International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-10 Issue-4, November 2021

A Cryptographic Application of the M-Injectivity of $M_n(Z_p)$ Over Itself

Wannarisuk Nongbsap , Madan Mohan Singh

Abstract- In this paper, we present a public key scheme using Discrete Logarithm problem, proposed by Diffie and Hellman (DLP)[1], particularly known as the Computational Diffie-Hellman Problem (CDH)[12]. This paper uses the Elgamal encryption scheme [6] and extends it so that more than one message can be sent. The combination of Hill Cipher[14] and the property of the matrix ring $M_n(Z_p)$, of being left m-injective over itself, where p is a very large prime, are major contributions towards the proposal of this scheme.

Keywords:- m-injective, R-monomorphisms, $M_n(Z_p)$, public key cryptography, Discrete Logarithm Problem, Computational Diffie-Hellman Problem, Hill Cipher.

I. INTRODUCTION

Let R be a ring with identity element. A left ideal I of R is a subgroup of R, with respect to addition, if for any $x \in I$ and $r \in R$, $rx \in I$. A Principal Ideal Ring (PIR) is a ring whose every ideal (left or right) is generated by a single element. A ring R is von Neumann regular if for any $a \in R$, there exists $b \in R$ such that $a = aba$ [13].

A non-empty set M is a left R-module if M is an abelian group with respect to addition and if there exists a map $.: R \times M \longrightarrow M$ such that (i) $(r+s).m = r.m + s.m$ (ii) $r.(m_1 + m_2) = r.m_1 + r.m_2$ (iii) $(rs).m = r.(sm)$ (iv) $1.m = m$, $\forall r, s \in R$ and $\forall m_1, m_2 \in M$ [3]. Also, we recall that a function h from a ring R to a ring S is a left R homomorphism if $\forall x, y \in R$, (i) $h(x+y) = h(x) + h(y)$ (ii) $h(rx) = rh(x)$, $\forall r \in R$([3],[4]).

A left R module E is injective over R if for any left R-monomorphism $\alpha: M \to M'$ of left R-modules M and M' and any left R- homomorphism $f: M \to E$, there exists a left R-homomorphism $g: M' \to E$ such that $g_o\alpha = f$ [15]. We shall now give Baer's criterion and then modify it to introduce the concept of m-injective rings. Let E be a left R-module. According to Baer's criterion, E is injective over R if and only if for every left ideal A of R, any left R-homomorphism $f: A \longrightarrow E$ can be extended to a left R-homomorphism $g: R \longrightarrow E$([1],[2],[3]).

In our study, $E = R$ and using Baer's criterion, we define m-injective in the following manner.

A ring R, regarded as a module over itself, is left m-injective over itself if for any left ideal A of R, any left R-monomorphism $f: A \longrightarrow R$ can be extended to a left R-monomorphism $g: R \longrightarrow R$. As in the definition of homomorphism, a function h from a ring R to another ring S is a left R-monomorphism if $\forall x, y \in R$, (i) $h(x+y) = h(x) + h(y)$ (ii) $h(rx) = rh(x)$, $\forall r \in R$ (iii) h is one-one. This concept of self m-injective rings is an extension of the concept of Self injective rings which was introduced by Y. Utumi [5] in the year 1965. In [5], Utumi studied the properties of commutative rings which are injective over themselves. In this paper, $R = M_n(Z_p)$ is a non-commutative finite ring. A public key cryptography is an encryption scheme that uses a public key known to every one and a private key known only to the one whose decrypts the message. The problem used in this paper is discrete logarithm problem i.e for a very large prime p and given two known values d and r such that $d = r^t (mod\ p)$, it is difficult to find t[1] and given r, r^t, r^k, modulo p, it is difficult to find r^{tk} modulo p, unless one of t and k is known[12]. Lester Hill invented the Hill Cipher in 1929. Hill Cipher is a polygraphic substitution cipher based on linear algebra. The most vital component of the Hill Cypher is the key matrix. The key matrix is used to encrypt the messages, and its inverse is used to decrypt the encoded messages. It is important that the key matrix be kept secret between the message senders and the intended recipients. The receiver of the message decodes the key matrix using its inverse. In this paper, the key matrix is also the encoding matrix and its inverse is the decoding matrix. The main drawback of Hill Cipher is in selecting the correct encryption key matrix for encryption. If the key matrix is not properly chosen, the generation of decryption key matrix i.e. the inverse of encryption matrix is not possible. This is because if the encryption key matrix is invertible then only the inverse of encryption matrix is possible. In our paper, there is a quick generation of the invertible key matrix due to the m-injectivity of the ring $M_n(Z_p)$ over itself.

Notation:-$\bar{x}$ used in this paper will denote the integer x modulo p.

II. RESULTS AND DISCUSSION

Before we present our cryptographic scheme, we prove the following results.

Theorem 2.1 If every left ideal of a ring R is a direct summand of R then R is left m-injective over itself.

Proof. Let A be any left ideal of R. Let $f: A \longrightarrow R$ be a left R-monomorphism. Since A is a direct summand of R, there exists a left ideal B of R such that $A \oplus B = R$.

