I. J. Computer Network and Information Security, 2012, 5, 56-62
Published Online June 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.05.07

A Modified Hill Cipher using Randomized Approach

Prof. A.V.N.Krishna, Principal, PJMS CET, hari_avn@rediffmail.com
K.Madhuravani, Research Scholar, PJMS CET, kokk_madhu28@rediffmail.com

***Abstract* —** In Hill Cipher, the plain text is divided into equal sized blocks. The blocks are encrypted one at a time. Cipher text only Crypto analysis of Hill Cipher is difficult. But it is susceptible to known plain text attack. In this work, Hill Cipher is improvised to make it more secure. The output of hill cipher is randomized to generate multiple cipher texts for one plain text. Any one cipher text is used for transmission of data. This approach thwarts any known plain text attacks and also chosen cipher text attacks.

Index Terms— Cipher text, Hill cipher, Known plain text, Randomized Approach, Security analysis

I. INTRODUCTION

Historically, encryption schemes were the first central area of interest in cryptography. They deal with providing means to enable private communication over an insecure channel. A sender wishes to transmit information to a receiver over an insecure channel that is a channel which may be tapped by an adversary. Thus, the information to be communicated, which we call the plaintext, must be transformed (encrypted)to a cipher text, a form not legible by anybody other than the intended receiver. The latter must be given some way to decrypt the cipher text, i.e. retrieve the original message, while this must not be possible for an adversary. This is where keys come into play; the receiver is considered to have a key at his disposal, enabling him to recover the actual message, a fact that distinguishes him from any adversary. An encryption scheme consists of three algorithms: The encryption algorithm transforms plaintexts into cipher texts while the decryption algorithm converts cipher texts back into plaintexts. A third algorithm, called the key generator, creates pairs of keys: an encryption key, input to the encryption algorithm, and a related decryption key needed to decrypt. The encryption key relates encryptions to the decryption key. The key generator is considered to be a probabilistic algorithm, which prevents an adversary from simply running the key generator to get the decryption key for an intercepted message. The following concept is crucial to probabilistic cryptography. The Hill cipher algorithm [2, 3] is a polygraphic cipher algorithm based on linear transformation, and is invented by Lester S.Hill in 1929. Hill cipher is a block cipher algorithm where plaintext is divided into equal size blocks. In a Hill cipher, the key is a non-singular matrix of size n x n in which n is the size of the block. The plaintext P is encrypted as C = KP mod m in which C is the cipher text block and K is key matrix. The key matrix in the Hill cipher needs to have a multiplicative inverse. The decryption of cipher text C produces. Plaintext as P = K^{-1}C mod m such that gcd (det (K) mod m, m) =1. Cipher text only crypto analysis of Hill cipher is difficult. First a brute force attack on Hill cipher is difficult because the key is a n*n matrix. Each entry in the matrix can have one of the 26 values. At a glance, thisa means that the size of key domain is 26^{n*n} . Hill Cipher is no longer used due to the vulnerability against known-plaintext attack. It still serves an important pedagogical role in cryptology and

linear algebra. Hill Cipher has resistant towards frequency analysis, high speed and high throughput With probabilistic encryption algorithms [4, 5], a crypto analyst can no longer encrypt random plain texts looking for correct cipher text. Since multiple cipher texts will be developed for one plain text, even if he decrypts the message to plain text, he does not know how far he had guessed the message correctly. To illustrate, assume a crypto analyst has a certain cipher text ci. Even if he guesses message correctly, when he encrypts message the result will be completely different cj. He cannot compare ci and cj and so cannot know that he has guessed the message correctly. Under this scheme, different cipher texts will be formed for one plain text. Also the cipher text will always be larger than plain text. This develops the concept of multiple cipher texts for one plain text. This concept makes crypto analysis difficult to apply on plain text and cipher text pairs.

