International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 02, February 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-9663

A NOVEL KEYLESS VKS ALGORITHM

Dr. S. Kiran[1], P. Veereshkumar Goud[2], V. Siva Kumar[3]

1Assistant Professor, 2Student III B. Tech, 3Student III B. Tech,

Dept. of CSE, YSREC of YV University, Proddatur (India)

ABSTRACT

Security place vital role in data communication. There are so many methods available to break data while transmission. To provide protection for information new technologies are essential. Other side breaking algorithms also readily available to unprotect the information. In this aspect, present paper concentrate on keyless transmission of information using VKS algorithm. In this paper, new methods are introduced such as cut and splice, and digit swapping, to enhance the protection elegant pairing algorithm used to generate final cipher text.

Key words: cut and splice, secure transmission, privacy, digit swap, pairing algorithm.

I. INTRODUCTION

The concept of cryptography defines how to secure the data during transmission. Encryption is a process in cryptography which converts the information from readable form to unreadable form. In the process of encryption "Key" plays a key role in converting the information from readable form to unreadable form. Depending on the type of transmission keys are derived as two types public key and private key. As technology is growing intruders hacking the data or sharing the confidential data. To avoid intruders or third party there is a need of better secure algorithm generations.

1.1. Services of cryptography

Cryptography provides broad services such as certification, access control, privacy, integrity and security [4,5]. In cryptography, there exist two types of transmissions such as symmetric and asymmetric.

1.1.1. Symmetric cryptography: In symmetric mechanism, a unique key is used for mutually in both directions.

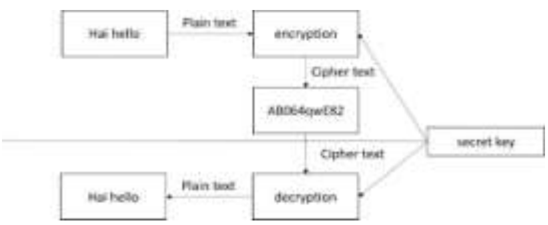


Fig 1. Symmetric cryptography

1.1.2. Asymmetric cryptography: The asymmetric mechanism uses two pieces referred as public and private key. Where the key used at one end is differ from another end.

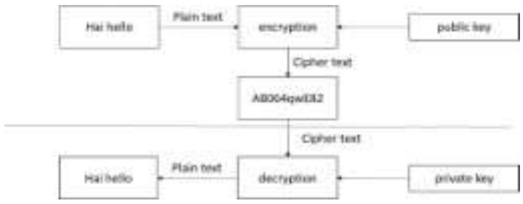


Fig 2. Asymmetric cryptography

II. LITERATURE SURVEY

N. Saisumanth, Jiwan Pokharel, Dr. Ch. Rupa and T. Vijaya Saradhi [7] This paper proposes a keyless[2] algorithm where key has been need not share between sender to receiver and It is always available in the cipher text. The following methods are implemented in case of encryption process: one's complement and graycode generation.

Chandra Prakash Dewangan, Shashikant Agrawal This paper investigated the encryption process on the basis of Avalanche effect.

T. Nie at el. This paper mainly concentrate on how to enhance the consumption of power during transmission in the network with security.

Suparna Karmakar, Sayani Chandra: Reported on enhancing the security of data with various mathematical operations such as perty net and analysis technic which data becomes unpredictable by using above operations.

III. EXISTING METHOD

The existed JS[6] algorithm proposed a new method in key generation by considering the plain text. Further the plain text has been divided into 64-bit chunks, and they split into 30-4-30 bit positions. To achieve the security operations such as gray code, XOR different shift functions to be applied to generate unpredictable cipher text.

