Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Enhancement of Confidentiality of Data Transmitted Over Covert Channel Using Grid Cipher Scheme

Dr. Raju Singh Kushwaha[1]

1

Received: 6 December 2011 Accepted: 31 December 2011 Published: 15 January 2012

Abstract

In this fast developing world, the interchange of information is playing a key role. Everything needs information and processes them. This interchange of information needs an authentication, confidentiality and integrity. The security of information is provided many algorithms. There are vast numbers of algorithms for symmetry key cipher. All these algorithms have used either complicated keys to encrypt the plain text to cipher text or a complicated algorithms used for it. The level of security of algorithms is dependent on either number of iterations or length of keys. A comparative study have been made with RSA, DES, IDEA, BAM and other algorithms with frequency distribution, bit ratio to check the security level of proposed algorithm. Finally, a comparison has been made for time complexity for encryption of plain text and decryption from cipher text with above existing algorithms.

Index terms— Plain text, cipher text, symmetric key algorithm, grid, RSA Algorithm time complexity and frequency distributions.

1 Introduction

ryptography is the study of transmitting secret messages securely from sender to receiver. [4]The original text, called plain text it's encrypted form is called cipher text, which is sent to the receiver. The recipient decrypts the text to get the plain text. The model of secret key system, first proposed by Shannon ([4]) is shown in figure1.

Figure **??**: The model of secret key system proposed by shannon There are many algorithms had developed to providing security of information but each of them having some merits and demerits. There is no single algorithm is sufficient to provide security. In this paper, an effort has been made to develop a new block cipher algorithms using a set of 16 grids where each grid is 4X4 matrix [2]. Each grid is capable to store 16 characters and finally, all ASCII characters value has Author : Assistant Professor Department of Computer Science Sri Ram Murti Smarak College of Engineering & Technology, Bareilly, (U.P.), India. . E-mail : rajukushwaha36@gmail.com been stored in grid set. The algorithm has been performing two steps. In first step, the plaintext has been broken into number of block eight characters. Each character from each block has been converted into bit stream and placed in the grid set. After placing all characters, new bit stream for each character of the block has been calculated using grid number, row number and column number. In second step, the stream bit is consist of eight bit for single character, calculate their decimal value and assigns the ASCII character for this decimal value. [6]To ensure the security of encryption algorithm many effects have done. These are avalanche, bit ratio, non-homogeneity and time complexity. The avalanche effect means a small change in plain text (or key) should produce a significant change in cipher text. [4]The bit ratio effect means the changes the bit values from same position between plain text and cipher text. The non-homogeneity test is a technique to test nonhomogeneity of the source and encrypted file. The time complexity defines how efficiently the proposed algorithm will encrypt the plain text and decrypt from encrypted text.

2 II.

Literature survey [4] In this paper, the Frame based encryption process is proposed, this is also block cipher scheme which break the plain text into eight character size block. Find their positional value from the frame and put their corresponding ASCII value. This forms a 8-bit stream of data which is swapped with another string and generate their ASCII character. This character is send to the receiver.

[2] In this paper, the proposed algorithm used the 26 characters, 10 numerals and single space character. This form a block of 37 characters, when plain text is encrypted into cipher text the plain text character is taken their value from this block of 37 character and form a matrix of order 3*3. Select a Key matrix of same order and encrypt the data with this process and result is taken modulus by 37. Cipher text is generated and sends to the receiver. [5] In this paper, the proposed algorithm compress the plain text with arithmetic algorithm the resultant value of compress data is encrypt with RSA algorithm, the cipher text is generated and send to the receiver.

Hill cipher's or linear block cipher is susceptible to cryptanalysis and unusable in practice, still serves an important pedagogical role in both cryptology and linear algebra. It is this role in linear algebra that raises several interesting questions [1].

In this paper, the proposed algorithm is a modified form of RSA algorithm named RSA1, which enhance the security of RSA algorithm. The resultant value of RSA algorithm is converted into corresponding ASCII character value and then send to the receiver. [7] III.

