A New Encryption Scheme Involving Spiral Rotation Technique Alongwith Aryabhata's Substitution Code

Niharika Belwanshi[1], S S Shrivastava[2]
[1]Research Scholar, Department of Mathematics, Institution for Excellence in Higher Education, Bhopal, (M.P.), India
[2]Professor, Department of Mathematics, Institution for Excellence in Higher Education, Bhopal, (M.P.), India
Corresponding Author: niharikabelwanshi85@gmail.com

***Abstract*: The aim of this paper is to propose a new encryption scheme involving Spiral Rotation Technique and Aryabhata's Substitution Code. The 'Spiral Rotation Technique' is applied on a matrix representation of data, and 'Aryabhata's Substitution Code' is a plotting of numbers to words. The 'Byte Rotation Technique' is applied on different blocks of plaintext. In a single processor system, multithreading helps run multiple tasks at the same time. Thus, this type of encryption method produced a new encryption model and creates a double security system which is very fast and secure.**

***Keywords*: Spiral Rotation, Aryabhata Substitution, Encryption and Decryption, Byte Rotation Technique.**

1. Introduction

The science of making message in secret code is known as cryptography [2, 3, 12]. Cryptography is the art and science of securing communication by converting information into an unreadable format to protect it from unauthorized access. There are two types of cryptographic process known as Encryption and Decryption. Encryption is the process of converting plain text (readable data) into cipher text (encoded data). Decryption is the process of converting ciphertext back into plaintext. In encryption and decryption process a mathematical function is used called cipher. There are two primary types of cryptography known as Symmetric and Asymmetric. In symmetric cryptography the same key is used for both encryption and decryption and symmetric key cryptography is also known as classical cryptography. In asymmetric cryptography, two different keys are used- a public key for encryption and a private key for decryption. Cipher or key to the algorithm is shared in Symmetric key encryption.

A. Spiral Rotation Technique[6, 11]

Spiral Rotation Technique is an Encryption method that involves organizing data into a matrix and then rotating it in a spiral pattern. This method sometimes known as a "Spiral Rotation Encryption Algorithm". This technique is applied to data arranged in a matrix format before encryption and decryption. This makes the data harder to recognize and adds an extra layer of security before encryption. It helps protect information by making it more difficult for hacker to find patterns or guess the original data.

B. Aryabhata Substitution Code[4]

Aryabhata Substitution Code, also known as the Aryabhata cipher is a method of representing numbers using a Sanskrit alphabet. Aryabhata Substitution Code is a plotting of numbers to words that divided into two groups of consonants and vowel. First 25 consonants are called Varga letters (k to m) and other 8 consonants are called Avarga (y to n). The varga letters represents square such as 1, 100, 10000, and the avarga letters represents non-squares such as 10, 1000.

C. Byte Rotation Technique[1, 5, 7, 8, 9, 10]

Byte Rotation is a technique whose bits or bytes of data are cyclically shifted horizontal or vetical. This technique is a Symmetric key Block Cipher technique. There are two types left rotation and right rotation.

This technique is applied on different blocks of plaintext and used in cryptography to enhances security by shifted bits or bytes. In this technique each block size is of 16 bytes. In this technique, firstly we break the plain text into blocks of 16 bytes each. Here each block is represented in the form of 2D array. After then to encrypt the text, we apply the byte rotation on rows and columns.

2. Related Work

Certain encryption and decryption techniques of a message involving Spiral Rotation Technique and Aryabhata Substitution Code have been established by Bhati [1], Kandele [5], Kumar [6], Mahendran [7], Mandle [8], Mittal [9], Mittal [10], Paul [11] and others.

Looking importance and usefulness of encryption and decryption techniques of a message, we propose to establish a new encryption and decryption techniques of a message involving Byte Rotation Technique, Spiral Rotation Technique and Aryabhata Substitution Code, following on the lines of above authors.

3. Methodology

In this proposed work to encrypt and decrypt a message we used triple technique, one is 'Byte Rotation Technique', second is 'Spiral Rotation Technique' and third is 'Aryabhata Substitution Code'. 'Byte Rotation and Spiral Rotation Technique' is applied on different blocks pf plaintext and executed in parallel manner.

