ISSN 2278-3091
Volume 8, No.5, September - October 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse96852019.pdf
https://doi.org/10.30534/ijatcse/2019/96852019

Information Security Using Hilbert With Hash Value

Koduru Prasada Rao[1] , Dr G Lavanya Devi [2]
[1] Research Scholar , Department of CS&SE, AU College of Engineering(A), Andhra University, Visakhapatnam, India, kpraomtech@gmail.com
[2]Assistant Professor, Department of CS&SE , AU College of Engineering(A), Andhra University ,Visakhapatnam, India lavanyadevig@yahoo.co.in

ABSTRACT

The vast growth of technology the speed of data transfer are increased. During data transmission through internet the data are prone to vulnerabilities. Intruders may gain access and modify the data. Cryptology is a science of securing data. So we propose a security approach is Hilbert with hash value. This future is confusing the intruders and generate a variety of cipher texts with hash value to the same plain text. We illustrate the range of property differ by algorithm such as RSA and show cryptanalysis of projected algorithm by resist a range of attacks and stronger than exist algorithms.

Key words : Cryptology, Hash value, Hilbert , RSA

1.INTRODUCTION

The world is small because of today' s technology and playing important role in globalization of nations when communication taking place among people of one nation to the other nation as well as people in the society by using internet. In this connection there is major aspect to effect the security problems of information when communication. Now the life of humans is linking with the electronics documents/transactions in every activity or most of the activities such as electricity bill, withdraw money or deposit money etc. Lot of security aspects are considered when data is transformed through electronic media is a big challenge. Confidentiality, authentication, integrity and non repudiations are the security services for the information [1]. Even many approaches for security are used for protecting their information from attackers. Due to the assailability, the attackers are breaking the security services when data is sending as an electronic document. The electronic transactions are protected by all security services i.e. to protect from hackers all security services must be satisfied. For increasing the security of communication by signing, encrypting, decrypting the document and send the information document [1]. When encryption and decryption keys are equal called symmetric cryptosystem [2] otherwise encryption and decryption keys are not equal called asymmetric cryptosystem [1]. The common components of security mechanism are plaintext ,cipher text, key ,encryption algorithm or decryption algorithm or both encryption algorithm and decryption algorithm. In symmetric cryptosystem the operations are performed on the intelligible message using the key1 in the sender side and same key1 is used in receiver side for decrypting the intelligible communication. In asymmetric cryptosystem the operations are performed for transforming the intelligible message into unintelligible message using the key1 in sender side and in receiver side for transforming the unintelligible message into intelligible message use different key2.The unintelligible message which is called as Cipher Text(CT) depends on the key used and intelligible message. Decryption algorithm produces the intelligible message by the key2. The properties of Hilbert matrix [3], the prime numbers are used for proposing many encryption algorithms based on symmetric and positive [4]. Many of asymmetric algorithms proposed by using the keys such as private and public keys but very few proposed using fractions/ bits [7]-[8]-[9] and linear algebra [10] . Here fractions are used instead of bits. The encryption algorithm [10] is vulnerable to all four attacks and some of symmetric encryption algorithm like blowfish [11], IDEA [12] & asymmetric encryption algorithm like RSA [13] is not opposed to all attacks. But the proposed asymmetric algorithm is opposed to to all attacks [14]. A security approach is proposed using Hilbert[18]. The asymmetric key cryptographic algorithm RSA has the time complexity constant i.e O(k4) [5]. In linear algebra which is initiated by considering '1' and took the fractional units for forming the needed matrix is called the Hilbert matrix. For iteration of this process smaller matrix 3x3 order. Here for identifying the Hilbert matrix by the order mxm which is the based on the size of intelligible message. The entities of the matrix as follows $H_{ij}=1/i+j-1$. This matrix is used by sender side by selecting randomly because the size of matrix is depending on the size of intelligible message by increasing the key1 will become more complex. For practical applications m is restricted and by multiplying the Hilbert matrix with intelligible message to get the unintelligible message as CT [18]. Then the jumbled message in converted into intelligible message by inverse Hilbert matrix [18]. The time complexity of generated key is not constant because key size is depending on the size of the Hilbert matrix [19].

2. SECURITY APPROACH USING HILBERT WITH HASH VALUE

The proposed method consists of hash value append into the sender side algorithm. Hashing creates a unique fixed length signature of group of data. Hashes are created with an algorithm such as message digest or secure hash algorithm.

