Malaya Journal of Matematik, Vol. 9, No. 1, 130-135, 2021

https://doi.org/10.26637/MJM0901/0022

A public key Cryptography based on the m-injectivity of Z_{pq} over itself

Wannarisuk Nongbsap[1]* and Madan Mohan Singh[2]

Abstract

In this paper, we present a new public key scheme which is based on factoring, RSA encryption, proposed by Rivest-Shamir-Adleman(1978) [5]and discrete logarithm problem(DLP) [6], proposed by Diffie and Hellman[15], particularly, known as the Computational Diffie-Hellman Problem (CDH)[17]. The idea of DLP was mainly applied to groups, Finite fields and Elliptic Curves but in this paper, we are going to apply it to a particular ring Z_{pq}, where p and q are two large primes. The encryption and decryption processes of the proposed scheme uses the Elgamal encryption scheme related to DLP. Also, the proposed system benefits from the fact that this ring is m-injective over itself i.e, the existence of many R-monomorphisms from this ring to itself, which are subjected to certain conditions.

Keywords

m-injective, R-monomorphisms, Public Key Cryptography, RSA Cryptosystem, Discrete Logarithm Problem, Computational Diffie-Hellman Problem.

MSC 2010 Classifications:

94860, 14G50, 11T71, 68P25, 81P94.

[1] *Department of Mathematics, St. Anthony's College-793001, India.*

[2] *Department of Basic Sciences and Social Sciences, North-Eastern Hill University, Shillong-793022, India*

***Corresponding author**: [1]wnongbsap@gmail.com; [2]mmsingh2004@gmail.com

Article History: Received **24** January **2020**; Accepted **09** September **2020**

Contents

1. Introduction

We have the following definitions. Let R be a ring with identity element. A left ideal I of R is a subgroup of R with respect to addition and for any $x \in I$ and $r \in R$, $rx \in I$. 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 $\forall m_1, m_2 \in M$[2]. 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)$h(rx) = rh(x)$, $\forall r \in R$([2],[3]).

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 $g_o\alpha = f$[18]. 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 $f : A \longrightarrow E$ 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 rings which are m-injective over themselves is an extension of the concept of Self injective rings which was introduced by Y. Utumi [4] in the year 1965. In [4], Utumi studied the proper-

ties of commutative rings which are injective over themselves. In this paper, $R = Z_{pq}$ is a finite commutative ring.

A public key cryptography or asymmetric cryptography is a cryptographic system that uses two types of keys, viz, public keys which may be disseminated widely and private keys known only to the owner. One of the problems used in this paper is RSA, based on factoring. It stands on the idea that for a known value e relatively prime to $\phi(n)$(Euler's totient function), there exists inverse d of e modulo $\phi(n)$. Computing $\phi(n)$ is difficult without the knowledge of the prime factors of n and thus d remains untraced by an attacker. The second problem used here is the discrete logarithm problem, particularly, the Computational Diffie-Hellman Problem i.e given two known values h and t such that $h = t^s (mod\ n)$, it is difficult to find s[12] and knowing t, t^s, t^k modulo n, it is difficult to find t^{sk} modulo n. In this paper, $n = pq$ is a product of two primes, just like the one which was first used in [11]. Before proposing our public key scheme, we would like to prove the following results based on the m-injectivity of Z_{pq}.
Notation:-$\bar{x}$ used in this paper will denote the integer x modulo n and $\langle \bar{x} \rangle$ will denote the ideal generated by $\bar{x}$.