In the proposed method firstly we apply the secret key matrix along with congruence modulo 26 and thereafter we apply the 'Byte Rotation Technique' for encryption a message and find an intermediate cipher and then we apply 'Spiral Rotation Technique' and obtain another cipher. After that we use 'Aryabhata Substitution Code' and obtain final cipher text. In reverse process firstly we apply 'Aryabhata Substitution Code' and obtain intermediate cipher and then we apply 'Spiral Rotation Technique' and we get another cipher and then we use the 'Byte Rotation Technique' to get original plain text.

Numerical values for alphabets and some symbols used in the paper given in the following table:

Table 1
Alphabets and their numeric code

A	1	N	14
B	2	O	15
C	3	P	16
D	4	Q	17
E	5	R	18
F	6	S	19
G	7	T	20
H	8	U	21
I	9	V	22
J	10	W	23
K	11	X	24
L	12	Y	25
M	13	Z	26

Table 2
Aryabhata substitution code

k = 1	kh = 2	g = 3	gh = 4	ṅ = 5
क	ख	ग	घ	ङ.
c = 6	ch = 7	j = 8	jh = 9	ñ = 10
च	छ	ज	झ	ञ
ṭ = 11	ṭh = 12	ḍ = 13	ḍh = 14	ṇ = 15
ट	ठ	ड	ढ	ण
t = 16	th = 17	d = 18	dh = 19	n = 20
त	थ	द	ध	न
p = 21	ph = 22	b = 23	bh = 24	m = 25
प	फ	ब	भ	म

Other remaining 8 consonants are avarga letters:

Table 3
Avarga letters

य	र	ल	व
ś = 70	ṣ = 80	s = 90	h = 100
श	ष	स	ह

The varga letters (k to m) represented squares such as 1, 100, 10000. The avarga letters (y to h) represented non-squares such as 10, 1000. This creates a notational system in place values for numbers as large as 10^{17}:

Table 3
Place values for numbers

17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
au	au	ai	ai	o	o	e	e	*l*	*l*	r	r	u	u	i	i	a	a
औ	औ	ऐ	ऐ	ओ	ओ	इ	इ	ऌ	ऌ	ऋ	ऋ	उ	उ	इ	इ	अ	अ

y = 30	r = 40	*l* = 50	v = 60

4. Algorithm

Encryption:

The steps for encryption algorithm are as follows:

1. Take a non-singular square matrix of order 4 as key (say K).
2. Arrange the character/symbol of plain text in a block size of 16 bytes as 4 × 4 matrix.
3. Convert the alphabet/symbol into their corresponding values using conversion table (agreed by sender and receiver) and call this resultant matrix N (say).
4. Multiply the key matrix K and plain text matrix N under modulo 26. i.e., NK (MOD 26) = A.
5. Obtain the transpose of A, say A^T.
6. Apply the vertical rotation on last three columns of A^T such that rotate three bytes from second column, rotate two bytes from third column, rotate one byte from fourth column and first column unchanged. Call this resultant matrix A^T_{vr}.
7. Apply the horizontal rotation on last three rows of A^T_{vr} such that rotate three bytes from second rows, rotate two bytes from third row, rotate one byte from fourth row and first row remains unchanged. Obtain another matrix say C_{hr}.
8. Spiral rotate the entries of the resultant matrix:

   $S_r =$

a_{11}	a_{12}	a_{13}	a_{14}
a_{21}	a_{22}	a_{23}	a_{24}
a_{31}	a_{32}	a_{33}	a_{34}
a_{41}	a_{42}	a_{43}	a_{44}

   In such a way that, $a_{11} \rightarrow a_{12} \rightarrow a_{21} \rightarrow a_{31} \rightarrow a_{22} \rightarrow a_{13} \rightarrow a_{14} \rightarrow a_{23} \rightarrow a_{32} \rightarrow a_{41} \rightarrow a_{42} \rightarrow a_{33} \rightarrow a_{24} \rightarrow a_{34} \rightarrow a_{43} \rightarrow a_{44} \rightarrow a_{11}$ by moving one or more steps forward. Let the transformed matrix be S_r.
9. Convert the numeric values of element of S_r into alphabets using Aryabhata's Substitution Code, we get cipher text.

Decryption:

The steps for decryption algorithm as follow:

1. Consider the cipher text and arrange it in a square matrix of order 4 of block sized of 16 bytes. After arranging convert them into numeric values using

Aryabhata's Substitution Code, and get a resultant matrix say Z.