Here SHA-1 algorithm which is 160 bit key produces 128 bit hash value. This value is appended into the cipher text which is generated by the Hilbert Matrix, then we get the sender side cipher text hash value (CTHV). In the receiver side the hash value is decrypted , when decryption of hash value(HV) both the values are same and cipher text in receiver side decrypted by using the inverse of Hilbert Matrix. The proposed method had shown in below diagram (figure 1) along with case study.

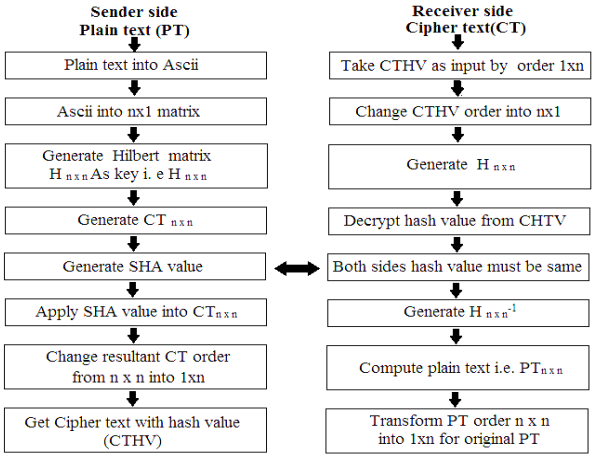


Figure 1: Hilbert with Hash value

A.Case Study

Plain text**:** rama
Plain text in ASCII codes: 114 97 109 97
Key: The order of key size is depending on the plain text size, if plain text size is n then the size of key is n x n, for practical point of view here order of key considered as 4 x 4 which is shown below

$$\begin{bmatrix} 1 & 1/2 & 1/3 & 1/4 \\ 1/2 & 1/3 & 1/4 & 1/5 \\ 1/3 & 1/4 & 1/5 & 1/6 \\ 1/4 & 1/5 & 1/6 & 1/7 \end{bmatrix}$$

4X4

By multiplying plain text and key we get the below cipher text (CT)
CT: r9&La0↑m6$←a0 ↑
Generating the Hash value such as: Applying this hash value into cipher text we get cipher text with hash value(CTHV): r9&La0 ↑m6$←a0 ↑V7372696E69766173.

Algorithm1 Algorithm for Encryption
Input: Plain Text (PT)
Output: Cipher text with hash value(CTHV)

1 Consider Plain Text(PT)
2 PT is converted into ASCII Codes
3 Convert ASCII Codes into n x 1 matrix i.e. $PT_{n x1}$
4 choose the secret key e1 in n x n based on Hilbert Matrix i.e. $H_{n x n}$ where the order depending upon plain text
5 Generate the cipher text (CT) by using
$CT_{n x n} = PT_{n x 1} X H_{n x n}$
6 Generate SHA value using SHA algorithm
7 Apply SHA value into the Cipher text (CT)
8 Convert resultant matrix cipher text with hash value (CTHV) order from n x n → 1 x n

Algorithm2 Algorithm for Decryption
Input : Cipher text with hash value (CTHV)
Output: Plain Text (PT)

1 Consider CTHV as input of by order 1 x n
2 Convert CTHV into n x 1 matrix
3 Consider Hilbert Matrix i.e. $H_{n x n}$ where n is the size of cipher text
4 Decrypt the hash value from cipher text with hash value (CTHV)
5 Both sides i.e. sender and receiver sides hash value must be the same then we have the $CT_{1 x n}$
6 Calculate $H_{n x n}^{-1}$ from $H_{n x n}$ by using any linear algebra
7 Compute $PT_{n x n}=CT_{1 x n}X(H_{n xn})^{-1}$
8 Transform PT order form n x n → 1 x n to get original text

The Equations are shown

$$H_{i,j} = i + j - 1 \quad (1) \qquad (1)$$

Where i , j > 1

$$CT_{n x n} = PT_{n x 1} X H_{n x n} \qquad (2)$$

PT=[114 97 109 97] is multiplied by the hilbert matrix of H_{4x4}

$$\begin{bmatrix} 1 & 1/2 & 1/3 & 1/4 \\ 1/2 & 1/3 & 1/4 & 1/5 \\ 1/3 & 1/4 & 1/5 & 1/6 \\ 1/4 & 1/5 & 1/6 & 1/7 \end{bmatrix}$$