Manuscript received on September 09, 2021.
Revised Manuscript received on September 16, 2021.
Manuscript published on September 30, 2021.

* Correspondence Author
Wannarisuk Nongbsap*, Assistant Professor, Department of Mathematics, St. Anthony's College, Shillong, Meghalaya, India.
Dr. Madan Mohan Singh, Associate Professor, Department of Basic Sciences and Social Sciences, School of Technology, North Eastern Hill University, Shillong, Meghalaya, India.

Let $g: R \longrightarrow R$ be defined by

$$g(x) = \begin{cases} f(x), & if \quad x \in A \\ x, & if \quad x \in B \end{cases}$$

m, g extends f and g is a left R-monomorphism

Theorem 2.2 If a Principal Ideal Ring R is von Neumann Regular then R is left m-injective over itself.

Proof. Let $a \in R$. Let $f: Ra \longrightarrow R$ be a left R-monomorphism. Since R is regular, there exists $b \in R$ such that $a = aba \Rightarrow e = ba = baba$.

Now idempotent element $e = ba \in Ra$. Again $R = Re + R(1-e) \subseteq Ra + R(1-e)$.

Hence, $R = Ra + R(1-e)$. Let $x \in Ra \cap R(1-ba) \Rightarrow x = ra$ and $x = s(1-ba)$ for some $r, s \in R$. Now, $xba = raba = ra = x$. So, $0 = x(1-ba) = s(1-ba)(1-ba) = s(1-ba) = x$. Hence, Ra is a direct summand of R, therefore, R is left m-injective over itself.

A field F is von Neumann regular and it is well known that matrix rings over von Neumann regular rings are von Neumann regular. Since $M_n(F)$ is a Principal Ideal Ring which is von Neumann Regular, it is obvious that $M_n(F)$ is left m-injective over itself. However, to make use of this property in the proposed scheme, we shall consider one of the left ideals A of $M_n(F)$. .

Let A be a left ideal of F [9] generated by

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

then

$$A = \left\{ \begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & 0 & 0 & \dots & 0 \\ a_{31} & 0 & 0 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1} & 0 & 0 & \dots & 0 \end{pmatrix} : \quad a_{i1} \in F, \quad 1 \leq i \leq n \right\}$$

Let $f: A \longrightarrow M_n(F)$ be a left R-monomorphism.

Suppose $f \left(\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix} \right) = \begin{pmatrix} x_{11} & x_{12} & x_{13} & \dots & x_{1n} \\ x_{21} & x_{22} & x_{23} & \dots & x_{2n} \\ x_{31} & x_{32} & x33 & \dots & x_{3n} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ x_{n1} & x_{n2} & x_{n3} & \dots & x_{nn} \end{pmatrix}$,

for some $\begin{pmatrix} x_{11} & x_{12} & x_{13} & \dots & x_{1n} \\ x_{21} & x_{22} & x_{23} & \dots & x_{2n} \\ x_{31} & x_{32} & x_{33} & \dots & x_{3n} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ x_{n1} & x_{n2} & x_{n3} & \dots & x_{nn} \end{pmatrix} \in M_n(F).$

Then $\forall \begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & 0 & 0 & \dots & 0 \\ a_{31} & 0 & 0 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1} & 0 & 0 & \dots & 0 \end{pmatrix} \in A,$

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$$f\left(\begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & 0 & 0 & \dots & 0 \\ a_{31} & 0 & 0 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1} & 0 & 0 & \dots & 0 \end{pmatrix}\right) = f\left(\begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & 0 & 0 & \dots & 0 \\ a_{31} & 0 & 0 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1} & 0 & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}\right)$$

$$= \begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & 0 & 0 & \dots & 0 \\ a_{31} & 0 & 0 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1} & 0 & 0 & \dots & 0 \end{pmatrix} f\left(\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}\right)$$

$$= \begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & 0 & 0 & \dots & 0 \\ a_{31} & 0 & 0 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1} & 0 & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} & x_{13} & \dots & x_{1n} \\ x_{21} & x_{22} & x_{23} & \dots & x_{2n} \\ x_{31} & x_{32} & x_{33} & \dots & x_{3n} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ x_{n1} & x_{n2} & x_{n3} & \dots & x_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11}x_{11} & a_{11}x_{12} & a_{13}x_{13} & \dots & a_{1n}x_{1n} \\ a_{21}x_{11} & a_{21}x_{12} & a_{23}x_{13} & \dots & a_{2n}x_{1n} \\ a_{31}x_{11} & a_{31}x_{12} & a_{33}x_{13} & \dots & a_{3n}x_{1n} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1}x_{11} & a_{n1}x_{12} & a_{n3}x_{13} & \dots & a_{nn}x_{1n} \end{pmatrix}$$

Since f is one-one, at least one of $x_{1j}, 1 \le j \le n$ is nonzero. For if all are zero then

$$f\left(\begin{pmatrix} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & 0 & 0 & \dots & 0 \\ a_{31} & 0 & 0 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1} & 0 & 0 & \dots & 0 \end{pmatrix}\right) = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

This is a contradiction. Suppose, we assume that $x_{11} \neq 0$.