II. LITERATURE SURVEY

Several researches have been done to improve the security of Hill cipher. Yi-Shiung Yeh [15] presented a new polygraph substitution algorithm based different bases. Their algorithm uses two co-prime base numbers that are securely shared between the participants. Although their algorithm thwarts the known-plaintext attack, requires many mathematical manipulations. It is time consuming and is not efficient for dealing bulk data. Sadeenia [13] tried to make Hill cipher secure by using dynamic key matrix obtained by random permutations of columns and rows of the master key matrix and transfers an encrypted plaintext and encrypted permutation vector to the receiving side. The numbers of dynamic keys are generated n! Where n refers the size of the key matrix. Each plaintext is encrypted by a new key matrix that prevents the known-plaintext attack on the plaintext but it is vulnerable to known-plaintext attack on permutation vector, the same vulnerability of original Hill cipher. [7] proposed a modification to [13] that works similar to Hill cipher permutation method, but it does not transfer permutation vector, instead both sides use a pseudo-random permutation generator, and only the number of the necessary permutation is transferred to the receiver. The number of dynamic keys is the same as [13]. Ismail [6] tried to improve the security of Hill cipher by introduction of an initial vector that multiplies each row of the current key matrix to produce the corresponding key of each block but it has several inherent security problems. Lin Ch [10] claimed that taking random numbers and using one-way hash function thwarts the known-plaintext attack to the Hill cipher but their scheme is vulnerable to choosen-ciphertext attack. Mohsen Toorani [11,12] proposed a symmetric cryptosystem based on affine transformation. It uses one random number and generates other random numbers recursively using HMAC in chain. Ahmed Y Mahmoud [15] proposed a modification to Hill cipher based on Eigen values HCM-EE. The HCM-EE generates dynamic encryption key matrix by exponentiation with the help of Eigen values but it is time consuming. The paper[1] proposes a modification to the Hill cipher based on circulant matrices. In works [7,8], the Author discusses the idea of randomization of cipher texts to thwart Chosen cipher text attacks. In the present work an attempt is made to provide randomization to the output of Hill Cipher to make it free from chosen plain text and Cipher text attacks.

III. METHODOLOGY OF PROPOSED WORK

This work is broadly divided into

a) Generating the initial cipher text from plain text using Hill cipher.

b) Consider a session key using circulant matrix and converting it into matrix to match the dimensions of Quanary vector.

c) Generating basins by multiplying Quanary vector with circulant matrix and considering a mod n on the output.

d) Mapping basins on the output of Hill cipher to generate multiple cipher texts for one plain text.

Consider the plain text, PT such that

[KA] * [PT] *[KB-1] mod n = Cipher text generated

Consider KA, KA-1 as private and public keys of A, KB, KB-1 as private and public keys of B. and KS as session key to be shared securely among participants A & B. n is a large prime number considered to avoid any crypto analytical attacks on it.

Rather transferring the generated Cipher text directly it is converted to multiple Cipher texts. For it, the algorithm uses a Session Key (KS) which is to be shared between A & B. To provide for secured sharing of session key KS, it is multiplied with KB-1 to get Ksc.

$$| KS| * | KB-1| = KSc.$$

At B, Ksc is multiplied with KB to get back Ks

$$| KSC| * | KB| = KS$$

$$| KS| * | KB-1| = KSc.$$

At B, Ksc is multiplied with KB to get back Ks

$$| KSC| * | KB| = KS$$

A Quinary vector is considered as Global parameter. The Quinary vector is multiplied with Session key, KS to generate a sequence. The sequence is divided into basins equal to number of characters of alphabet considered. For example we are considering 26 characters of English language. The sequence is divided into 26 basins, each characters of English language is mapped to random value from corresponding basin values. Thus multiple Cipher texts will be formed for each output from Hill Cipher.

IV. EXAMPLE

1. A Quinary Vector is considered which is a global parameter **.**

'n' considered =29 (prime number).

$$K_A = \begin{vmatrix} 5 & 7 & 10 \\ 13 & 17 & 7 \\ 0 & 5 & 4 \end{vmatrix} \qquad K_A^{-1} = \begin{vmatrix} 21 & 14 & 1 \\ 0 & 8 & 25 \\ 13 & 3 & 8 \end{vmatrix}$$

$$K_B = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix} \qquad K_B^{-1} = \begin{vmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{vmatrix}$$

Consider

$$K_S = \begin{vmatrix} 17 & 5 & 5 \\ 5 & 17 & 5 \\ 5 & 5 & 17 \end{vmatrix}$$

a circulant matrix is considered.

To share K_S with Receiver 'B',

$$K_S \; *| K_B^{-1} | \; = \; K_{SC.}$$

$$\begin{vmatrix}4 & 9 & 15\\15 & 17 & 6\\24 & 0 & 17\end{vmatrix}\begin{vmatrix}17\\5\\5\end{vmatrix} = \begin{vmatrix}9\\6\\9\end{vmatrix} \text{ mod 29, which is transferred to B.}$$

At 'B', $K_{SC} * |K_B| = K_S$ which is used to generate basins.

