International Journal of Engineering & Technology, *7 (2.33) (2018) 209-211*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An improved novel Hill cipher using RCLT Title of the article

V. Hema [1] *, Dr. M. Ganaga Durga [2]

[1] *Research Scholar, Bharathiar University, Asst. Professor, Dr. MGR Janaki College of Arts and Science for Women, Chennai*
[2] *Research Supervisor, Bharathiar University, Asst.Professor, Department of CS, Govt. Arts College for Women, Sivagangai*
**Corresponding author E-mail: 1vhema23@gmail.com*

Abstract

Security is the only buoyant to the frailest link. In this communication world, the implementation of sturdy cryptographic and integrity checking algorithms is the smart solution to the frailest link. So, the proposed paper provides the new-fangled pattern of cryptographic scheme in concert with Number Theory which safeguard the integrity and confidentiality of intricate data and communications. By using this system, client's burden of security issues associated with the data hosting in the untrusted remote server is abridged. By manipulating some features of the Galois Field, a new method of key generation is proposed. The proposed system is resilient against the various attacks and cannot be understood by the intruders. It is simple yet robust and will surely improve the overall security with higher efficiency.

Keywords: *Key generation; Encryption; Decryption; RNS; CRT.*

1. Introduction

A Hill cipher is a polygraph based cipher which divides the original text into groups of letters of a fixed size and then each group is transformed into a different group of letters [1]. A Hill cipher achieves this transformation by using basic matrix multiplication which provides good diffusion. This linear algebra based technique which represent the groups of letters as vectors such as C = K × P (mod m), where C represents cipher text, K represents key matrix and P represents plaintext respectively. The main hitch of Hill cryptosystem is choosing the key matrix for encipherment. If the encoded key matrix is not properly generated, the decryption key matrix generation is difficult. If the matrix is selected randomly, sometimes it is difficult to obtained correct encryption key matrix using one or two runs. Also there is no deterministic method is available in generating the key matrix. In order avoid these downside, we come up with new algorithm based on the amalgamation of Hill cipher with number theory concept. To strength this proposed algorithm the key matrix using Galois field and the random seed but not randomly.

This offers some advantages such as encryption which resistant towards frequency analysis, high speed and high throughput. This paper provides different flavour to the existing symmetric key substitution Hill Cipher (HC) algorithm by using random lookup table and Galois Field and contributes the following:

- We design an improved version of Novel Hill Cipher technique (NHC) to strength security issues associated with it.
- We extend this algorithm to resist against the known plain text, frequency analysis and other attack on the outsourced data.
- The secure key exchange scheme is proposed using RNS and CRT concept in number theory.
- This system acquires less communication and computational overheads.

The theoretical and experimental analysis shows that our proposed protocol is robust and proficient in terms of the external attacks. The rest of this paper is organized as follows: We introduce the cryptographic techniques and present the description of the new proposed system in section III. In section IV, we present the discussion part. Finally we conclude the whole paper in section V

2. Related works

The susceptibility to cryptanalysis has rendered this system to be unfeasible in practice. But it quiet obliges a vital pedagogical role in cryptology [11]. Several researches offer their innovative thoughts to improve the strength of the core Hill technique. The following are the some of the existing Hill cipher based cryptographic.

Yeh et al. proposed the scheme for encipherment and decipherment which uses two co-prime base numbers. But it is time-consuming task and thwarts towards the known-plaintext attack. Saeednia designed a cipher technique which uses the random permutation key matrix tries for encoding purposes yet it could not handle the known-plaintext attack problem [4]. Alasdair had devised a new version of Hill cipher which uses the ASCII values for its operations but their scheme is not efficient to withstand the attacks. Based on non-invertible matrices, Rushdi and Mousa proposed a new technique in 2009. This system converts each plaintext character into two cipher text characters. This method is time consuming and involves the complex computation.