Let us define a function $g: M_n(F) \longrightarrow M_n(F)$ on a generator of $M_n(F)$ by

$$g\left(\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}\right) = \begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} & x_{15} & \dots & x_{1(n-1)} & x_{1n} \\ 0 & 1 & x_{12} & x_{13} & x_{14} & \dots & x_{1(n-2)} & x_{1(n-1)} \\ 0 & 0 & 1 & x_{12} & x_{13} & \dots & x_{1(n-2)} & x_{1(n-2)} \\ . & . & . & . & . & \dots & . & . \\ . & . & . & . & . & \dots & . & . \\ . & . & . & . & . & \dots & . & . \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Then $\forall \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix} \in M_n(F)$,

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$$g\left(\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}\right) =$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} & x_{15} & \dots & x_{1(n-1)} & x_{1n} \\ 0 & 1 & x_{12} & x_{13} & x_{14} & \dots & x_{1(n-2)} & x_{1(n-1)} \\ 0 & 0 & 1 & x_{12} & x_{13} & \dots & x_{1(n-2)} & x_{1(n-2)} \\ . & . & . & . & . & \dots & . & . \\ . & . & . & . & . & \dots & . & . \\ . & . & . & . & . & \dots & . & . \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} a_{11}x_{11} & a_{11}x_{12}+a_{12} & a_{11}x_{13}+a_{12}x_{12}+a_{13} & \dots & a_{11}x_{1n}+a_{12}x_{1(n-1)}+\dots+a_{1(n-1)}x_{12}+a_{1n} \\ a_{21}x_{11} & a_{21}x_{12}+a_{22} & a_{21}x_{13}+a_{22}x_{12}+a_{23} & \dots & a_{21}x_{1n}+a_{22}x_{1(n-1)}+\dots+a_{2(n-1)}x_{12}+a_{2n} \\ a_{31}x_{11} & a_{31}x_{12}+a_{32} & a_{31}x_{13}+a_{32}x_{12}+a_{33} & \dots & a_{31}x_{1n}+a_{32}x_{1(n-1)}+\dots+a_{3(n-1)}x_{12}+a_{3n} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1}x_{11} & a_{n1}x_{12}+a_{n2} & a_{n1}x_{13}+a_{n2}x_{12}+a_{n3} & \dots & a_{n1}x_{1n}+a_{n2}x_{1(n-1)}+\dots+a_{n(n-1)}x_{12}+a_{nn} \end{pmatrix} =$$

$$\begin{pmatrix} a_{11}x_{11} & \sum_{1\le j\le 1;2\le s\ge 2} a_{1j}x_{1s}+a_{12} & \sum_{1\le j\le 2;3\ge s\ge 2} a_{1j}x_{1s}+a_{13} & \dots & \sum_{1\le j\le (n-1);n\ge s\ge 2} a_{1j}x_{1s}+a_{1n} \\ a_{21}x_{11} & \sum_{1\le j\le 1;2\le s\ge 2} a_{2j}x_{1s}+a_{22} & \sum_{1\le j\le 2;3\ge s\ge 2} a_{2j}x_{1s}+a_{23} & \dots & \sum_{1\le j\le (n-1);n\ge s\ge 2} a_{2j}x_{1s}+a_{2n} \\ a_{31}x_{11} & \sum_{1\le j\le 1;2\le s\ge 2} a_{3j}x_{3s}+a_{32} & \sum_{1\le j\le 2;3\ge s\ge 2} a_{3j}x_{1s}+a_{33} & \dots & \sum_{1\le j\le (n-1);n\ge s\ge 2} a_{3j}x_{1s}+a_{3n} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1}x_{11} & \sum_{1\le j\le 1;2\le s\ge 2} a_{nj}x_{1s}+a_{n2} & \sum_{1\le j\le 2;3\ge s\ge 2} a_{nj}x_{1s}+a_{n3} & \dots & \sum_{1\le j\le (n-1);n\ge s\ge 2} a_{nj}x_{1s}+a_{nn} \end{pmatrix} \text{———(1)}$$

It can be easily verified that g is a well-defined left R-monomorphism extending f. Also, from equation (1), we have

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} & x_{15} & \dots & x_{1(n-1)} & x_{1n} \\ 0 & 1 & x_{12} & x_{13} & x_{14} & \dots & x_{1(n-2)} & x_{1(n-1)} \\ 0 & 0 & 1 & x_{12} & x_{13} & \dots & x_{1(n-2)} & x_{1(n-2)} \\ . & . & . & . & . & \dots & . & . \\ . & . & . & . & . & \dots & . & . \\ . & . & . & . & . & \dots & . & . \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} a_{11}x_{11} & \sum_{1\le j\le 1;2\le s\ge 2} a_{1j}x_{1s}+a_{12} & \sum_{1\le j\le 2;3\ge s\ge 2} a_{1j}x_{1s}+a_{13} & \dots & \sum_{1\le j\le (n-1);n\ge s\ge 2} a_{1j}x_{1s}+a_{1n} \\ a_{21}x_{11} & \sum_{1\le j\le 1;2\le s\ge 2} a_{2j}x_{1s}+a_{22} & \sum_{1\le j\le 2;3\ge s\ge 2} a_{2j}x_{1s}+a_{23} & \dots & \sum_{1\le j\le (n-1);n\ge s\ge 2} a_{2j}x_{1s}+a_{2n} \\ a_{31}x_{11} & \sum_{1\le j\le 1;2\le s\ge 2} a_{3j}x_{1s}+a_{32} & \sum_{1\le j\le 2;3\ge s\ge 2} a_{3j}x_{1s}+a_{33} & \dots & \sum_{1\le j\le (n-1);n\ge s\ge 2} a_{3j}x_{1s}+a_{3n} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1}x_{11} & \sum_{1\le j\le 1;2\le s\ge 2} a_{nj}x_{1s}+a_{n2} & \sum_{1\le j\le 2;3\ge s\ge 2} a_{nj}x_{1s}+a_{n3} & \dots & \sum_{1\le j\le (n-1);n\ge s\ge 2} a_{nj}x_{1s}+a_{nn} \end{pmatrix}.$$