2. Results and Discussion

Proposition 2.1. *Let $n \geq 2$. Consider $Z_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$. Let $x, y \in \{1, 2, 3, ..., n-1\}$*
(i)If $\langle \bar{x} \rangle = \langle \bar{y} \rangle$ then $gcd(x,n) = gcd(y,n)$
(ii)If $gcd(x,n) = a$ then $\langle \bar{x} \rangle = \langle \bar{a} \rangle$ and $a|n$

Proof. (i) Let $g = gcd(x,n)$ then $g|x$ and $g|n$ and also $g = xl + nk$ for some $l, k \in Z$. This implies that $\bar{g} = \bar{x}\bar{l} + \bar{n}\bar{k} = \bar{x}\bar{l} \in \langle \bar{x} \rangle = \langle \bar{y} \rangle$. This shows that $\bar{g} = \bar{y}\bar{p}$, for some $\bar{p} \in Z_n$. From this, we get $n|g - yp \Rightarrow g - yp = nq$, for some $q \in Z$. This implies that $g = nq + yp \Rightarrow g|y$. For if $g \nmid y$ then there exists $s, r \in Z$ such that $y = gs + r$, where $r < g$. This implies that $\overline{gs+r} = \bar{y} \in \langle \bar{y} \rangle = \langle \bar{x} \rangle$. This shows that $\overline{gs+r} = \bar{x}\bar{t}$, for some $\bar{t} \in Z_n$. This implies that $n|(gs + r - xt)$. Since $g|n \Rightarrow g|(gs + r - xt) \Rightarrow g|r$, which is a contradiction. Hence, $g|y$ and therefore, $g|gcd(y,n)$ i.e, $gcd(x,n)|gcd(y,n)$. Similarly, we can show that $gcd(y,n)|gcd(x,n)$. Hence, the result.
(ii)$gcd(x,n) = a \Rightarrow a|x \Rightarrow x = ar \Rightarrow \bar{x} = \bar{a}\,\bar{r} \subseteq \langle \bar{a} \rangle$, for some $r \in Z$.
Hence, $\langle \bar{x} \rangle \subseteq \langle \bar{a} \rangle$. Also, $a = xl + nk$, for some $l, k \in Z$. This implies that $\bar{a} = \bar{x}\bar{l} + \bar{n}\bar{k} = \bar{x}\bar{l} \in \langle \bar{x} \rangle$. This shows that $\langle \bar{a} \rangle \subseteq \langle \bar{x} \rangle$ hence, they are equal and clearly $a|n$. □

We can generalise the above two results to get a proposition below:-

Proposition 2.2. *If $\langle \bar{x}_1 \rangle = \langle \bar{x}_2 \rangle = \langle \bar{x}_3 \rangle = ... = \langle \bar{x}_t \rangle$ in Z_n then*
(i)$gcd(x_1,n) = gcd(x_2,n) = gcd(x_3,n) = ... = gcd(x_t,n) = a$(say)
(ii)$\langle \bar{a} \rangle = \langle \bar{x}_1 \rangle = \langle \bar{x}_2 \rangle = ... = \langle \bar{x}_t \rangle$, where $x_1, x_2, ..., x_t \in \{1, 2, 3, ..., n-1\}$ and $a|n$

Let us take a nonzero proper ideal A of Z_n. Suppose $A = \langle \bar{x}_1 \rangle = \langle \bar{x}_2 \rangle = \langle \bar{x}_3 \rangle = ... = \langle \bar{x}_t \rangle$ and let $a = gcd(x_1,n) = gcd(x_2,n) = gcd(x_3,n) = ... = gcd(x_t,n)$ then by the above arguments, $A = \langle \bar{a} \rangle$ and $a|n$.

Lemma 2.3. *Let $A = \langle \bar{a} \rangle$ be an ideal of Z_n as taken above and let $f : A \longrightarrow Z_n$, $n \geq 2$, be a monomorphism. Let $f(\bar{a}) = \bar{b}$ for some $\bar{b} \in Z_n, \bar{b} \neq \bar{0}$ then*
(i)$a|b$
(ii)If $b|n$ then $b = a$
(iii)$gcd(\frac{n}{a}, \frac{b}{a}) = 1$
(iv)If a is prime then $gcd(n, \frac{n}{a} + \frac{b}{a}) = 1$ or a
(v)If a is prime such that $gcd(n, \frac{n}{a} + \frac{b}{a}) = a$ then $gcd(n, \frac{b}{a}) = 1$
(vi)For a prime a, $gcd(n, \frac{n}{a} + \frac{b}{a}) = 1$ if and only if $a^2 \nmid n + b$
(vii)For a prime a, $gcd(n, \frac{b}{a}) = 1$ if and only if $a^2 \nmid b$