3 Proposed work

The algorithms are based on the grid. A single grid consists of 16 characters. Then total number of grid is16 required for representing ASCII set. The total ASCII character are 256.

4 Algorithms: a) Sender Prospects: Encryption

Step 1: Represent each character of plain text by another character which is equivalent a number, generated from reference grid model .Then, the substitute character is represented by the bit sequence (x,y,frame no).

Step 2: Grouping the modified plain text into blocks of eight characters. If modified test is not properly divided by eight then blank characters will be padded with last block.

Step 3: Convert each block into equivalent bit streams.

Step 4: This bit stream converted into Decimal equivalent.

Step 5: Apply RSA algorithm to encrypt this decimal value.

Step 5.1: Select two prime number P,Q; Calculate n=P*Q;; Calculate _(n)= (P-1)*(Q-1); Select integer e; gcd(f(n),e)=1; 1<e<f(n); Calculate d; d=e^-1 mod f(n); Public key KU= {e, n}; Private Key KR= {d, n};

Step 5.2: Encryption Plain text : M< n Cipher Text : C=M^e (mod n);

Step 6: This Decimal value is changed into ASCII character. This is cipher Text.

Step 7: Repeat steps 2 to 5 until all characters of plain text become converted into cipher text.

5 b) Receiver Prospects

6 Decryption

Step 1: Take cipher text and extract ASCII Character Value individual.

Step 2: Change this value into decimal Equivalent.

Step 2.1: Decryption Cipher Text : C Plain Text : M = C^d (mod n);

Step 3: Convert this decimal into bit stream.

Step 4: First Two bit represent X-axis, Second two bit Represent Y-axis and remaining four bit represent grid number. Match bit stream with above process and take the ASCII value.

Step 5: Convert This ASCII Value into Character set.

Step V.

7 Conclusion & future scope

It is observed from the result the proposed algorithm is extremely efficient and a sufficiently strong encryption algorithm enhance the security of data transmitted over covert channel. A degree of freedom value of 256 ensures the maximum variety of characters in the cipher text which ensures its strength against an attack. Frequency Distribution also speaks the encrypted character evenly distributed from 0 to 255. So, it has been made more difficult for attacker to recover plain text from cipher text. This algorithm provide security over data in two ways , Firstly the arrangement of grid is only known by both parties only and secondly the key is used in RSA algorithm is also unpredictable by the intruders. There is some extra effort have made in grid and their storage format then this algorithm give more better result in terms of security and speed of encryption & Decryption.

