ROTATIONAL SHIFTS AND BUILDING BLOCKS BASED SECURITY CIPHER

Ch. Rupa[1], R. Sudha Kishore[2], P. S. Avadhani[3]
[1,2]Department of Computer Science Engineering, VVIT, A.P., India
[3]Department of CS & SE, Andhra University, Vizag, A.P., India

ABSTRACT

Development in information technology brought up various problems and threats associated with it. It is essential to make the communication between two parties secret. In this paper we proposed a method to provide more security in relation to the key, here the sender doesn't have any necessity of transferring a key along with ciphertext while communicating. At receiver side needs to generate reference tables and Building blocks for decrypting the data as same as at sender side. Here reference table uses rotational shifts towards top- down and down-top based on indexing of the bits and building blocks uses character indexing blocks and transpose indexing blocks. These are the main components of the proposed method. The main strength of the paper is cryptanalysis of the proposed algorithm shows that it is resistant to various attacks.

KEYWORDS: *Rotational shifts, Reference Table, Building Blocks (3X3), Character Indexing, Transpose Indexing.*

I. INTRODUCTION

The extreme development of internet makes convenient to transmit and access and distribute the information. Over the last few decades, many security algorithms such as Block cipher [1], Private Key [2, 14] or public key algorithms [3,9, 12] are used to produce the codeword from the data word. Weather it may be the rapid growth of the technology or the lack of security in relation to the keys are causes to face the security problems like loss or modify the privacy information by attacking [4, 14]. This proposed algorithm reduces these kinds of problems and gives the better solution. It improves the efficiency in the aspect of less time complexity, satisfies all security services and improves the confusion.

Any authenticated schemes have the following properties i.e. Confidentiality which is referred as secret information shared between sender and receiver; any outsider cannot read the information [3, 13]. The sender traces his identity, which only the designated receiver can loosen and verify. An anonymous adversary cannot send a malicious message masquerading as the original sender, because he does not have the necessary tools to generate the signature is referred as authentication. Next important security service as a property is Non – repudiation [3, 9]. Here the signature firmly establishes the identity of the sender. The sender cannot deny having sent the message and the signature. The last property is Message recovery [13]. Here, upon receipt of the cipher text, the recipient decrypts it and separates the signature and the message and verifies the authenticity of the sender. Only he will be able to do so because he alone has the necessary tools.

All security algorithms need to satisfy these properties for providing the complete security to the information while in communication [15]. Then only can protect the secure data by all the perspectives of the attackers. In this paper we proposed a method as an algorithm for providing the security to the data with out transmit a key through encrypted data communication. That is if sender wants to send any data to the receiver, first it itself generates a table referred as rotational shifts table

and its resultant is called as resultant reference table. By the reference of these tables sender will creates 3X3 building blocks by using the mathematical operations like transpose which are used to convert plaintext into cipher text. Now, only ciphertext can be participated in the communication channel with out a key. At receiver side, it itself generate the tables and blocks which are generated at sender side without regards of the tables and blocks information from sender side. Here, the ciphertext is converted into plain text with the help of receiver generated things as tables and blocks. In this paper we developed an algorithm up to converting the ciphertext into plaintext only but can enhance this work until verification process at receiver side like whether the received plaintext is genuine or not by using any hashing mechanisms like MD5[16], SHA [17], etc. This method has may advantages than exiting methods moreover it con satisfies all security services along with the resistant from the cryptanalysis attacks.

The rest of the paper is organized by the following way. Section 2 consists of proposed method. Section 3 holds the advantages of the proposed method. Results and discussion with cryptanalysis are illustrated in Section 4.