Ismail et al.[3] proposed MRIV Hill technique which uses one-time-one key matrix method for encipherment. Each block is encrypted by using its own key. The product of current key with a secret Initial Vector (IV) is used as the unique key in this system. This algorithm offers a better security compared to others.

Rangel-Romero proposed cipher algorithm which is vulnerable towards known-plaintext attack. Besides, Ismail et al. (2006) does not tackle the non-invertible key matrix problems which may lead to failure in decryption. Bibhudendra also proposed an advanced algorithm which solves the non-invertible key matrix problem exist in Ismail et.

2.1. Seed based key matrix

A random seed (ℜ) is a prime number used for symmetric key generation. In traditional techniques, decipherment requires the inverse of a key matrix for its operation. Inverse matrix calculation requires more computational overheads. Without the inversion, the encrypted text cannot be decrypted. In order to solve this problem, this new type of key matrix generation is proposed and encipherment is performed based on this key matrix. The random number ℜ is shared with the receiver, but it send as a residue using Residue Number System. The Receiver uses the Chinese Remainder Theorem (CRT) to extract the number and generated the key matrix to decrypt it.

2.2. Random char lookup tab (RCLT)

The grid allows the user to translate the characters into numerals. A grid can be randomized using a pseudo random alphanumeric string (δ) which gives a small level of encryption and can be shared with the recipient. The coordinates are converted into a vector of numbers and then it is dotted with the matrix M.

The coordinates for each letter of the plaintext is found and used. The alphabet tab consists of the 26 upper-case alphabet followed by the period (.), the asterisk (*), and the blank space (#) etc. The encryption or decryption is performed using the 87 characters generated randomly based on the string δ as shown in Table 2. The coordinates are converted into a vector of numbers and then it is dotted with the matrix M .

Table 1: Numerical Representation of 87-Letter CLT

1	2	3	4	5	6	7	8	9	10	11
I	C	E	r	a	m	1	2	3	b	d
12	13	14	15	16	17	18	19	20	21	22
F	G	H	j	k	L	n	o	p	q	S
23	24	25	26	27	28	29	30	31	32	33
T	U	v	w	x	Y	z	4	5	6	7
34	35	36	37	38	39	40	41	42	43	44
8	9	0	+	-	*	/	$	@	&	%
45	46	47	48	49	50	51	52	53	54	55
!	#	blk	,	.	;	:	“	?	A	B
56	57	58	59	60	61	62	63	64	65	66
D	E	F	G	H	I	J	K	L	M	N
67	68	69	70	71	72	73	74	75	76	77
O	P	Q	R	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	
!	^	_	‘	(	)	[	]	{	}	

2.3. Galois field

A Galois field is also often known as a finite field, is an algebraic object with two operation represented by + and *. It is convenient for cryptographic applications to scramble and descramble the data. The most popular and widely used application of GF is in cryptography. Since each byte of data is represented as a vector in a finite field, encryption and decryption using mathematical arithmetic is very straightforward and is easily computable. The elements in the field can take η different values is referred to as GF (η).It is computed based on the size of the block using generator. A finite field exists if and only if it has size Pm, where p is prime and mε N.

2.4. Residue number system (RNS)

A RNS is defined by a vector of K moduli (i.e) (m1, m2….mk). The moduli must be pairwise co-prime, which means that, any pair of moduli, the only common factor is 1. In a RNS, each operand is represented by a list of its residues. For any given integer x,

$$x= (x1|x2|...|xk) \text{ RNS } (P1|P2|...|Pk) \qquad (2)$$

Where xi = x mod Pi and ∀ i,j Pi is relatively prime to Pj

3. Proposed scheme

We devise a new algorithm called INHC using RCLT. This is capable of enciphering the sensitive data by the sender before transmission to the cloud and deciphering the disguised data by the receiver after transmission through the cloud. In this proposed algorithm, each character in the plain text is taken and their corresponding character code is obtained from look up table. Each character is then converted into corresponding non-negative integers using RCLT. A block of m letters is then considered as a number vector of n dimensions. The key matrix of size m × m is generated in which m is the size of the block using GF. Then, the summation of key matrix and each column vector is obtained. Then perform in-place rotation about 90 degree in order to strength the security. The encipherment and decipherment is done by means of several phases which is discussed below. This technique makes use of a secure key contract scheme which allows the sharing of information through the unsecure channel.