Now, determinant of $\begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} & x_{15} & \dots & x_{1(n-1)} & x_{1n} \\ 0 & 1 & x_{12} & x_{13} & x_{14} & \dots & x_{1(n-2)} & x_{1(n-1)} \\ 0 & 0 & 1 & x_{12} & x_{13} & \dots & x_{1(n-2)} & x_{1(n-2)} \\ . & . & . & . & . & \dots & . & . \\ . & . & . & . & . & \dots & . & . \\ . & . & . & . & . & \dots & . & . \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$ is x_{11}, which is nonzero so its inverse exists. Hence, multiplying to the right of the above equation by the inverse of the above matrix, we get back the matrix

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

The definition of g as an extension of the left R-monomorphism f can be utilised in the encryption and the decryption processes of the proposed scheme below. Also, image of the identity element of $M_n(Z_p)$,under the function g, selected above can be taken as the key matrix in the encryption process and its inverse in the decryption process. Since for any prime p, Z_p is a field and hence $M_n(Z_p)$ is left m-injective over itself. So, using the m-injectivity of $M_n(Z_p)$ over itself and the discrete logarithm problems, we propose the following scheme.

Public and Private Keys Generation

A user X who wants to create public and private keys has to do the following steps:-

1. Choose a very large prime p
2. Choose a large positive integer n
3. Choose r such that $1 < r < p$
4. Choose t_i such that $1 < t_i < p-1$ and $t_i \nmid p-1,\ 1 \le i \le n-1$
5. Compute $dx_i \equiv r^{t_i}(mod\ p), 1 \le i \le n-1$

Public keys are (p, n, dx_i, r) and private keys are $t_i, 1 \le i \le n-1$.

Encryption

The plaintext space is $M_n(Z_p)$. Suppose another user Y wants to send a message in the form of a phrase, whose every character corresponds to the letters of the English alphabets, punctuations and symbols. The characters will be placed row-wise in a matrix and they will be encrypted using the key matrix. Let the characters of the phrase be represented in the matrix

$$M = \left\{ \begin{pmatrix} \overline{c_{11}} & \overline{c_{12}} & \overline{c_{13}} & \dots & \overline{c_{1n}} \\ \overline{c_{21}} & \overline{c_{22}} & \overline{c_{23}} & \dots & \overline{c_{2n}} \\ \overline{c_{31}} & \overline{c_{32}} & \overline{c_{33}} & \dots & \overline{c_{3n}} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ \overline{c_{n1}} & \overline{c_{n2}} & \overline{c_{n3}} & \dots & \overline{c_{nn}} \end{pmatrix} \right\}$$

, where each $c_{ij}, 1 \le i \le n, 1 \le j \le n$ represents the corresponding character in the phrase. Now, using $X's$ public keys, Y will have to do the following steps:-

1. Choose k such that $1 < k < p-1$ and $k \nmid p-1$
2. Compute $x_{1i} \equiv {dx_i}^k(mod\ p), 1 \le i \le n-1$
3. Compute $x_{1n} \equiv r^k(mod\ p)$
4. Construct the key matrix $\begin{pmatrix} \overline{x_{11}} & \overline{x_{12}} & \overline{x_{13}} & \overline{x_{14}} & \overline{x_{15}} & \dots & \overline{x_{1(n-1)}} & \overline{x_{1n}} \\ \overline{0} & \overline{1} & \overline{x_{12}} & \overline{x_{13}} & \overline{x_{14}} & \dots & \overline{x_{1(n-2)}} & \overline{x_{1(n-1)}} \\ \overline{0} & \overline{0} & \overline{1} & \overline{x_{12}} & \overline{x_{13}} & \dots & \overline{x_{1(n-2)}} & \overline{x_{1(n-2)}} \\ . & . & . & . & . & \dots & . & . \\ . & . & . & . & . & \dots & . & . \\ . & . & . & . & . & \dots & . & . \\ \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} & \dots & \overline{0} & \overline{1} \end{pmatrix}$ using the first three steps above
5. Compute $\overline{c} =$