2

Figure 1: Part 2

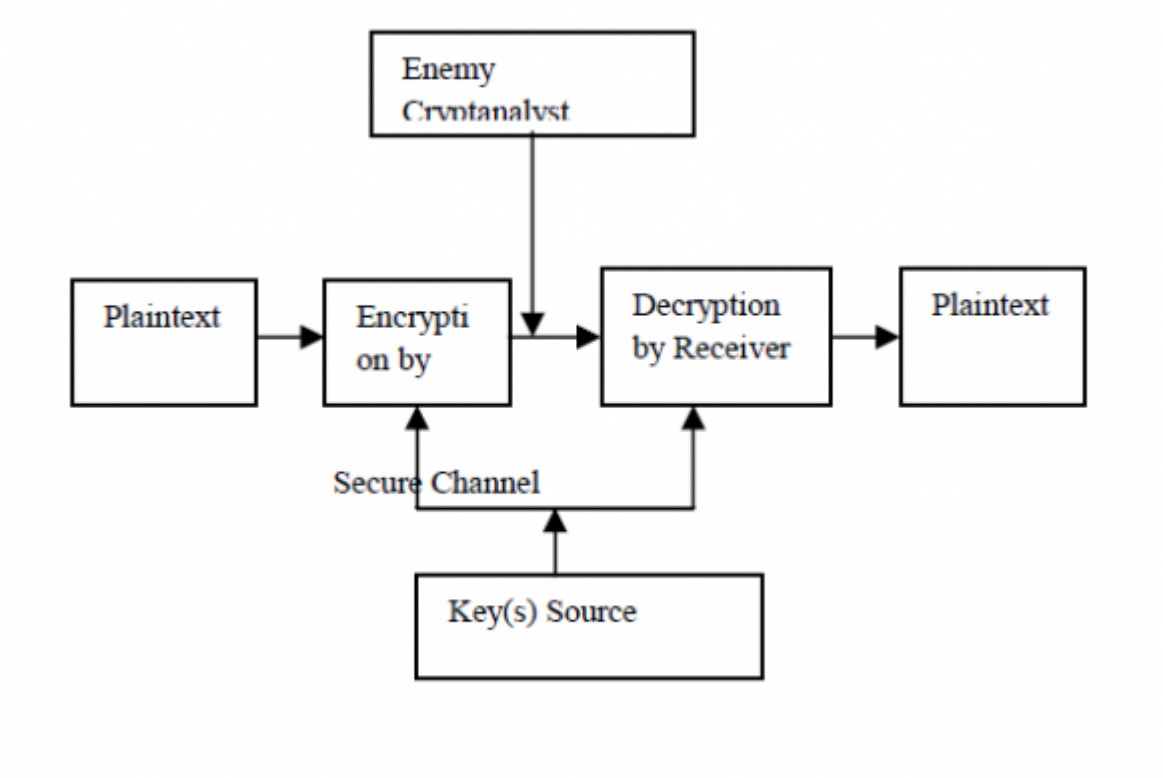

Figure 2:

IV. Result

a) Sender Prospects

Take the word "Crypto" encrypt this with the help of above algorithm.

Plain text	ASCII Value	(X,Y, Grid No)	Bit stream	decimal No
C	67	0,3,3	00110011	
R	114	0,2,6	00100110	
2012Y P T	121 112 116	2,1,6 0,0,6 1,0,6	10010110 00000110	010001
May O	111	3,3,5	11110101	

Apply RSA algorithm to encrypt this decimal value and the resultant cipher text is== 3&–F<õ

b) Receiver Prospects

Sender & Receiver both are well known algorithm & encrypted text is in ASCII Format. Receive the Cipher Text C= 3&–F<õ , Apply RSA algorithm to decrypt the cipher text in Decimal value format.

Decimal Value	Bit Stream	(X, Y, Grid No)	ASCII Value
51	00110011	0,3,3	67
38	00100110	0,2,6	114
150	10010110	2,1,6	121
70	00000110	0,0,6	112
(06 245	01000110 11110101	1,0,6 3,3,5	116
D			111
D			
D			
D			
)			
E			

Figure 3:

[Nalini and Rao] *A New Encryption and Decryption Algorithm Combining the Features of Genetic Algorithms(GA) and Cryptography*, G Nalini , Raghavendra Rao .

[Bowman] John C Bowman . *Math 422 Coding Theory & Cryptography*, (Edmonton, Canada) University of Alberta

[Shannan ()] 'Communication Theory of Security System'. C E Shannan . *Bell, System Technical Journal* 1949. 28 p. .

[Singh and Vatsa] 'Confidentiality & Authentication Mechanism For Bio-Metrics Information transmitted over Low Bandwidth channel'. Raju Singh , A K Vatsa . *International Journal of Network Security & it's Application* 3 p. 3.

[Feistel ()] 'Cryptography and Computer Privacy'. H Feistel . *Scientific American* 1973. 228 (5) p. .

[Uttam Kr Mondal and Mondal ()] 'Frame Based Symmetric Key Cryptography'. Satyendranath Uttam Kr Mondal , Mondal . *Int. J. Advanced Networking and Applications* 2011. p. .

[RSA-2 Algorithm Speed and Security enhancement through public key cryptography International Journal of Engineering Scienc 'RSA-2 Algorithm Speed and Security enhancement through public key cryptography'. *International Journal of Engineering Science & Technology* 2010. 2 (8) p. . (J. SaiGeethaet. al.)