Proof. (i)$\bar{0} = f(\bar{0}) = f(\bar{n}) = f(\overline{\frac{n}{a}a}) = \overline{(\frac{n}{a})} f(\bar{a}) = \overline{(\frac{n}{a})}\bar{b} = \overline{(\frac{n}{a}b)}$.
This implies that n divides $\frac{n}{a}b$. Hence, a divides b.
(ii)Suppose b divides n then $n = bx$ for some $x \in Z$. Now, $f(\bar{a}\bar{x}) = \bar{b}\bar{x} = \bar{n} = \bar{0}$. Since f is a monomorphism, $\bar{a}\bar{x} = \bar{0}$. This implies that $n|ax$ which gives $ax = nt = bxt$ and hence $a = bt$. This shows that $b|a$. From (i) we get $a = b$.

(iii)Let $g = gcd(\frac{n}{a}, \frac{b}{a})$ then $g|\frac{n}{a}$ and $g|\frac{b}{a}$.
So, $\frac{n}{a} = gk$ and $\frac{b}{a} = gl$, for some $k, l \in Z$. This implies that $n = agk$ and $b = agl = a\frac{n}{ak}l = \frac{nl}{k} \Rightarrow bk = nl \Rightarrow n|bk$.
Again, $\bar{0} = \overline{bk} = f(\bar{a})\bar{k} = f(\overline{ak})$. Since f is one-one, we have $\overline{ak} = \bar{0}$.
Hence, $n|ak \Rightarrow agk|ak \Rightarrow g|1 \Rightarrow g = 1$.

(iv)Let $g = gcd(n, \frac{n}{a} + \frac{b}{a})$ then $g|n$ and $g|\frac{n}{a} + \frac{b}{a}$. This implies that $g|n + b$ showing that $g|b$. By (iii), we have $g|a$, therefore, $g = 1$ or $g = a$.

(v)This can be done using (iii).

(vi)Suppose $gcd(n, \frac{n}{a} + \frac{b}{a}) = 1$. If possible, let us assume that $a^2 \mid n + b$ then $a|\frac{n}{a} + \frac{b}{a}$. Since $a|n$, we have $a|1$, which is impossible.
Conversely, suppose $a^2 \nmid n + b$ then $a \nmid \frac{n}{a} + \frac{b}{a}$. Let $g = gcd(n, \frac{n}{a} + \frac{b}{a})$. Following the same steps as in (iv), we find that $g = 1$ or $g = a$. Suppose $g = a$, since $a \nmid \frac{n}{a} + \frac{b}{a}$, this implies that $g \nmid \frac{n}{a} + \frac{b}{a}$ which is a contrary to our assumption.

Hence, g=1.
(vii)Proof of (vii) is similar to the proof of (vi). □

Proposition 2.4. *If a divides b, where b is nonzero element of Z_{pq} then $f : \langle\bar{a}\rangle \longrightarrow Z_{pq}$ defined by $f(\bar{a}) = \bar{b}$, is an R-monomorphism.*

Proof. Let $\bar{x} \in Zpq$ then $f(\bar{x}\bar{a}) = \bar{x}\bar{b}, \forall \bar{x}\bar{a} \in \langle\bar{a}\rangle$. Clearly, f is an R-homomorphism. Suppose $f(\bar{x}\bar{a}) = \bar{0}$. Since a divides b, there exists $s \in Z$ such that $b = as$. Now, $a|pq$, therefore, $a = p$ or $a = q$. Suppose $a = p$. Suppose $\overline{xb} = \bar{0}$ then $pq|xb \Rightarrow pq|xps \Rightarrow q|xs$. Since q is prime, then $q|x$ or $q|s$. Suppose $q|x \Rightarrow pq|px \Rightarrow pq|ax \Rightarrow \overline{ax} = \bar{0}$. Suppose $q|s \Rightarrow q|ps \Rightarrow q|b$. Since p and q are relatively prime, we have $pq|b$, which is impossible as $\bar{b}$ is nonzero. Hence, f is one-one and therefore, f is an R-monomorphism. □

With the above results, we are now in a position to prove the following theorem.