$$\begin{pmatrix} \overline{c_{11}x_{11}} & \overline{\sum_{1\le j\le 1;2\le s\ge 2} c_{1j}x_{1s}} + \overline{c_{12}} & \overline{\sum_{1\le j\le 2;3\le s\ge 2} c_{1j}x_{1s}} + \overline{c_{13}} & \dots & \overline{\sum_{1\le j\le (n-1);n\ge s\ge 2} c_{1j}x_{1s}} + \overline{c_{1n}} \\ \overline{c_{21}x_{11}} & \overline{\sum_{1\le j\le 1;2\le s\ge 2} c_{2j}x_{1s}} + \overline{c_{22}} & \overline{\sum_{1\le j\le 2;3\le s\ge 2} c_{2j}x_{1s}} + \overline{c_{23}} & \dots & \overline{\sum_{1\le j\le (n-1);n\ge s\ge 2} c_{2j}x_{1s}} + \overline{c_{2n}} \\ \overline{c_{31}x_{11}} & \overline{\sum_{1\le j\le 1;2\le s\ge 2} c_{3j}x_{1s}} + \overline{c_{32}} & \overline{\sum_{1\le j\le 2;3\le s\ge 2} c_{3j}x_{1s}} + \overline{c_{33}} & \dots & \overline{\sum_{1\le j\le (n-1);n\ge s\ge 2} c_{3j}x_{1s}} + \overline{c_{3n}} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ \overline{c_{n1}x_{11}} & \overline{\sum_{1\le j\le 1;2\le s\ge 2} c_{nj}x_{1s}} + \overline{c_{n2}} & \overline{\sum_{1\le j\le 2;3\le s\ge 2} c_{nj}x_{1s}} + \overline{c_{n3}} & \dots & \overline{\sum_{1\le j\le (n-1);n\ge s\ge 2} c_{nj}x_{1s}} + \overline{c_{nn}} \end{pmatrix}$$ by multiplying M to the left of the key matrix.

Y sends to X the encrypted message $(\overline{x_{1n}}, \overline{c})$.

Decryption

For the decryption of the message c, X should do the following steps:-

1. Compute ${x_{1n}}^{-1}(mod\ p)$

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

2. Using the private keys $t_i, 1 \le i \le n-1$, the inverse of the key matrix can be found. Multiplying to the right of $\overline{c}$ by the inverse, the original message can be retrieved. Let us take an example of a set of 3×3 matrix, where the entries are from Z_p, to see how the above algorithms work. We take $p = 9999999967$, $r = 893$, $t_1 = 57$ and $t_2 = 965$ then $dx_1 = 208470610$ and $dx_2 = 1129150215$ modulo p. In the encryption process, suppose parameter $k = 85$ then ephemeral key $x_{13} = 6614283676$ and its inverse ${x_{13}}^{-1} = 2600308453$.

Suppose the messages to be sent are $m_{11} = 61$, $m_{12} = 108$, $m_{13} = 4326$, $m_{21} = 192$, $m_{22} = 84$, $m_{23} = 67$, $m_{31} = 88$, $m_{32} = 6304$ and $m_{33} = 98$ modulo p then using the key matrix $\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ 0 & 1 & x_{12} \\ 0 & 0 & 1 \end{pmatrix}$ the messages are encrypted in the matrix $\begin{pmatrix} \overline{8560977214} & \overline{3940845636} & \overline{612479046} \\ \overline{1044387382} & \overline{1584300798} & \overline{4385601600} \\ \overline{4645344203} & \overline{3226144123} & \overline{4074839108} \end{pmatrix}$.

Multiplying by the inverse ,

$$\begin{pmatrix} x_{11}^{-1} & -x_{11}^{-1}x_{12} & {x_{12}}^2{x_{11}}^{-1} - x_{13}{x_{11}}^{-1} \\ 0 & 1 & -x_{12} \\ 0 & 0 & 1 \end{pmatrix} =$$

