A New Modal of Hill Cipher using Non – Quadratic Residues

L. Sreenivasulu Reddy

Abstract*— *This paper is improved the security on Hill cipher by using Non-Quadratic residues of a prime number $p \geq 53$. In Hill Cipher, a plain text is encrypted using a fixed value '26' during the computation. The paper explains how using Non-Quadratic residues during encryption improves security.

Key Words : modular arithmetic inverse, inner key, outer key, linear congruence's, Quadratic residues, Non-Quadratic residues, GL (n, Z).

I. INTRODUCTION

In cryptography Hill cipher [1] has been a prominent block cipher. Considering only 26 alphabetic characters 'a' to 'z', Hill developed a block cipher, the encryption of which can be described by the equation

$$C \equiv KP \bmod 26, \qquad (1.1)$$

Where K is a key matrix of size n X n, P is a plaintext vector and C is the cipher text vector both having n components. Decryption of cipher is carried out by using the relation

$$P \equiv K^{-1}C \bmod 26 \ldots\ldots\ldots\ldots.. \qquad (1.2)$$

Where K^{-1} is the modular arithmetic inverse [2] of the key matrix K.

The brute force approach to break the cipher text is infeasible, because the size of the key matrix 'K' is large. However, the cipher text can be broken, if plaintext and the corresponding cipher text are known partially (approximately up to 'n' column vectors).

In this paper our objective is to modify the Hill cipher by introducing an additional key. To this end, we use Non-Quadratic residues of a large primes , $P \geq 53$ to map the characters of plain text to the set $\mathbf{Q}\ (\mathbf{Z})^{*}_{\mathbf{P}}$. And during encryption and decryption, modulo is taken with respect to 'P' instead of '26', as is the case with Hill cipher. So, the private key space is (K, P), unlike only K in Hill Cipher.

In section 2, definitions and theorems used are mentioned. In Section 3, the encryption procedure is explained. In section 4, an example is given, which explains the process. Section 5 concludes with a summary of the work and its' implications

II. DEFINITIONSAND THEOREMS

Congruence:

Let 'm' be a positive integer. 'a' is congruent to 'b' modulo 'm' if m | (a-b). Where a, b, m are integers, symbolically a≡b (mod m).

Linear congruence in one variable:

A congruence of a form ax ≡ b (mod m), where 'x' is an unknown integer, is called a linear congruence in one variable.

Inverse of a modulo 'm':

Given an integer a with (a,m)=1, a solution of ax ≡ 1 (mod m) is called an Inverse of a modulo 'm'.

System of linear congruence:

Let A and B be n x k matrices with integer entries, with (i,j)the entries a_{ij} and b_{ij} respectively. 'A' is congruent to 'B' modulo 'm' if $a_{i\,j} \equiv b_{ij}$ (mod m) for all pairs (i,j) with $1 \leq i \leq n$ and $1 \leq j \leq k$. Symbolically, A ≡ B (mod m) if A is congruent to B modulo 'm'.

Inverse of a matrix modulo 'm' :

If **A** and $\overline{A}$ are n x n matrices of integers and if **A** $\overline{A} \equiv \overline{A}$ A ≡ I (mod m), where I is the identity matrix of order n, then $\overline{A}$ is said to be an inverse of A modulo m.

Quadratic Residue :

If 'm' is a positive integer, the integer 'a' is a quadratic residue of 'm' if (a, m) = 1 and the congruence $x^2 \equiv a \pmod{m}$ has a solution. If the congruence $x^2 \equiv a \pmod{m}$ has no solution, then 'a' is defined as quadratic non residue of 'm' .

General linear group of degree 'n' over ' $\mathbf{Q}\ (\mathbf{Z})^{*}_{\mathbf{P}}$ ' :

The set of Invertible matrices of order n over the set of Integers of a matrix multiplicative group is called "General linear group of degree 'n' over '$\mathbf{Q}\ (\mathbf{Z})^{*}_{\mathbf{P}}$ ', denoted by GL (n, $\mathbf{Q}\ (\mathbf{Z})^{*}_{\mathbf{P}}$).

Theorems :

a. If p is an odd prime, then there is exactly (p-1)/2 quadratic residues of p and (p-1)/2 quadratic non-quadratic residues of p among the integers 1, 2… p-1.

b. If 'A' is an n x n matrix with integer entries and m is a positive integer such that (det A, m) = 1, then the matrix $\overline{A} = \overline{\Delta}$ (adj A) is an inverse of A modulo m, where $\overline{\Delta}$ is an inverse of Δ = det A modulo m.

III. IMPLEMENTATION DETAILS

A.Encryption Algorithm:

The encryption algorithm takes 'm' successive plaintext letters and substitutes for these 'm' cipher text letters [3].This cipher is a polygraphic encipherment similar to Hill cipher.