II. PROPOSED METHOD

In this work we have devised an algorithm for data cryptography which is improved version of existing algorithms as DES [4], Sierpinski [5], and cheating text [6]. In this paper we have proposed a method to encrypts the data and transmit the secure codeword i.e. ciphertext with out a key. It specifies that the sender encodes the data by using Encryption algorithm which uses the reference table as discussed in section 2.2 and section 2.3 then the resultant is referred as ciphertext. It is only transmitted to the receiver. Whenever the secure codeword as ciphertext only is received by the receiver then immediately decrypt the ciphertext by using decryption algorithm which is also used reference table as shown in section 2.4 and section 2.3 to get the original data. This proposed method initially has three modules that are Reference table creation, creation of three character and index Blocks with the size of 3x3 and Transpose blocks. Encryption and decryption of an original text is done based on these three modules of the reference algorithm. This process is shown as Figure 1.

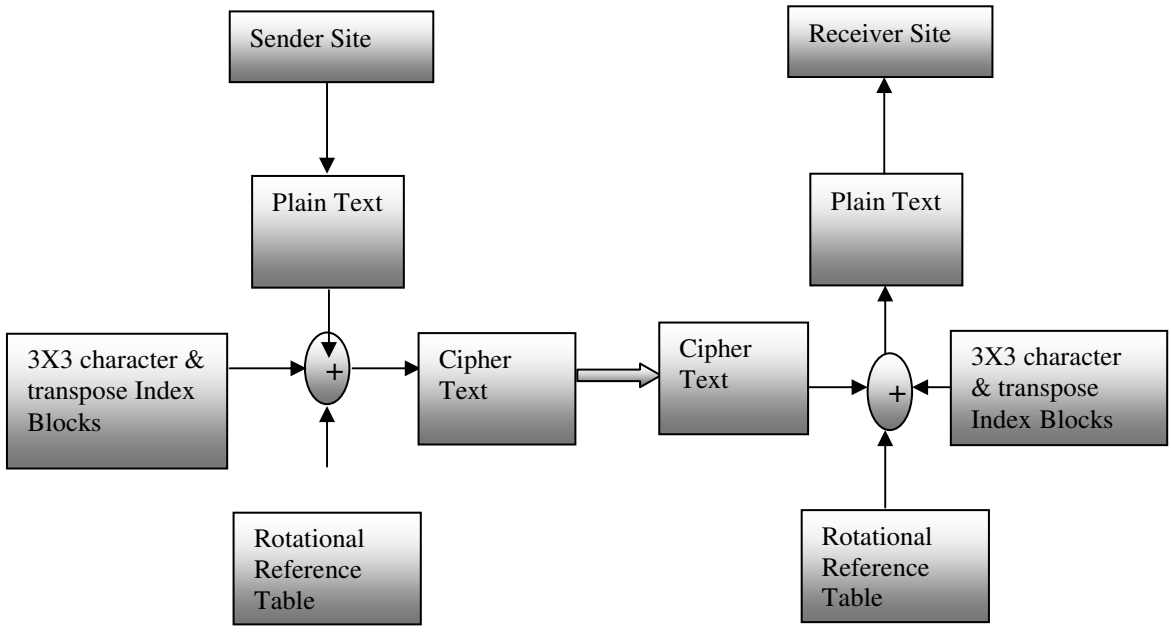


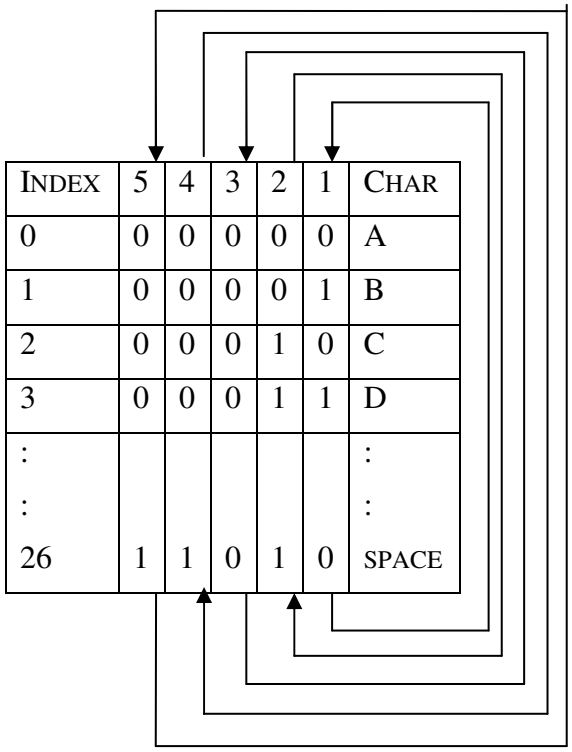
Figure 1. Process of Proposed Method

2.1. Methodology of Reference Table Creation

In module 1 the reference table is created by the principle of rotational shift as shown in Table 1. This table holds seven columns. First column is for index, Column 2 to column 6 (i.e 1 to 5) are reserved for bits representation of the characters (i. e A to Z and a delimiter). Seventh column stores the corresponding Alphabetic character. Here, it applies top to down rotational shift for even indexing

columns and circular down to top shift for odd indexing columns. The resultant reference table is shown as table 2. In this context, if two or more rows obtain the same index then update the index by the nearest prime value of that index. If that prime value is also existed then again find the nearest prime number of the prime value. Repeat this procedure until get all values is unique in a table. It is shown as Table 2.

Table1. Rotational shift reference table