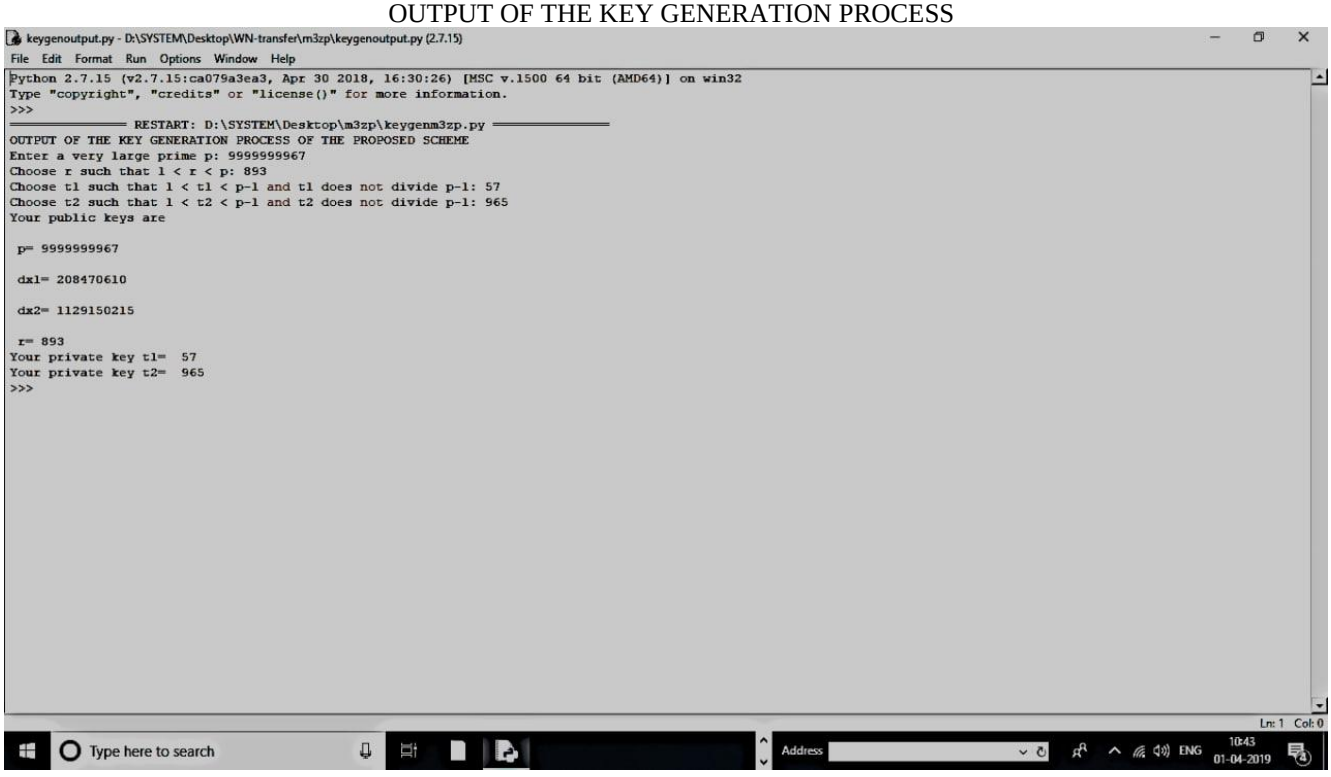
$$\begin{pmatrix} \overline{2600308453^{57}} & \overline{-6614283676^{965}2600308453^{57}} & \overline{2600308453^{57}(6614283676^{1930} - 6614283676)} \\ \overline{0} & \overline{1} & \overline{-6614283676^{965}} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}$$

, of the key matrix,

we get the required messages as $\begin{pmatrix} \overline{61} & \overline{108} & \overline{4326} \\ \overline{192} & \overline{84} & \overline{67} \\ \overline{88} & \overline{6304} & \overline{98} \end{pmatrix}$.

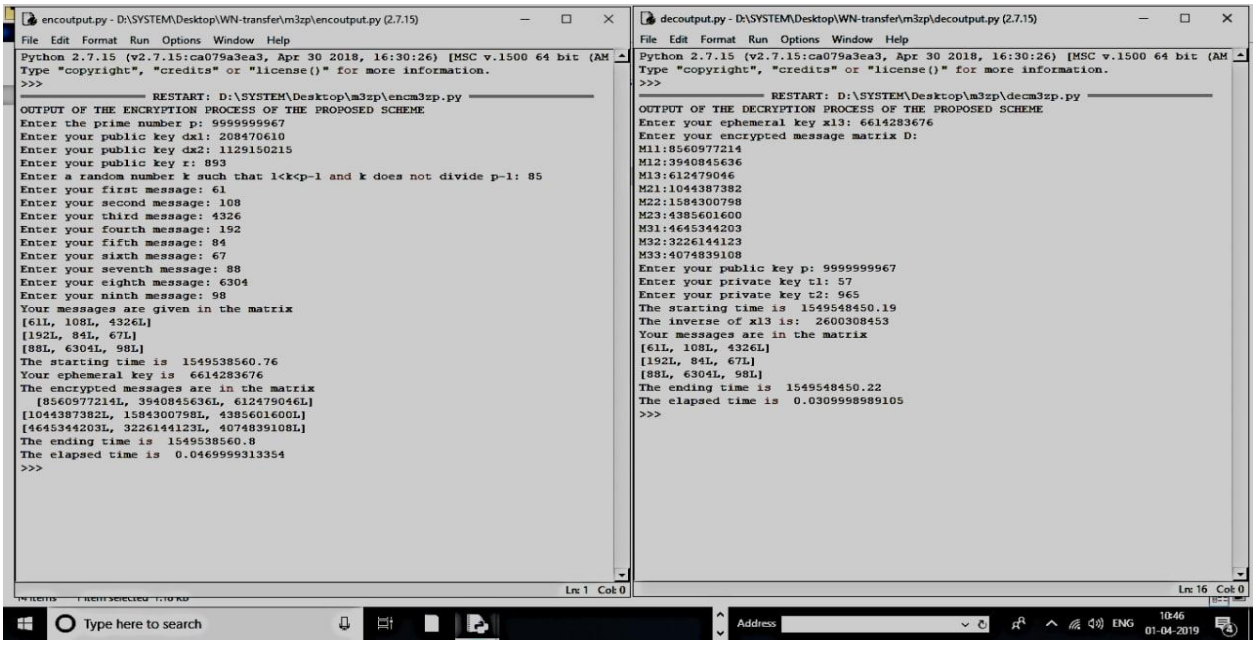
The following are the images of the outputs of the three programs done in connection with the scheme ,viz, program to generate public and private keys, program to encrypt a message and program to decrypt the message. The elapsed times of the encryption and decryption processes are shown in the following outputs. These elapsed times during the encryption and decryption processes were recorded using Python Language, version 2.7.15, using GNU multi precision library(GMP) on 3.2 GHz processor with 4 GB RAM.