2. Spiral rotate the entries of the resultant matrix:

D =

a_{11}	a_{12}	a_{13}	a_{14}
a_{21}	a_{22}	a_{23}	a_{24}
a_{31}	a_{32}	a_{33}	a_{34}
a_{41}	a_{42}	a_{43}	a_{44}

such a way that $a_{44} \rightarrow a_{43} \rightarrow a_{34} \rightarrow a_{24} \rightarrow a_{33} \rightarrow a_{42} \rightarrow a_{41} \rightarrow a_{32} \rightarrow a_{23} \rightarrow a_{14} \rightarrow a_{13} \rightarrow a_{22} \rightarrow a_{31} \rightarrow a_{21} \rightarrow a_{12} \rightarrow a_{11} \rightarrow a_{44}$ by moving one or more steps forward. Let the transformed matrix be D.

3. Apply the horizontal rotation on last three rows of D such that rotate three bytes from second row, rotate two bytes from third row, rotate one byte from fourth row and first row remains unchanged, we get a matrix say D_{hr}.
4. Apply the vertical rotation on last three columns of D_{hr} such that rotate three bytes from second column, rotate two bytes from third column, rotate one byte from fourth column and first column remains unchanged, we get a matrix say F_{vr}.
5. Obtain the transpose of matrix F_{vr} and denoted by F^{T}_{vr} (say B).
6. Calculate $BK^{-1} \pmod{26} = P$.
7. Convert the element of P into alphabet/symbol using conversion table (agreed by sender and receiver) and arrange them row wise, we get original plain text.

Ittustration:

Encryption Steps:

1. Consider a non-singular matrix (say K) of order 4 × 4 as key matrix:

$$K = \begin{bmatrix} 2 & 1 & 2 & 1 \\ 3 & 5 & 2 & 2 \\ 5 & 1 & 3 & 1 \\ 3 & 1 & 3 & 2 \end{bmatrix}$$

2. Consider the plaintext:
"Sare Jahan Se Acha" is a patriotic song from India.
Pick up a part of this message as given below:
SAREJAHAANSEACHA
3. Arrange them in a block size of 16 bytes i.e. 4 × 4 matrix (say P), we get.

$$P = \begin{bmatrix} S & A & R & E \\ J & A & H & A \\ A & N & S & E \\ A & C & H & A \end{bmatrix}$$

4. In the above block matrix substitute numeric values of letters from Table 1, as follows:

$$N = \begin{bmatrix} 19 & 1 & 18 & 5 \\ 10 & 1 & 8 & 1 \\ 1 & 14 & 19 & 5 \\ 1 & 3 & 8 & 1 \end{bmatrix}$$

5. Multiply the key matrix K and text matrix N under modulo system 26 (as agreed by sender and receiver), we get the following Multiplicative matrix as given below:

NK (mod 26) = A (say)

$$\Rightarrow A = \begin{bmatrix} 19 & 1 & 18 & 5 \\ 10 & 1 & 8 & 1 \\ 1 & 14 & 19 & 5 \\ 1 & 3 & 8 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 & 2 & 1 \\ 3 & 5 & 2 & 2 \\ 5 & 1 & 3 & 1 \\ 3 & 1 & 3 & 2 \end{bmatrix}$$

$$(\text{mod } 26) = \begin{bmatrix} 16 & 21 & 5 & 23 \\ 14 & 24 & 23 & 22 \\ 24 & 17 & 24 & 6 \\ 2 & 25 & 9 & 17 \end{bmatrix}$$

6. Obtain the transpose of A, we get

$$A^{T} = \begin{bmatrix} 16 & 14 & 24 & 2 \\ 21 & 24 & 17 & 25 \\ 5 & 23 & 24 & 9 \\ 23 & 22 & 6 & 17 \end{bmatrix}$$

7. Now apply the vertical rotation on last three columns of A^{T}, such that rotate three bytes from 2nd column, rotate two bytes from 3rd column, rotate one byte from 4th column and 1st column remains unchanged. Denote the resultant matrix by A^{T}_{vr}, we get-

$$A^{T}_{vr} = \begin{bmatrix} 16 & 24 & 24 & 17 \\ 21 & 23 & 6 & 2 \\ 5 & 22 & 24 & 25 \\ 23 & 14 & 17 & 9 \end{bmatrix}$$