INDEX	5	4	3	2	1	CHAR
0	0	0	0	0	0	A
1	0	0	0	0	1	B
2	0	0	0	1	0	C
3	0	0	0	1	1	D
: : 26	1	1	0	1	0	: : SPACE

Table 2. Resultant Reference table

INDEX	5	4	3	2	1	CHAR
16	1	0	0	0	0	A
2	0	0	0	1	0	B
3	0	0	0	1	1	C
0	0	0	0	0	0	D
: : 17	1	0	0	0	1	: : SPACE

Module 2 consists of two stages. In a stage 1, needs to create three blocks by the order of 3X3 which store all the characters (A to Z) including delimiter by sequentially as shown in Figure 2, Figure 3 and Figure 4. With the reference of the resultant reference table fill up the blocks with the value regards the corresponding character as stage 2. Those are referred as Figure 5, Figure 6 and Figure 7.

A	B	C
D	E	F
G	H	I

Figure 2. Character Block 1

J	K	L
M	N	O
P	Q	R

Figure 3. Character Block 2

S	T	U
V	W	X
Y	Z	→

Space as delimiter

Figure 4. Character Block 3

16	2	3
0	1	6
7	12	13

Figure 5. Index Block 1

10	11	8
9	14	15
4	5	18

Figure 6. Index Block 2

19	23	17
22	27	26
17	28	31

Figure 7. Index Block 3

16	0	7
2	1	12
3	6	13

Figure 8. Transpose Index Block 1

10	9	4
11	14	5
8	15	18

Figure 9. Transpose Index Block 2

19	22	17
23	27	28
17	26	31

Figure 10. Transpose Index block 3

In this proposed method no key is participating in the communication. First, sender as an encoder converts the original data in to ciphertext using reference algorithm which is formatted based on the reference tables and 3X3 blocks and Encryption algorithm as discussed in section 2.1 and section 2.2. At sender side, only ciphertext can be placed on the transmission media with out any key. Now, at receiver side, receiver decodes the ciphertext which has received by the sender into plaintext by the reference of reference algorithm and Decryption algorithm as shown in the following sections.

2.1.1 Reference Algorithm

This algorithm is used by both encoder and decoder for encoding the plaintext and for decoding the ciphertext. It is designed based on the rotational reference table and its resultant table as well as character blocks and Index blocks. At both sender and receiver side generate the reference tables and 3X3 blocks by its own using the following algorithm. It acts as a key at both sender and receiver sides.