At 'B', $\begin{vmatrix}17 & 17 & 5\\21 & 18 & 21\\2 & 2 & 19\end{vmatrix}\begin{vmatrix}9\\6\\9\end{vmatrix} = \begin{vmatrix}17\\5\\5\end{vmatrix}$ mod 29

Plain Text considered = A S P
01 19 16

Cipher text generator = $|KA| * |PT| * |K_B^{-1}| =$

Encryption process:

$$\begin{vmatrix}5 & 7 & 10\\13 & 17 & 7\\0 & 5 & 4\end{vmatrix} * \begin{vmatrix}1\\19\\16\end{vmatrix} * \begin{vmatrix}4 & 9 & 15\\15 & 17 & 6\\24 & 0 & 17\end{vmatrix} \text{ mod 29}$$

$$= \begin{vmatrix}12\\06\\03\end{vmatrix}$$

2. Methodology to generate Basins

Consider a Quinary vector, a global parameter: Consider a Circulant matrix, K_S . Represent the circulant matrix to match with the dimensions of Quinary vector. Multiply the Quinary vector with circulant matrix and calculate the modularity of product with 29 and a sequence is generated. This sequence is divided into basins of equal values equal to the number of characters of alphabet considered. Any one value of the basin is considered randomly which is mapped with character of Cipher text generated from Hill Cipher.

Example:

$$\text{Quinary Vector} = \begin{vmatrix}0 & 0 & 0\\0 & 0 & 1\\ & \vdots & \\4 & 4 & 4\end{vmatrix} * \begin{vmatrix}17 & 5 & 5\\5 & 17 & 5\\5 & 5 & 17\end{vmatrix} \text{ mod 124}$$

=0-124

Basins Formed:

b(1)	(0	43	86	5)	b(2)	(48	91	10	53)
b(3)	(96	15	58	101)	b(4)	(20	63	103	26)
b(5)	(68	111	30	73)	b(6)	(116	35	78	121)
b(7)	(40	83	2	45)	b(8)	(88	71	50	93)
b(9)	(12	55	98	17)	b(10)	(60	103	22	65)
b(11)	(108	27	70	113)	b(12)	(32	75	118	37)
b(13)	(80	123	42	85)	b(14)	(4	47	90	9)
b(15)	(52	95	14	57)	b(16)	(100	19	62	105)
b(17)	(24	67	110	29)	b(18)	(72	115	34	77)
b(19)	(120	39	82	144)	b(20)	(6	49	92	11)
b(21)	(54	97	16	59)	b(22)	(102	21	64	107)
b(23)	(26	69	112	31)	b(24)	(74	117	36	79)

b(25)	(122	41	84	3)	b(26)	(46	89	8	51)
b(27)	(94	13	56	99)	b(28)	(18	61	104	23)
b(29)	(66	109	25	71)	b(30)	(114	33	76	119)
b(31)	(38	81	0).						

Output of Hill cipher = 12 6 3
Cipher text 1 = 32 78 15
Cipher text 2 = 75 35 58

A random value from basins 12,6 & 3 will replace the output of Hill cipher to be transmitted.

Decryption process:

Cipher text 1 = 32 78 15
Corresponding Basin value = 12 6 3

$$\begin{vmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{vmatrix} * \begin{vmatrix}21 & 14 & 1\\ 0 & 8 & 25\\ 13 & 3 & 8\end{vmatrix} * \begin{vmatrix}12\\ 6\\ 3\end{vmatrix} = \begin{vmatrix}1\\ 19\\ 16\end{vmatrix}$$

3. Security Analysis:

The main limitation with Hill Cipher is that if sufficient elements of plain text & Cipher text are obtained, the key can be retrieved. Thus the Hill Cipher prone to known Plain text attack. In this model, since multiple Cipher texts are generated, the Cipher text transmitted, when mapped with known Plain text, it will not generate the key. Thus the given model is free from Plain text attack. Since multiple CT's are formed, It is also free from chosen Cipher text attack.

Thus if the CT transferred is 32 78 15

then $K_A^{-1} * CT_1 * K_B \neq PT$;
similarly $K_A^{-1} * CT_2 * K_B \neq PT$;

$$|K_A^{-1}| * \begin{vmatrix}32\\ 78\\ 15\end{vmatrix} = \begin{vmatrix}10\\ 13\\ 16\end{vmatrix}$$

$$|K_B| * \begin{vmatrix}10\\ 13\\ 16\end{vmatrix} = \begin{vmatrix}7\\ 26\\ 2\end{vmatrix} \rightarrow$$ Does not transformed to original Plain text

Similarly,

$$|K_A^{-1}| * \begin{vmatrix}75\\ 35\\ 58\end{vmatrix} = \begin{vmatrix}6\\ 19\\ 17\end{vmatrix}$$

$$|K_B| * \begin{vmatrix}6\\ 11\\ 17\end{vmatrix} = \begin{vmatrix}25\\ 6\\ 9\end{vmatrix} \rightarrow$$ Different Plain text is formed

Thus the given model is free from Known Plain text & Chosen Cipher text attacks.