$CT_{1 x 4} \leftarrow CT_{4 x 4}$ (3)
$CT_{1 x 4} \leftarrow$ Hash value (4)

Equation (2) generates the cipher text in 4 x 1 order, and in the above matrices , the plain text is arranged as 114,97,109,97 & the matrix elements by order 4 x 1 along with the generated secret key encryption key as e1 i.e. Hilbert matrix of unit fractions of linear algebra as shown above equation(2). Here the elements of unit fractions of Hilbert matrix is 1,1/2,1/3,1/4,1/5,1/6,1/7 by the order 4 x 4 . The resultant matrix of equation (2) is the cipher text (CT) which is in the

order of 4x4. Alter the resultant matrix I. e cipher text (CT) in the jumbled message format by the order of 1 x 4 as shown in the equation (3) i.e. r9 & La0 ↑m6$←a0↑7372696E69766173. Equation (4) the hash value is added into cipher text (CT) using any one SHA algorithm then we get cipher text with hash value (CTHV).

$$CT_{n\,x\,1} \leftarrow CT_{1\,x\,n} \quad (5)$$

$$\text{Hash value} \leftarrow CT_{n\,x\,1} \quad (6)$$

$$PT_{n\,x\,n} \leftarrow CT_{n\,x\,1} \; X \; H_{n\,x\,n}^{-1} \quad (7)$$

Here n is considered as 4. Equation 5 says that the cipher text which in the order 1 x 4 is converting into the order 4 x 1. Equation 6 says that decrypting the hash value from the cipher text. For getting the plain text in equation 7 cipher text which is in the order 4 x 1 is multiplied by the inverse Hilbert matrix which is the another secret key e2 as $H_{4\,x\,4}^{-1}$. Here two different keys are used in the both sides e1 & e2 which are two private keys but asymmetric.

3. CRYPTANALYSIS

We Consider crypto algorithms these algorithms are represented in the algebraic form for solving these algebraic for recovering the secret key is called Cryptanalysis or The measurement of attacks proved using the characteristics of algorithm design to interpret PT or secret keys is called cryptanalysis.

3.1. Degree of difference Cryptanalysis

The proposed algorithm uses two different keys one key for encryption and another key for decryption. Both sides' i.e. encryption and decryption uses different keys so it is difficult for breaking keys of sender and receiver side. The generation of key by RSA algorithm is constant i.e. O [k^4] [5]. But the generation of key using proposed algorithm is not a constant. If the hackers hack any one of key the data is not retrieved by hacker without knowing about another key because in this paper used two private asymmetric keys. This property will satisfy Zero Knowledge Protocol [6]. The degree of differential is nothing but degree of difference. The properties of Encryption algorithm are shown below table 1.

.

Table 1: Degree of difference Cryptanalysis

Property	RSA	Hilbert
Generation of key of Time Complexity	It is constant $O(k^4)$[5]	It is not constant (dependent on key size)
Third party required for transmission of key	Yes	Yes
If any one of the key broken then hacker can hack the data	Yes	It is very complex because two different keys are used both sides
Asymmetric Key	Yes	Yes
Both private, public keys are used or any one key is used	Both	Private keys but asymmetric
Which one satisfies Zero Knowledge protocol?	No	Yes

3.2. Chosen plain text / Cipher text attack

This is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of cipher texts. Prior to encryption the attacker has no channel for providing access to plain text. In all practical cipher text –only attacks, the attacker still has some knowledge of the plain text [15]. Assume that the size of plain or cipher text is N-bytes then it produces the N X N_{PN} various types of cipher / plain texts. For example if we select cipher text / plain text of size 160 bytes that it produces 160 x 160_{P160} various types of cipher / plain text. In addition to this the cipher text added the hash value and for assuming the hash value from the cipher text is difficult for attacker.