8. Applying the horizontal rotation on last three rows of A^{T}_{vr}, such that rotate three bytes from 2nd row, rotate two bytes from 3rd row, rotate one byte from 4th row and 1st row remains unchanged. Denote the resultant matrix by C_{hr}, we get

$$C_{hr} = \begin{bmatrix} 16 & 24 & 24 & 17 \\ 23 & 6 & 2 & 21 \\ 24 & 25 & 5 & 22 \\ 9 & 23 & 14 & 17 \end{bmatrix}$$

9. Spiral Rotating all the entries of C_{hr} about the diagonal elements by only one step from the first entry, we get

$$S_{r} = \begin{bmatrix} 17 & 16 & 6 & 24 \\ 24 & 24 & 17 & 5 \\ 23 & 2 & 23 & 21 \\ 25 & 9 & 22 & 14 \end{bmatrix}$$

10. Convert the numeric values of Sr into their corresponding alphabet letters using Table 2, 3 and 4 (Aryabhata's Substitution Code), we get the following ciphertext matrix

$$E\ (say) = \begin{bmatrix} th & t & c & bh \\ bh & bh & th & ṅ \\ b & kh & b & p \\ m & jh & ph & ḍh \end{bmatrix}$$

Therefore, ciphertext is

thtcbhbhbhthn ḅkhbpmjhphḍh

Via secure channel this ciphertext and key is sent to the receiver.

Decryption Steps:

1. Consider the cipher text
   thtcbhbhbhthn ḅkhbpmjhphḍh
2. Arrange them in a square matrix (row wise) of order 4 in a block of 16 bytes, we get
$$Z\ (say) = \begin{bmatrix} th & t & c & bh \\ bh & bh & th & ṅ \\ b & kh & b & p \\ m & jh & ph & ḍh \end{bmatrix}$$
3. Convert the above character matrix of ciphertext into their corresponding numeric values using Table 2, 3 and 4 (Aryabhata's Substitution Code), we get
$$Z = \begin{bmatrix} 17 & 16 & 6 & 24 \\ 24 & 24 & 17 & 5 \\ 23 & 2 & 23 & 21 \\ 25 & 9 & 22 & 14 \end{bmatrix}$$
4. Spiral Rotating all the entries of Z about the diagonal elements by only one step from the last entry, we get
$$D = \begin{bmatrix} 16 & 24 & 24 & 17 \\ 23 & 6 & 2 & 21 \\ 24 & 25 & 5 & 22 \\ 9 & 23 & 14 & 17 \end{bmatrix}$$
5. Applying the horizontal rotation on last three rows of D, such that rotate three bytes from 2 nd row, rotate two bytes from 3rd row, rotate one byte from 4th row and 1st row remains unchanged, we get
$$D_{hr}\ (say) = \begin{bmatrix} 16 & 24 & 24 & 17 \\ 21 & 23 & 6 & 2 \\ 5 & 22 & 24 & 25 \\ 23 & 14 & 17 & 9 \end{bmatrix}$$
6. Now apply the vertical rotation on last three columns of D_{hr}, such that rotate three bytes from 2nd column, rotate two bytes from 3rd column, rotate one byte from 4th column and 1st column remains unchanged, we get
$$F_{vr}\ (say) = \begin{bmatrix} 16 & 14 & 24 & 2 \\ 21 & 24 & 17 & 25 \\ 5 & 23 & 24 & 9 \\ 23 & 22 & 6 & 17 \end{bmatrix}$$
7. Obtain the transpose of F_{vr}, we get
$$F^{T}_{vr} = \begin{bmatrix} 16 & 21 & 5 & 23 \\ 14 & 24 & 23 & 22 \\ 24 & 17 & 24 & 6 \\ 2 & 25 & 9 & 17 \end{bmatrix} = B\ (say)$$
8. Calculate
   $BK^{-1} \pmod{26} = P\ (says)$
   $\Rightarrow P$
$$= \begin{bmatrix} 16 & 21 & 5 & 23 \\ 14 & 24 & 23 & 22 \\ 24 & 17 & 24 & 6 \\ 2 & 25 & 9 & 17 \end{bmatrix} \begin{bmatrix} 13 & 19 & 17 & 5 \\ 3 & 12 & 7 & 9 \\ 12 & 21 & 2 & 11 \\ 0 & 12 & 7 & 11 \end{bmatrix} \pmod{26}$$
$$\Rightarrow P = \begin{bmatrix} 19 & 1 & 18 & 5 \\ 10 & 1 & 8 & 1 \\ 1 & 14 & 19 & 5 \\ 1 & 3 & 8 & 1 \end{bmatrix}$$
9. Convert the above matrix into their corresponding alphabet/symbol using Table 1, we get a plaintext matrix as follows:
$$\begin{bmatrix} S & A & R & E \\ J & A & H & A \\ A & N & S & E \\ A & C & H & A \end{bmatrix}$$
10. Arrange the characters of above matrix in row wise, we get the original plain text as
    SAREJAHAANSEACHA

Note: We can encrypt the whole message by considering a large matrix.