OUTPUT OF THE KEY GENERATION PROCESS



fig(i) Output Of The Encryption And Decryption Processes

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)



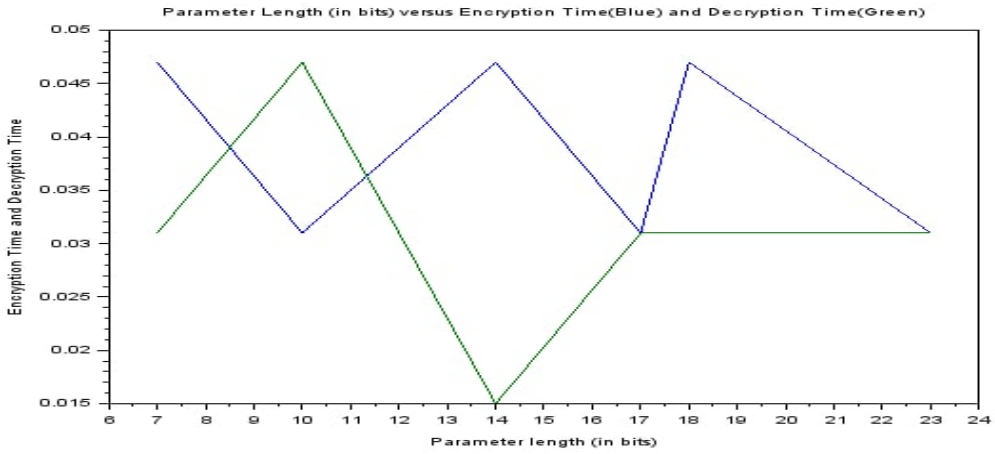
fig(ii) The following table gives us the elapsed time during the encryption and decryption of different messages.

RECORDS OF ELAPSED TIMES

Parameter(k)	Length of k(in bits)	Encryption time(in ms)	Decryption time(in ms)
85	7	0.0469999313354	0.0309998989105
750	10	0.0309998989105	0.0469999313354
9436	14	0.0469999313354	0.0150001049042
87241	17	0.0309998989105	0.0309998989105
146382	18	0.0469999313354	0.0309998989105
7419628	23	0.0310001373291	0.0309998989105

The above table shows that with an increase in the bit length of parameter k, the elapsed times for the encryption process increases and decreases alternately. This is not true in the case of the decryption process, where the elapsed time is seen to alternately increase and decrease at the beginning and then maintains consistency. However, this may vary depending on the public keys p, dx_1, dx_2 and r and k in the encryption process. Again, there are differences between the encryption and the decryption times where on varying h, the former is greater than the latter and vice versa. The graph of the encryption time is a zigzag curve. However, the graph of the decryption time is initially zigzag at the beginning and then becomes parallel to the X-axis with the increase in the bit length of k. Again, on observing the graph, we find that the two curves intersect each other at some points. This shows that for some bit lengths of k, the encryption and decryption times are equal.

GRAPH OF THE ENCRYPTION AND DECRYPTION PROCESSES



fig(iii)

III. SECURITY OF THE SCHEME

The private keys $t_i, 1 \leq i \leq n-1$ have been chosen randomly. An adversary who tries to find t_i will have to solve $n-1$ congruences $dx_i \equiv r^{t_i}(mod\ p)$. These are the Discrete Logarithm Problems. Again, in the encryption process, k has been chosen randomly. Also, we have $x_{1i} \equiv dx_i^k(mod\ p)$ which is equivalent to $x_{1i} \equiv r^{t_i k}(mod\ p)$.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

These are the Computational Diffie-Hellman Problems [12]. So, in total, an adversary has to solve $2(n-1)$ hard problems. Hence, the security of this scheme is based on DLP and CDH. Again, this scheme makes use of the Elgamal encryption scheme so its security is based on the intractibility of the DLP and the Computational Diffie-Hellman Problem(CDH). The key matrix used in the encryption process and its inverse used in the decryption process should not be revealed otherwise all intercepted messages can be easily decoded. Now, $\overline{x_{1i}}, 1 \leq i \leq n-1$ are known only to the sender. It is difficult to find them as they depend on k which is again known only to the sender. Thus, the above two matrices are not easily traceable. For practical security reasons, it is recommended that p should have at least 1024 bits. This can resist attacks like the Exhaustive Key Search method, Shank's Baby-Step Giant Step, Pollard's Rho method, Pohlig-Hellman algorithm, Index Calculus method which require more time and enough memory in the computer to store elements of Z_p[10]. In the encryption process, even if x_{1n} is revealed to everyone, it is difficult to trace these messages because x_{1n} appears in the n^{th} column where every entry in this column is a linear combination of the unknown $x_{1s}, n \geq s \geq 2$ and the unknown messages. To be precise, every entry of this column consists of $2(n-1)$ unknowns and only one known value. This adds to the security of the scheme. In the first, second, ... upto the $(n-1)^{th}$ columns, the messages are in a linear combination of x_{1s} , which are known only to the sender of the messages. This shows that the proposed scheme is semantically secured. Hence, without using private keys no one will be able to decrypt the messages.