3.3 . Known plain text attack

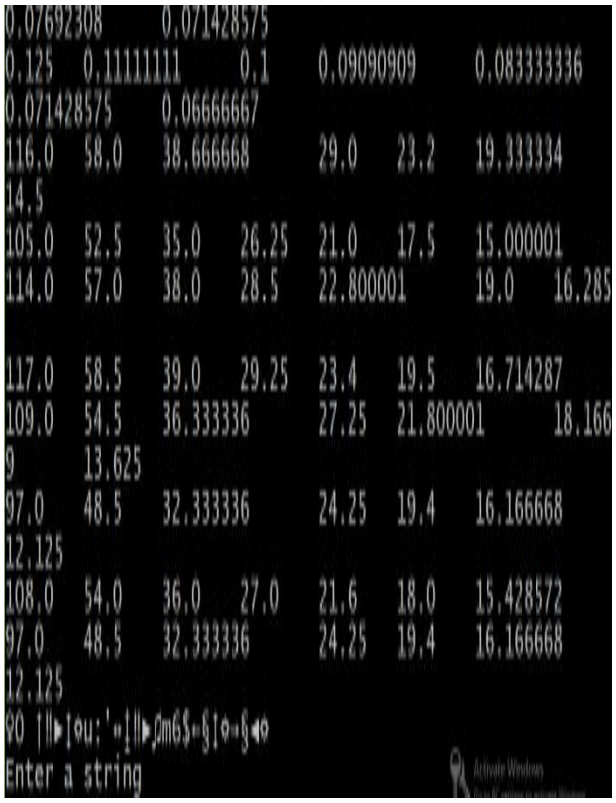
The hacker will have the knowledge about cipher text and one plain text –cipher text pair for attacking the plain text and encryption algorithm [16]. Assume size of plain text is 160 bits then 160 * 160_{P160} number of attempts required. Even if these many attempts made that it is difficult for breaking the hash value.

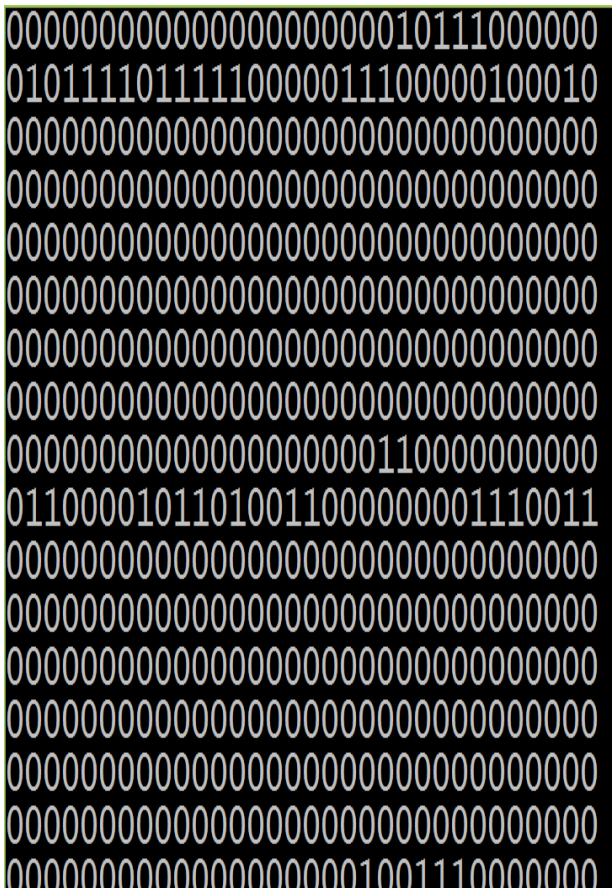
3.4. Cipher text only attack

The cryptologist can understand the encoding formula and cipher text should be decoded within the cipher text attack [15]. Suppose if the plain text size is 64 bits then the range of bits within the secret secret's(key) is 128 bits i.e. the chance of secret's $1/2^{128}$ and hence range of makes an attempt should be created for locating the secret's 2^{128}. Additionally the cipher is enclosed with the hash value so breaking the hash value is difficult.

4. CONCLUSION and RESULTS

In this paper a new algorithm developed by exploitation properties of David Hilbert and Henkel matrix. This algorithmic program needs to be enforced within the traffic management, domestic security and strengthen the zero knowledge protocol etc... The results of this algorithm are shown below.





5. FUTURE SCOPE

Further work will be extended and developing this expected methodology into Zero Knowledge protocol [6]. ZK protocols [7] prevail over main concern wide used password based authentication. The ZK protocol can be strengthened by using the above proposed asymmetric algorithm.