3.1. Notations and preliminaries

In this sub section, we list some notations and schemes used in the proposed system.

Table 2: Notations Used in This Scheme

δ	a pseudo random alphanumeric string
M	Message matrix
κ	Key Matrix
ω	Check sum code
η	Length of alphanumeric string
ℜ	Random number
fbi	Finite ordered set of file blocks
Len	Length of the file blocks
GF(n)	Galois Field
X	Modulus

3.2. Encipherment technique

The technology behind this cryptosystem includes the substitution cipher based on the Random Char Lookup Tab (RCLT) tableau generated randomly based on δ. The grid allows the user to translate the characters into numerals. A grid can be randomized using a pseudo random alphanumeric string (δ) which gives a small level of encryption and can be shared with the recipient. The message matrix and key matrix is obtained based on the scheme mentioned below. The encryption scheme performed using Message matrix (M), Key Matrix Key Matrix (κ) and In-place transpose (υ). The enciphering and deciphering is given by

$$\gamma: M + \kappa \rightarrow \upsilon(C) \qquad (1)$$

$$\psi: C + \kappa \rightarrow \upsilon(M) \qquad (2)$$

Where γ denotes the ciphering and ψ denotes the deciphering

3.3. Key generation scheme

A new type of key matrix generated based on random seed ℜ used for both encryption and decryption. The Galois field is generated using generator based on the order of the matrix then the key matrix κ generated as follows:

$$\kappa_{11} =(\Re * \varepsilon\,(1, 1\,)\,) \bmod x \;\; \kappa_{12} = (\Re * \varepsilon\,(1, 2\,)\,) \bmod x \;\; \kappa_{13} = (\Re * \varepsilon\,(1, 3\,)\,) \bmod x \qquad (3)$$

Where ε (i, j) is the elements in the Galois Field of order M.

This technique of key generation avoids cost effective matrix inverse operation for decryption purposes. This key generation scheme is proposed to enhance the security of information stored in untrusted server and provides the shield against the various attacks.

3.4. Key exchange scheme

The sender and receiver agree with the initial inputs $\Re$ used for key matrix construction. The residue of $\Re$ is calculated using Residue Number System (RNS) which send to the receiver for key generation. The residue is generated as follows:

$$n= (n_1|n_2|...|n_k) \text{ RNS } (P_1|P_2|...|P_k) \quad (4)$$

Where ni = n mod Pi and $\forall$ i,j Pi is relatively prime to Pj
The residue is converted into original seed $\Re$ by the receiver using the Chinese Remainder Theorem (CRT) for decryption purposes. CRT is given by:

$$\Re= \sum_{i=1}^{n} \text{Ai * Ti * ri mod M.} \quad (5)$$

3.5. Construction of the proposed scheme

The proposed system consists of following phases which is used by the user to ensure integrity and confidentiality of out sourced data. The phases are
Phase 1: Preliminary Phase
In this phase, the random string □ is obtained for RCLT generation. The checksum code is calculated and appended with the string send to the recipient. Galois field GF (□) is initiated and generated. Choose the moduli required for RNS and CRT system.
Phase 2: Key Generation Phase
The symmetric key is generated based on the seed and the GF using equ. (3). the key is securely exchanged using the RNS and CRT scheme.
Phase 3: Block Generation Phase.
The file f is divided into finite ordered set of β blocks (i.e.) f= {fb1, fb 2…fbβ } where $1 \leq i \leq \beta$. Encrypt the file blocks using IRCLT based cipher techniques.
Phase 4: Enc & Dec Phase
Translate the sensitive information into secure core by means of the following steps.