5. Result and Discussion

To encrypt and decrypt the message there is no single algorithm is sufficient to fulfill the purpose. Therefore, to remove the deficiency and finding better solution a number of researchers are working in the field of cryptography. In this paper we develop a new algorithm which involves 'Byte Rotation Technique', 'Spiral Rotation Technique' and 'Aryabhata Substitution Code'. This algorithm has two steps. Firstly the plaintext is divided into number of chosen blocks, where size of each block is 16 bytes. After applying byte rotation technique, we get an intermediate cipher. In the second step we use spiral rotation technique and Aryabhata substitution code. Therefore, such type of algorithm provides a double security system. Hence with a cipher text only attack, the block cipher cab be difficult to break. Hence, encryption scheme involving spiral rotation technique alongwith Aryabhata substitution code, system is more justified technique providing higher security and higher speed in this wireless world.

6. Conclusion

There are various advantages, disadvantages and challenges

of an algorithm. Since our algorithm is developed by spiral rotation technique and Aryabhata substitution code, therefore our system proposed a good strategy. It uses spiral rotation to shuffle the letters and Aryabhata substitution to replace them with numbers, making it harder for attackers to break. The spiral pattern changes the letter positions, while the Aryabhata substitution methods adds extra security by converting them into numbers. This combined approach makes the system more secure and powerful against different types of attacks. Overall, our encryption method provides a strong and reliable way to protect information.

References

[1] Bhati Sunita, Bhati Anita, Sharma S. K.: A New Approach towards Encryption Schemes: Byte-Rotation Encryption Algorithm, Proceedings of the World Congress on Engineering and Computer Science, Vol II WCECS, 2012, pp. 1-4.

[2] Forouzan Behrouz A: Cryptography & Network Security, McGraw Hill Education, 2007.

[3] Kahate atul: Cryptography and Network Security, Tata McGraw Hill, New Delhi, 2008.

[4] Kak S.: "Aryabhata's Mathematics," in RSA Conference, 2006.

[5] Kandele Suyash and Anand Veena: A Novel Square-Expanded-Matrix-Rotation (SEMR) Cryptography Method, International Journal of Engineering Research and Technology (IJERT), Volume 4, Issue 04, April-2015, pp. 1366-1378.

[6] Kumar S. Sanal and Sherfin S. Anfino: A Cryptographic Encryption Technique Byte- Spiral Rotation Encryption Algorithm, Journal of Discrete Mathematical Science and Cryptography, Volume 22 (2019), No. 3, pp. 371-376.

[7] Mahendran R: Byte Rotation with CBC Encryption Algorithm, International Journal of Machine and Construction Engineering, Volume 1, Issue 1, August 2014.

[8] Mandle Amit Kumar, Namdeo Varsha: Encryption and Decryption of a Message Involving Byte Rotation Technique and Invertible Matrix, International Journal of Engineering and Advanced Technology (IJEAT), Volume-9 Issue-2, December, 2019, pp. 1160-1163.

[9] Mittal Ayush and Gupta Ravindra Kumar: A New Encryption Scheme Involving Finite Field and Byte Rotation Technique, Journal of Xi'an University of Architecture & Technology, Volume XII, Issue III, 2020, pp. 1166-1174.

[10] Mittal Ayush and Gupta Ravindra Kumar: Cryptographic Scheme Involving Byte Rotation Technique and Laplace Transformation, Journal of Xidian University, Volume 14, Issue 3, 2020, pp. 145-151.

[11] Paul Manas and Mandal Jyotsna Kumar: A Novel Symmetric Key Cryptographic Technique at Bit Level Based on Spiral Matrix Concept, International Conference on Information Technology, Electronics and Communications (ICITEC – 2013), Bangalore, India, March 30 – 31, 2013, pp. 06-11.

[12] Stallings William: Cryptography and Network Security Principles and Practices, Prentice Hall, 2005.