6. REFERENCES

[1] Ch. Rupa et. al, "**Fast Comparison Encryption Scheme using cheating text technique"** International Journal of Engineering Science and Technology, Vol. 2 (6) , pp. 1725-1728, 2010.

[2]David Point cheval: "**symmetric cryptography and practical security"** Journal of Teleommunication & Information Technology, pp. 42- 56, 2002.

[3] Y Matsuo, : "**Matrix Theory, Hilbert Scheme and Integrable System**". Arxiv: hep-th /9807085, arxiv. org, 1998.

[4]Jerry crow,: "**Prime numbers in Public Key Cryptography"**, SANS Institute InfoSec Reading Room, pp. 1 – 18 , 2003.

[5] Ren- Junn Hwang. et. al: "**An Efficient Decryption method for RSA System"**, IEEE- AINA, 2005.

[6] Feigenbaum, J.:" **Overview of Interactive Proof Systems and Zero-Knowledge"**, IEEE- Contemporary Cryptology, pp. 423-440 , 1992.

[7] T.Arumuga Maria Devi,: "**Analysis of Error metrics Different Levels of compression on modified Haar wavelet Transform**, Int. Journal of Comp. Science and Inf. Security. vol. 9, No.1, pp. 127-133 , 2011.

[8] Lianqing Zhao,:" **Error Diffusion Algorithm Based on Hilbert Matrix and Image Content",** Proceedings of 2010 Asia-Pacific Youth Conference on Communication (APYCC 2010 E-BOOK). pp. 192-196 , 2010.

[9] Xinjie Li, Gong sheng Li: "**A Note on Solving High-order Hilbert Matrix Equation by Tikhonov Regularization"**, Journal of Information & Computational Science. pp. 1957– 1966, 2012.

[10] JhansiRani, Durga Bhavani,: "**Symmetric Encryption Using Sierpinski Fractal Geometry"**, ICIP Springer- Verlag Berlin Heidelberg,pp.240-245, 2011.
https://doi.org/10.1007/978-3-642-22786-8_30

[11] B. Schneier**,:** "**Description of a New Variable- Length Key, 64-Bit Block. Cipher (Blowfish), Fast Software Encryption**," Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, pp. 191-204, 1994.
https://doi.org/10.1007/3-540-58108-1_24

[12] Allen Michalski,: "**An Implementation Comparison of an IDEA Encryption Cryptosystem on Two General – Purpose Reconfigurable Computers".** 13th Int. Conf on Field Programmable Logic ad Applications, FPL 03, 2003.
https://doi.org/10.1007/978-3-540-45234-8_21

[13] Ming-Der Shieh, Jun-Hong Chen, Hao-Hsuan Wu and Wen -Ching Lin, : "**A New Modular Exponentiation Architecture for Efficient Design of RSA Cryptosystem"**, IEEE Transactions, Vol. 16, No. 9, pp. 1151-1162, 2008.
https://doi.org/10.1109/TVLSI.2008.2000524

[14] Rubesh Anand, P.M., Bajpai, G., Bhaskar, V.: "**Real-Time Symmetric cryptography using Quaternion Julia Set"**, International Journal of Computer Science and network Security 9(3) , 20-26, 2009.

[15] Alex Biryukov . et. al: "**From different Cryptanalysis to Cipher text attacks".** CRYPTO – LINCS 462. pp.72-88.1988.
https://doi.org/10.1007/BFb0055721

[16] Mitsur Matsui, et. al,: "**A New Method for Known Plaintext attack of FEAL Cipher",**Springer – Verlag, pp. 81 -91 (1998).
https://doi.org/10.1007/3-540-47555-9_7

[17] Coppersmith. D,:"**The data Encryption standard (DES) and its strength against attacks",** URL://research.ibm.com/journal rd/383/coppersmith.pdf.

[18] K.Prasada Rao , Dr Ch Rupa " **A novel security approach in the information and communication with ryptanalysis",**doi:1109 /ICHI-IEEE.2013.6887767 published in IEEE explore on 2014,INSPEC Accession Number:14562992.

[19] Koduru Prasada Rao, Dr G Lavanya Devi , K Srinivasa Rao " **Zero Knowledge Protocol Using Hilbert Unit Fractions** " International Journal of Engineering, Applied and Management Sciences Paradigms IJEAM) Volume 54 Issue 1 April 2019 pages 070 to 073 ISSN 2320-6608.