The substitution is determined by 'm' linear equations in which each character is assigned a distinct numerical value. These numeric values are the non-quadratic residue values of a prime number 'P'. The number 'P' is chosen so that 'P' has at least 26 quadratic residues (considering only the English lowercase alphabet).

Manuscript received on April 14, 2012.

Dr. L Sreenivasulu Reddy, Department of Computer Science & Engineering, Madanapalle Institute of Technology & Science, P.B.No.14, Angallu, Madanapalle-517325, A.P, India.
(E-mail:sreenivasulureddy.svu@gmail.com).

.

The characters are mapped one -one to $\mathbf{Q}\ (\mathbf{Z})^{*}_{\mathbf{P}}$ .However, the procedure has flexibility to consider any large prime greater than or equal to 53, unlike 26 in Hill cipher. So the procedure can be carried over to any plain text space.

For m = 3, the system can be described as follows:

$$C_1 \equiv (K_{11} P_1 + K_{12} P_2 + K_{13} P_3) \bmod P$$
$$C_2 \equiv (K_{21} P_1 + K_{22} P_2 + K_{23} P_3) \bmod P$$
$$C_3 \equiv (K_{31} P_1 + K_{32} P_2 + K_{33} P_3) \bmod P$$

This can be expressed in terms of column vectors and matrices:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \bmod P$$

(or)

$$C \equiv KP^{*} \bmod P.$$

Where C & P* are column vectors of length 3, representing the plain text and transferred matrix , and k is a 3 x 3 non-singular matrix in GL (n, $\mathbf{Q}\ (\mathbf{Z})^{*}_{\mathbf{P}}$).,representing the encryption key . Operations are performed with respect to mod P.

B.Description Algorithm:

First find the inverse of matrix $\overline{K}$ of a matrix K is applied to the transferred matrix C with respect to mod p, then the plaintext is recovered.

The deciphering process for this cipher system takes a transferred matrix C and obtains a plain text blocks using the transformation. Selection of matrix K is chosen that all the rows of KP* mod P are non-vanishing.

C. Security Analysis :

Polygraphic ciphers operating with blocks of size ‘n’ are vulnerable to cryptanalysis based on frequencies of bocks of size ‘n’ (for small n < 6)

For example according to some counts, the most common blocks of size 2 in English are ‘TH’ followed closely by ‘HE’. If a Hill digraph cipher system has been employed and the most common digraph is ‘KX’ followed by ‘VZ’ one can guess that the cipher text digraph ‘KX’ and ‘VZ’ corresponds to ‘TH’ and ‘HE’ respectively. This would mean that 19 7 and 7 4 are send to 10 23 and 21 25 respectively. If ‘A’ is the enciphering matrix this implies that

$$A \begin{bmatrix} 19 & 7 \\ 7 & 4 \end{bmatrix} \equiv \begin{bmatrix} 10 & 21 \\ 23 & 25 \end{bmatrix} \pmod{26}$$

Since $\begin{bmatrix} 4 & 19 \\ 19 & 19 \end{bmatrix}$ is an inverse of $\begin{bmatrix} 19 & 7 \\ 7 & 4 \end{bmatrix}$ (mod 26), we find that

$$A \equiv \begin{bmatrix} 10 & 21 \\ 23 & 25 \end{bmatrix} \begin{bmatrix} 4 & 19 \\ 19 & 19 \end{bmatrix} \equiv \begin{bmatrix} 23 & 17 \\ 21 & 2 \end{bmatrix} \pmod{26}$$

This gives the possible key. After attempting to decipher the cipher text using $\overline{A} = \begin{bmatrix} 2 & 9 \\ 5 & 23 \end{bmatrix}$ to transform the cipher text, one would know whether the guess was correct or not.

The procedure described in Section 3, achieves more security by taking a variable ‘P’ instead of fixed value 26.

IV. CONCLUSION

The decryption is possible only when outer key and private are known. Hence, the algorithm is less vulnerable to ‘Known Plain Text’ methods of attack.

REFERENCES

1. Introduction to Analytic Number Theory, fifth edition. T. Apostol .Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1995
2. An introduction to the theory of numbers, 5th ed.,I. Niven, H. S. Zuckerman and H. L. Montgomery, Wiley, New York, 1991.
3. Cryptography and Network security, William stallings, 3rd Edition, pearson Education
4. On the Modular Arithmetic Inverse in the cryptology of Hill cipher, 2005. V.U.K. sastry, V.Janaki, proceedings of North American Technology and Business conference, canada
5. Hill’s System of Data Encryption prepared by” Ben Kohler and Michael Ziegler”
6. A.Vanstone. Handbook of Applied cryptography Menezes, Alfred, paul C.Van Oorschot, and scott .New York: CRC press,1997
7. Saroj KumarPanigrahy,Bindudendra Acharya and debasish Jena,Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm, 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.
8. G.Sivagurunathan, V.Rajendran and Dr.T.Purusothaman. Classification of Substitution Ciphers using Neural Networks . IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.3, March 2010.