Key Algorithms for IoT Devices", Sensors, pp 1-23, October 2019, doi:10.3390/s19194312
- [5]. Y. K. Singh, S.K. Parui, "Simplet and Its application in Signal Encryption", Multidimensional Systems and Signal Processing, Vol. 15, No. 4, pp. 375-394, October 2004.
- [6]. Y. K. Singh, A Simple, fast and secure Cipher, ARPN Journal of Engineering and Applied Sciences, Vol. 6, No. 10, pp. 61-69, Oct. 2011.
- [7]. Y. K. Singh, "Generalization of Vigenere Cipher", ARPN Journal of Engineering and Applied Sciences, Vol 7, No. 1, pp. 39-44. January, 2012.
- [8]. Y. K. Singh, "Image Encryption Using Meitei Lock Sequence Generated from Hash Functions", Submitted to ADBU Journal of Engineering and Technology.
- [9]. Y. K. Singh, "Speech Encryption Using Meitei Lock Sequence Generated from Hash Functions", International Journal of Research in Engineering and Science, Vol. 6, No. 9, pp. 01-09, 2021.
- [10]. Y.K.Singh "A Lightweight Exchangeable Encryption Scheme for IoT Devices Based on Vigenere Cipher and MLS Keystream", In: Singh P.K., Noor A., Kolekar M.H., Tanwar S., Bhatnagar R.K., Khanna S. (eds) Evolving Technologies for Computing, Communication and Smart World. Lecture Notes in Electrical Engineering, vol 694, 2021 Springer, Singapore. https://doi.org/10.1007/978-981-15-7804-5_13
- [11]. Douglas R. Stinson. 1995. Cryptography, Theory and Practice. CRC Press.