Table1: Comparative study of algorithms based on security analysis

S No.	Algorithm	Security Analysis
1.	Hill cipher	Susceptible to Known Plain text attack
2.	Modifies Hill cipher	Free from Known Plain text attacks. Free from Chosen cipher text attacks

V. Conclusion & Future Work

In the given work the output of Classical Hill cipher is modified to generate multiple cipher texts and any one cipher text is used for transmission. During decryption process the received cipher text is initially transformed to output of Hill cipher which is decrypted back to plain text. Since randomization of Cipher text is made in this work it is relatively free from known plain text and chosen cipher text attacks at slightly more computational overhead. The work may be extended to append time stamp and nonce values for timing and acknowledgement support.

REFERENCES

[1] Adi Narayana Reddy Ka,Vishnuvardhan Bb,Krishna A V Nc, Madhuviswanathamd, i * "A Modified Hill Cipher Based on Circulant Matrices", presented in C3IT-2012, available online on www.Science Direct.com

[2]Chefranov A. G., "Secure Hill Cipher Modification SHC-M" Proc. Of the First International Conference on Security of Information and Network (SIN2007) 7-10 May 2007, Gazimagusa (TRNC) North Cyprus, Elci, A., Ors, B., and Preneel, B (Eds) Trafford Publishing, Canada, 2008: pp 34-37, 2007

[3]. D. Kalman and J.E. White, Polynomial equations and circulant matrices, Amer. Math. Monthly 108 (2001), 821–840.

[4]Georg J.Fuchsbauer: An Introduction to Probabilistic Encryption, 'Osjecki Matematicki List 6(2006), pp37-44

[5] Guo D, Cheng L.M., Cheng L.L: A New Symmetric Probabilistic Encryption Scheme Based on Chaotic Attractors of Neural Networks, Applied Intelligence, Vol 10, No.1, Jan 99, pp 71-84.

[6]. Hill LS Cryptography in an Algebraic Alphabet. American Mathematical Monthly 1929; 36: 306-312

[7]. Hill LS Concerning Certain Linear Transformation Apparatus of cryptography. American Mathematical Monthly 1931; 38: 135-154

[8]. Krishna A.V.N, S.N.N.Pandit, A.Vinaya Babu: A generalized scheme for data encryption technique using a randomized matrix key, Journal of Discrete Mathematical Sciences & Cryptography, Vol 10, No. 1, Feb 2007, pp73-81

[9] Krishna A.V.N, A.Vinaya Babu: A Modified Hill Cipher Algorithm for Encryption of Data in Data Transmission, Georgian Electronic Scientific Journal: Computer Science and Telecommunications 2007 !N0. 3(14) pp 78-83.

[10] Lin CH, Lee CY, Lee CY. Comments on Saeednia's improved scheme for the Hill cipher. Journal of the Chinese institute of engineers 2004; 27: 743-746

[11] Li C, Zhang D, Chen G. Cryptanalysis of an image encryption scheme based on the Hill cipher.*Journal of Zhejiang University - Science A* 2008; **9**: 1118-1123

[12]. Mohsen Toorani, Abolfazl Falahati. A Secure Cryptosystem based on Affine Transformation. Journal of Security and Communication Networks 2011. 2:207-215

[13]. Mohsen Toorani, Abolfazl Falahati. A secure variant of the Hill cipher. IEEE 2009. 313-316

[14] Saeednia S. How to Make the Hill Cipher Secure. *Cryptologia Journal* 2000; 24: 353-360

[15] William Stallings Cryptography and Network Security Principles and Practices. Printice Hall, 2006

[16] Yeh YS, Wu TC, Chang CC, Yang WC. A New Cryptosystem Using Matrix Transformation. 25th IEEE International Carnahan Conference on Security Technology 1991: 131-138

[17]. Y.Mahmoud Ahmed, Alexander G. Chefranov. "Hill Cipher Modification Based on Eigenvalues HCM-EE". In Proc. Of the First International Conference on Security of Information and Network (SIN2009) Gazimagusa (TRNC), North Cyprus, Elci, A., Orgun,

M., and Chefranov, A. (Eds), ACM NewYork, USA, pp. 164-167, 2009.

[18]. Y. Mahmoud Ahmed, Chefranov A. G., " Hill Cipher Modification Based on Pseudo-Random Eigenvalues HCM-PRE" Submitted to Turkish Journal of Electrical Engineering & Computer Science on 2-03-2010.

Dr.A.V.N.Krishna is a Ph.d in Computer Science & engineering. His fields of interest are Network Security and Mathematical modeling. He has published his work in Journals of International repute. He is actively engaged in Academic and research fields for the last 22 yrs.

Mrs K Madhura Vani is a research scholar actively engaged in research activities in Network Security area.