Algorithm

Step1: Give index to all the alphabets along with any delimiter as space.
i.e *index[k]*. Where '*k*' and '*val(index[k])*' = 0 to 26.
Step2: Convert *val(index[k])* into 5 bit binary.
For i= 0 to 26
For j= 1 to 5
Rotat[i][j]=Bin[i][j] =Binary(val(index[k]))
Step3: Apply separate rotation procedures for Even index (*Bin)* i.e j=2,4,6… and Odd_index(*Bin)* i.e j=1,3,5…..
Step3.1. If (*Odd_index (Bin)*) then I=0;
Repeat
rotat[i+1][j]=rotat[i][j]; i++;
Until (i<=25); rotat[0][j]=rotat[26][j]
Step3.2. If *(Even_ index(Bin))* then *rotat[26][j]=rotat[0][j]*; I=26;
Repeat
rotat[i-1][j]=rotat[i][j]; i - -;
until(i==1)
Step4: Convert *rotat* into ASCII values. i.e ascii[rotat].
Step5: Assign alphabets and space to *ascii[rotat]* by consecutive .
i.e Ascii[rotat]=alpha[t] where t= A to Z and delimiter as space.
Step6: Take 3 blocks with the size of 3X3. *Block[i][j]* where i=j=3
Step7: Arrange all alphabets including delimiter in to the blocks by sequence.
Block[i][j]=alpha[t] where t= A to Z and delimiter as space
Step8: Assign corresponding *Ascii[rotat]* values of *block[i][j]*;
Block1[i][j]=Ascii[rotat](block[i][j])
Step9: Find transpose (block[i][j]) i.e Transblock[i][j] =$(block1[i][j])^T$

2.2. Encryption Algorithm

At sender site, plaintext is converted in to ciphertext by using the transpose of 3X3 index blocks which make through the reference of reference table by sender itself. It has shown as follows.

Algorithm

Step1: Convert plaintext into tokens as character i.e *Char[t]*
Step2: Assign a value to *char[t]* by the reference of *Transblock*
Step3: Assign a token to val(char[t]) by the reference of *alphabets_ at_ ascii[rota]* from Sec 2.1 i.e Ciphertext.
Val(char[t])= alphabets_at_ascii(rota).

2.3. Decryption Algorithm

At receiver site, ciphertext is transformed in to plaintext by using the transpose of 3X3 index blocks which build through the orientation of reference table by receiver itself. It has shown as follows.

Algorithm

Step1: Convert ciphertext into tokens as character i.e *Rchar[t]*
Step2: Assign corresponding value to *Rchar[t]* by the reference of *Transblock.*
Step3: Assign a resultant token to *val(Rchar[t])* by the reference of *alphabets_at_ ascii[rota]* from Sec 2.1. i.e Plaintext.
Val(Rchar[t])= alphabets_at_ascii(rota).

III. ADVANTAGES OF PROPOSED METHOD

The need of securing the information from the third party is improves the security services like authentication and confidentiality. The digitization of sensitive data and transfer of it through a network along with the key is a main cause to attack the information by the eavesdropper. This proposed algorithm overcomes the limitations which are existed in the present approaches [1, 2, 3, 4, 8]. Unlike most of the security algorithms which include a separate key while transmitting the message our algorithm extracts the key from the message itself. The algorithm we proposed is easy to implement and requires no transmission of key through a third party. The main advantages of the present system are as follow.

Advantages

1. The proposed algorithm provides greater security in relation to the keys. As no explicit keys are required, we don't have any necessity of transferring key through the communication channel. Eventually, it reduces the intrusion by eavesdropper.
2. Here, key generation is occurs at both sides as sender and receiver by them own. Hence the chances are less for identifying a key by the unauthorised person.
3. It is using shifting operation but neither left shift nor right shift. Instead, here we use rotational shifts towards top - down and down -top based on indexing. It may improve the confidentiality and confusion.
4. We have constructed the algorithm such that it comprises the simpler algebraic operations like TRANSPOSE, SHIFT, and these operations are found to require lesser time complexity as compared to number generation [4] or any other logarithmic [5, 8] or exponential operations [6,9] as in other encryption techniques.