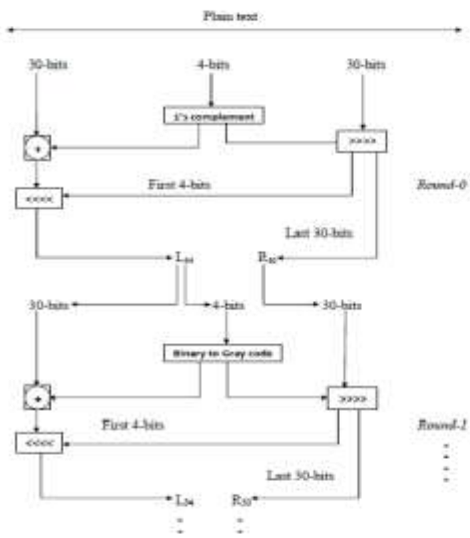


Fig 3. Diagrammatic representation of encryption

ISSN (O) 2454-9665
ISSN (P) 2454-0663

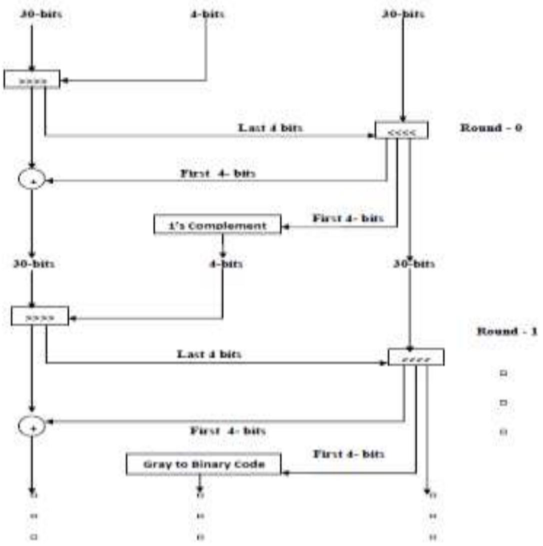


Fig 4. Diagrammatic representation of decryption

IV. PROPOSED METHOD

To provide security for data during transmission several approaches are available. The proposed method introduced a new technique by using genetic operators to provide the security for data. To achieve more security pairing [1,8] and digit swapping techniques are applied. In genetic operations cut and splice[3,7] is one of the operator which is derived from another genetic operator called as cross over.

4.1. Encryption process:

The encryption procedure of proposed method is represented with the help of algorithm and flow chart.

4.1.1. Algorithm:

Step 1: Read the input file

Step 2: Find ASCII value for each character in the file

Step 3: Find Binary Equivalent for ASCII

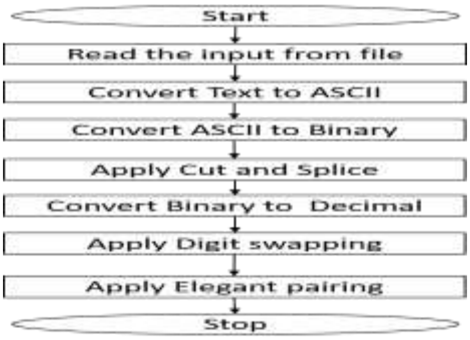
Step 4: Apply genetic operator cut and splice

Step 5: Find decimal equivalent for above operations

Step 6: Apply digit swapping

Step 7: Apply pairing function

4.1.2. Flow chart:



4.1.3. Example

Step 1: Read the input file

SECURITY

Step 2: Find ASCII value for each character in the file

83 69 67 85 82 73 84 89

Step 3: Find Binary Equivalent for ASCII

Decimal Values	Binary Values
83	01010011
69	01000101
67	01000011
85	01010101
82	01010010
73	01001001
84	01010100
89	01011001

Step 4: Apply genetic operator cut and splice

Binary Values	Changed binary values
01010011	10101010
01000101	01101000
01000011	10101000
01010101	01101010
01010010	00101010
01001001	01001001
01010100	00101010
01011001	10001011

Step 5: Find decimal equivalent for above

Binary values	Decimal Values
10101010	170
01101000	104
10101000	168
01101010	106
00101010	42
01001001	73
00101010	42
10001011	139

ISSN (O) 2454-9665
ISSN (P) 2454-0663

Step 6: Apply digit swapping

Decimal Values	Changed Decimal Values
170	140
104	170
168	168
106	160
42	27
73	34
42	49
139	132

Step 7: Apply pairing function

Changed Decimal Values		Paired value
140	170	29040
168	160	28552
27	34	1183
49	132	17473

4.2. Decryption process

The decryption procedure of proposed method is represented with the help of algorithm and flow chart.