IV. PERFORMANCE ANALYSIS

The encryption algorithm of the proposed scheme requires n modular exponentiations, viz, $dx_i^h, 1 \leq i \leq n-1$ and r^h. Within the encryption matrix $\bar{c}$, $\frac{n}{2}(n^2-n+2)$ modular multiplications are done and there are $\frac{n^2}{2}(n-1)$ modular additions. The decryption algorithm requires one application of Euclidean Extended Algorithm to find ${x_{1n}}^{-1}$ modulo p. However, it may be difficult to compute the number of operations required to find the inverse of the key matrix since this will depend on the value of n. At the end of the decryption process, one matrix multiplication is required.

V. CONCLUSION AND FUTURE WORKS

The existence of a left R-monomorphism from $M_n(Z_p)$ to itself formed a base for the creation of the encryption and decryption algorithms of the proposed scheme. The aim of this paper is also to show that the existence of rings which are left m-injective over themselves is applicable to the field of cryptography. Hence, in future, we would like to work with the same ring and find more key matrices, so that more and more messages can be encrypted at once and more hard problems can be used.

REFERENCES

1. W.Diffie, M.Hellman, New Directions in Cryptography, IEEE Trans. Inform. Theory 22(1976),472-492.
2. R. Baer, Abelian Groups that Are Direct Summands of Every Containing Abelian Group, Bull. Amer. Math. Soc. 46, 800-806, 1940.
3. C. Faith, Algebra: Rings, Modules and Categories, I. Berlin, p. 157, 1973.
4. T.Y.Lam, Lectures on Modules and Rings. New York: Springer-Verlag, p. 63, 1999.
5. Y.Utumi, On Continuous Rings and Self Injective Rings,University of Rochester, Rochester, Newyork (1965)158-173.
6. T. Elgamal, A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms, Journal and Magazine > IEEE Transactions on Information Theory, 1985, Volume 31, Issue 4, 409-472.
7. D. Poulakis, A Public Key Encryption Scheme Based on Factoring and Discrete Logarithm, Journal of Discrete Mathematical Sciences and Cryptography 12:6, 745-752(2009)
8. H. Elkamchouchi, K. Elshenawy and H.A.Shaban, Two New Public Key Techniques in the domain of Gaussian Integers, Proceedings of the Twentieth National Radio Science Conference, NRSC 2003 C17, 1-8(2003)
9. R.A. Ferraz, C. Polcino Milies, E. Taufer, Left ideals in matrix rings over finite fields: 1711.0928v1 ,[math. RA] 25 Nov, 2017
10. K. Rabah, Security of the Cryptographic Protocols Based on Discrete Logarithm Problem, Journal of Applied Sciences 5(9): 1692-1712, 2005, ISSN 1812-5654.
11. C. Meshram, X. Huang, S. A. Meshram, New Identity-Based Cryptographic Scheme for IFP and DLP based Cryptosystem, International Journal of Pure and Applied Mathematics, Volume 81 N0. 1 2012, 65-79
12. F. Bao, R.H. Deng, H.Zhu, Variations of Diffie-Hellman Problem, Variations of Diffie-Hellman Problem, International Conference on Information and Communications Security ICICS 2003: Information and Communications Security, 301-312
13. N.Jacobson, Basic Algebra II, 2nd ed. New York: W. H.Freeman,p-196, 1989
14. B. Worthington, An Introduction to Hill Ciphers Using Linear Algebra, University of North Texas MATH 2700.002, October 26, 2010
15. M.Kosters, Injective Modules and the Injective Hull of a Module, November 27, 2009

AUTHORS' PROFILE

Wannarisuk Nongbsap, I am working as an Assistant Professor, in the department of Mathematics, St. Anthony's College, Shillong , Meghalaya, India. I have finished my M.Phil on the topic "Rings over which some classes of Modules are injective- A Survey". My topic of research , at the moment, is on m-injective rings and their applications in Cryptography. So far, we have seen the applications of finite fields in Cryptography. The idea of m-injective rings is itself very new. So this area of research is different from other topics and I hope that this paper paves way to other papers that are related to this field.

Dr. Madan Mohan Singh, I am working as an Associate Professor, in the Department of Basic Sciences and Social Sciences, School of Technology, North Eastern Hill University, Shillong , Meghalaya, India. I have also worked for 30 years in the Department of Mathematics, Pachhunga University College, NEHU, Aizawl, Mizoram, India. My areas of interest are Number Theory, Algebraic Number Theory, Graph Theory, Numerical Analysis and Discrete Mathematics. I have been a reviewer of The Mathematical Reviews , published by American Mathematical Society(AMS). I have many publications in both National and International Journals. I am a life member of the Indian Mathematical Society (IMS), Indian Science Congress Association (ISCA), Assam Mathematical Society, Cryptography Research Society of India(CSRI), Bona Mathematica and Indian Institute of Public Administration(IIPA).