IV. RESULT AND DISCUSSION

Plaintext: master
Plaintext in transpose block data: 11 16 19 22 1 18
Ciphertext: kasver

4.1 Encryption and Decryption Scheme

Figure 2, Figure 3 and Figure 4 show insertion of characters in sequential order, and Figure 5, Figure 6 and Figure 7 show the insertion of index of characters by the reference Table 2. Now, transpose the three index blocks then the resultant is stored as separate blocks by the name of transpose index blocks. The plaintext in transpose block data is 11 16 19 22 1 18. Cipher text in characters with the reference of Table 2: kasver. Decryption procedure is exactly same as encryption done in reverse

order by the use of reference Table 2 and 3X3 character and transpose index blocks as shown as Figure 8, Figure 9 and Figure 10.

4.2 Cryptanalysis

Cryptanalysis analyses the attacks that are possible based upon the characteristics of the design of the algorithm in order to deduce a specific plaintext or the secret key used [7]. This rotational shifts and building blocks security cipher resistant all the four of cipher text only, known plain text, chosen plain text and chosen cipher text attacks. In the cipher text only attack, the cryptanalyst will know the encryption algorithm and the cipher text that has to be decoded [8]. Proposed method has fewer chances to break the ciphertext from the encryption algorithm with out having the knowledge regarding reference table. This table is not been in the communication. Hence this method can resistant from this attack.

The attacker will have knowledge of the cipher text and one or more plaintext-ciphertext pairs and encryption algorithm are referred as known plain text attack [10]. The proposed method case study shows that the plaintext that is known is more in size then the number of attempts will be less to find out the key. In the chosen plain text attack, the attacker selects the plaintext together with its ciphertext generated with the secret key. And in the chosen cipher text attack, the attacker selects the ciphertext together with its decrypted plaintext generated with the secret key. If we select a plaintext/cipher text of fixed size we get different types of cipher / plain texts due to of using prime numbers and for a plain / cipher text of size fixed size we get different types of cipher / plain texts because of using the prime numbers in the resultant of reference table.

V. CONCLUSIONS AND FUTURE WORK

The Rotational shifts and Building Blocks based security cipher provides a mechanism to transmit the encrypted data i.e. ciphertext without any external key. This directs to saving of certain amount of time consumed to transmit the key. The results depicted in the preceding section clearly show the better performance shown by the proposed algorithm as compared to other algorithms for security.

In this method we used circular shifts towards top – bottom and bottom to top depends on indexing of the cells as well as two kinds of building blocks for improving the confusion with more reliability of the communication. Time complexity is less comparatively existing algorithm because it uses shifts and transposes operations instead of logarithmic, exponentials. Eventually, it prevents eavesdropper from attacking the data being sent during communication process.

At present days information attacks are rapidly increasing due to the cause of globalisation. Hence, as a part of the future work we would like to implement this work using image watermarking to improve the security of the information. The robust watermarking method will be used for increasing the security of data hiding as well as quality compared with the existing algorithms.

REFERENCES

[1]. Ayushi, (2010), “A symmetric key cryptographic algorithm”, Int. Journal of Comp. Applications, vol. No. 15, pp 1- 4.
[2]. Sunil. T. et. al, (2011), “Secret Key establishment for symmetric encryption over Adhoc networks”, Proc. of WCECS 2011, Vol II, pp 1- 5.
[3]. Prakash. K et. al, (2011), Enrichment of security through cryptographic public key Algorithm based on bock Cipher”, IJCSE, Vol 2. No 3, pp 347 – 353.
[4]. Coppersmith. D, (1994) “The data Encryption standard (DES) and its strength against attacks”, URL://journal /rd/383/coppersmith.pdf.
[5]. Devaney, R.L, (1999) “Measure Topology and Fractal Geometry”, Key Curriculum Press, pp.65-75.
[6]. Ch. Rupa and P. S. Avadhani, (2009) “Message Encryption Scheme Using Cheating Text”, ITNG: Sixth International Conference on Information Technology: New Generations International Journal of Computer Science and Mathematical Applications, ISBN: 978-0-7695-3596-8/09(indexed by IEEE,dblp), pp. 470-475.
[7]. Vinod Kumar Godavarty, (2011) “Using Quasigroups for Generating Pseudorandom Numbers”, Arxiv preprint arXiv:1112.1048 - arxiv.org.
[8]. Milena Tvrdíková, (2012) **“**Information System Integrated Security”, IGI Global Dissimilator of Knowledge, pp 158-169.