- Perform the summation of message or cipher matrix and key matrix.
- The resulted matrix is rotated in-place by 90 degree

4. Result and discussions

The proposed cryptosystem utilizes the random lookup table, random seed based key generation and number theory concept is used to heal the security downside in the existing algorithms and it can be implemented by the use of a simple cryptographic protocol without compounding any additional computational costs.
The encryption process will be performed for a $n \times n$ block of data and it contains fewer number of operations which leads to lower computational costs. All the known attacks to Hill Cipher including zero-plaintext attack can be thwarted by means of the proposed cryptosystem. Comparison has been done between the proposed encryption algorithms and previous Hill algorithms. Obviously, this proposed scheme does not require calculation of the inverse key matrix for decryption process. The time complexity of matrix multiplication O (n3) is greatly reduced using this scheme. The amalgamation of cryptographic technique with number theory provides resilient against the various attacks. This modified algorithm which improve more strength to existing one by avoiding unsecure transfer of information through unsecure channel. In this system, only some random values are transferred to the receiver in the coded form. Based on this information, key matrix as well as original text is obtained.

5. Conclusion

We have proposed an enhanced version of Hill cipher which is an extension of core Hill cipher. We introduce a random matrix key which is computed based on the pseudo random technique. This significantly increased the resistance of the algorithm to the known plaintext attack. This offers a better encryption quality compared to the original Hill cipher and other. The proposed cryptosystem thwarts the various attacks such as known-plaintext, chosen cipher text, and chosen-plaintext attacks.

References

[1] L.S. Hill, “Cryptography in an Algebraic Alphabet,” American Mathematical Monthly, Vol.36, No.6, pp.306- 312, 1929.

[2] I.A. Ismail, M. Amin, and H. Diab, “How to repair the Hill cipher,” Journal of Zhejiang University-Science A, Vol.7, No. 12, pp.2022-2030, Dec. 2006.

[3] S. Saeednia, “How to Make the Hill Cipher Secure,” Cryptologia Journal, Vol.24, No.4, pp.353-360, Oct. 2000.

[4] J. Overbey, W. Traves, and J. Wojdylo, “On the Keyspace of the Hill Cipher,” Cryptologia Journal, Vol.29, No.1, p.59–72, 2005.

[5] K.H. Rosen, “Elementary Number Theory and Its Applications,” 2nd Edition, Addison-Wesley, 1988.

[6] D.E. Knuth, “The Art of Computer Programming,” Vol.2, Addison-Wesley, 1981.

[7] Secure Hill cipher modifications and key exchange protocol ,Mahmoud, Ahmed Y.; Chefranov, Alexander G.; Automation Quality and Testing Robotics (AQTR), 2010 IEEE International Conference on Volume: 2 Digital Object Identifier.

[8] A secure variant of the Hill Cipher, Toorani, M.; Falahati, A.; on, Digital Object Identifier: 10.1109/ISCC.2009.5202241, Publication Year: 2009.

[9] Invertible, Involutory and Permutation Matrix Generation Methods for Hill Cipher System ,Acharya, B.; Jena, D.; Patra, S.K.; Panda, G.; Advanced Computer Control, 2009. ICACC '09. International Conference on, Digital Object Identifier: Publication Year: 2009. 6.

[10] Prof. A.V.N.Krishna, K.Madhuravani, “A Modified Hill Cipher using Randomized Approach”, I. J. Computer Network and Information Security, June 2012.

[11] B. Karthikeyan, Jagannathan Chakravarthy, Ramasubramanian S, “Amalgamation of Scanning paths and Modified Hill Cipher for Secure Steganography”, Australian Journal of Basic and Applied Sciences, Volume 6(7), 2012.

[12] Rahul. R. Ravan, Atul R. Nigavekar, “Secured Data Communication using Novel Modification to Hill Cipher Algorithm with Self Repetitive Matrix”, International Journal of Science and Research (IJSR), Volume 2, Issue 4, April 2013.