4.2.1. Algorithm

Step 1: Read the generated cipher text

Step 2: Apply elegant unpairing function

Step 3: Apply reverse procedure of digit swapping

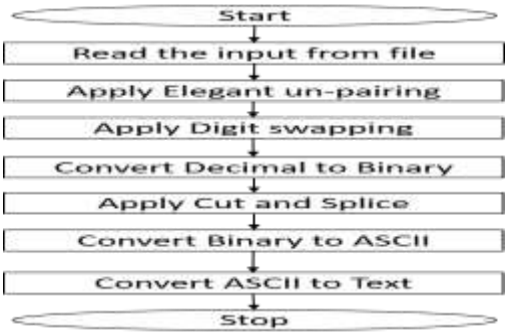
Step 4: Find binary equivalent for above operations

Step 5: Apply the genetic operator cut and splice

Step 6: Find ASCII equivalent for binary

Step 7: Generate appropriate equivalent values of ASCII

4.2.2. Flow chart



4.2.3. Example:

Step 1: Read the generated cipher text

29040 28552 1183 17473

Step 2: Apply elegant unpairing function

Paired values	Unpair values	
29040	140	170
28552	168	160
1183	27	34
17473	49	132

Step 3: Apply reverse procedure of digit swapping

Decimal Values	Changed Decimal Values
140	170
170	104
168	168
160	106
27	42
34	73
49	42
132	139

Step 4: Find binary equivalent for above

Decimal Values	Binary values
170	10101010
104	01101000
168	10101000
106	01101010
42	00101010
73	01001001
42	00101010
139	10001011

Step 5: Apply the genetic operator cut and splice

Binary values	Changed Binary values
10101010	01010011
01101000	01000101
10101000	01000011
01101010	01010101
00101010	01010010
01001001	01001001
00101010	01010100
10001011	01011001

Step 6: Find ASCII equivalent for binary

Binary values	Decimal values
01010011	83
01000101	69
01000011	67
01010101	85
01010010	82
01001001	73
01010100	84
01011001	89

Step 7: Generate appropriate equivalent values of ASCII SECURITY

V. CONCLUSION

In today's era communication playing a prominent role. So many hurdles are involved in communication related to securing the information. Especially, involvement of third party in accessing the secure information is major problem. The proposed work, concentrates on keyless approach for providing better security. The key approach needs exchange of key separately between sender and receiver, this procedure enhances the time analysis of decryption process, to avoid that keyless approach is proposed. In the proposed work, there is no need of chunk division for plain text. Further this work may be extended for Unicode system and also to be utilized to produce pairing algorithm. The major limitation of the existed JS method is the plain text must be always in the form of 64-bit of chunks, which can be overcome with the proposed VKS method.

VI. REFERENCES

[1]. B. Hari Krishna, I. Raja Sekhar Reddy, Dr.S. Kiran, R.pradeep Kumar Reddy, "Multiple text encryption, Key entrenched, distributed cipher using pairing functions and transposition ciphers" IEEE *Xplore* : 15 September 2016, DOI:_ 10.1109 /WiSPNET.2016.7566299.

[2]. Ch. Prem Kumar, Amit Verma , Ravi Prakash "Secure Reach Routing Algorithm Using Keyless Encryption", International Journal of Computer Technology and Applications, 9(11) 2016, pp. 5369-5376.

[3]. S. H. Ling, "Iterated Function System-Based Crossover Operation for Real-Coded Genetic Algorithm", Journal of Intelligent Learning Systems and Applications,2015,7,37-41.

[4]. Neha, Paramjeet Singh, Shaveta Rani "Optimal Keyless Algorithm for Security", International Journal of Computer Applications, Volume 124- No.10, August 2015.

[5]. Raza Ali, Muhammad Shoaib Ali, Syed Aurangzeb, Talha Mir, Zubair Zaland, "Keyless Averaging Encryption Algorithm", J.App.Em.Sc Vol 4, Issue 2,December 2013 pp. 153-156.

[6]. Jiwan Pokharel, N. Saisumanth, Dr. Ch. Rupa, T. Vijaya Saradhi, "A Keyless JS Algorithm", International Journal of Engineering Science & Advanced Technology Volume-2, Issue-5, 1397 – 1401.

[7]. Yilmaz KAYA, Murat UYAR, Ramazan TTEKIN, "A Novel Crossover Operator for Genetic Algorithms: Ring Crossover", 220485962.

[8]. Arnold L. Rosenberg, "Efficient Pairing Functions – and Why You Should Care", 0-7695-1573-8/02/$17.00 © 2002 IEEE.