[9]. Paul C. Kocher, (1998) "Timing Attacks on Implementations of Die-Hellman, RSA, DSS, and Other Systems", IEEE Transactions on Information Theory, pp 1- 10.
[10]. Alex Biryukov. et. al, (1998) " From Differenti Cryptoanalysis to Ciphertext-only attacks", CRYPTO – LNCS 1462, pp. 72 – 88.
[11]. Kocarev, L, (2001), "Chaos-based Cryptography: A Brief Overview", IEEE Circuits and Systems Magazine 1(3), pp. 6-21.
[12]. Ming-Der Shieh, Jun-Hong Chen, Hao-Hsuan Wu and Wen -Ching Lin, (2008), "A New Modular Exponentiation Architecture for Efficient Design of RSA Cryptosystem", IEEE Transactions, Vol. 16, No. 9, pp. 1151-1162.
[13]. Christian Cachin, Jan Camenisch, (2010) "Encrypting Keys Securely", IEEE Security & Privacy, pp: 66-69.
[14]. Sean O'Melia, Adam J. Elbirt (2010), "Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions", IEEE Trans. VLSI Syst. 18(11), pp. 1505-1518.
[15]. Yongge Wang and Yvo Desmedt, (2008) "Perfectly Secure Message Transmission Revisited", IEEE Transactions on Informaiton Theory, Vol. 54, No. 6, pp 2582-2596.
[16]. Xiaoyun Wang, Dengguo Feng, Xuejia Lai and Hongbo Yu, (2004) "Collisions For Hash Functions MD4, MD5, HAVAL-128 and RIPEMD", Science & Communication, pp 235-255.
[17]. Xiaoyun, Yiqun Lisa Yin and Hongbo Yu, (2005) "Collision Search Attack on SHA1", Lecture Notes in Computer Science, pp 134- 142.

AUTHORS

Ch. Rupa is working as Associate Professor in VVIT, Andhra Pradesh, INDIA. She has received B.Tech from JNTU, Hyderabad , M.Tech (CSIT) and Ph. D (CSE) degrees are from Andhra University. This author became a Life Member of CSI, ISTE, IAENG, IEI, IACSIT. She published more than 35 papers in various journals and conferences. JNTU Kakinada had awarded her as a Young Engineer of 2010. IEI awarded her as National young Engineer of 2011. Her main research interest includes information security, Image Processing, Security algorithms.

R. Sudha Kishore is working as Assistant Professor in VVIT, Andhra Pradesh, INDIA. He has received B. Tech and M. Tech degrees from JNTU Hyderabad. This author has overall 7 years teaching experience and guided more than 10 innovative projects as a part of his academic work. His research interests are Image processing, Information security, security algorithms.

P. S. Avadhani became a life member of CSI, ISTE, IAENG, IE, IEEE etc. He received his PhD degree from, IIT Kanpur, India in 1993. He is currently working as professor at Andhar University, visakhapatnam, INDIA. He had so many honors. He received best researcher award from Andhra University. He visited many other countries like USA Malaysia, etc. Number of research scholars are enhancing their knowledge under his esteemed guidance. His main areas of interests are Computer Algorithms, Public Cryptographic Algorithms, Data Security, Computer Graphics, Fuzzy Systems.