Theorem 2.5. *Z_{pq}, where p and q are not necessarily distinct, is m-injective over itself.*

Proof. Let A be an ideal of Z_{pq} and $f : A \longrightarrow Z_{pq}$ be a left R-monomorphism . Suppose $A = 0$ then taking $g : Z_{pq} \longrightarrow Z_{pq}$ to be the identity map, we find that g is a left R- monomorphism extending f.
Suppose $A = Z_{pq}$ then taking $g : Z_{pq} \longrightarrow Z_{pq}$ to be equal to f, we find that g is a left R-monomorphism extending f. Suppose A is a nonzero proper ideal of Z_{pq}. Then $A = \langle\bar{a}\rangle$ where $\bar{a} \neq 0$ and $a = p$ or $a = q$. Let $f : A \longrightarrow Z_{pq}$ be a left R-monomorphism defined by $f(\bar{a}) = \bar{b}$ where $\bar{b} \neq 0$.
We define $g : Z_{pq} \longrightarrow Z_{pq}$ by

$$g(\bar{x}) = \begin{cases} \overline{(\frac{pq}{a} + \frac{b}{a})}\bar{x}, & \text{if } (pq, \frac{pq}{a} + \frac{b}{a}) = 1 \\ \overline{(\frac{b}{a})}\bar{x}, & \text{if } (pq, \frac{pq}{a} + \frac{b}{a}) = a \end{cases}$$

Clearly, g is a well-defined left R homomorphism which extends f. For the first case, if $\bar{x} \in Kerg \Rightarrow g(\bar{x}) = \bar{0} \Rightarrow \overline{(\frac{pq}{a} + \frac{b}{a})}\bar{x} = \bar{0} \Rightarrow pq|(\frac{pq}{a} + \frac{b}{a})x$.
Since $gcd(pq, \frac{pq}{a} + \frac{b}{a}) = 1 \Rightarrow pq|x \Rightarrow \bar{x} = \bar{0}$ showing that g is one-one. Similarly, we can prove for the second case also. (by (iv) and (v)). Therefore, g is a left R-monomorphism. □

It is to be noted that since g is a one-one function from a finite set to itself, it will be bijective and hence it will have an inverse.

Before proposing our scheme, we would like to state the following result which is due to the Chinese Remainder Theorem[10].

Proposition 2.6. *Let $gcd(a,b) = 1$ and $c > 0$ then there exists an integer x such that $gcd(a + bx, c) = 1$*

The above result is used in the proposed scheme, in step 7.

The proposed Public Key Scheme

A user X who wants to create public and private keys has to do the following steps:-
1. Choose two large and distinct primes p and q.
2. Compute $n = pq$.
3. Compute $\phi(n) = (p-1)(q-1)$
4. Take a such that $1 < a < n$, $a|n$ and consider the ideal generated by $\bar{a}$.
5. Choose a monomorphic image $\bar{b} \in Z_n$ of $\bar{a}, b \in \{2,3,4,...,n-1\}$ such that $a^2 \nmid (n+b)$ and $b \neq a$.
6. Compute $t = \frac{n}{a} + \frac{b}{a}$.
7. Choose $z \geq 1$ such that $(n+tz, \phi(n)) = 1$ and let $e = n+tz$.
8. Compute d such that $ed \equiv 1(mod\ \phi(n))$.
9. Choose $s \geq 1$ such that t^s is not congruent to $1(mod\ n)$ and compute $h \equiv t^s(mod\ n)$

The public keys of X are (n,t,h,e) and the private keys are (s,d) .

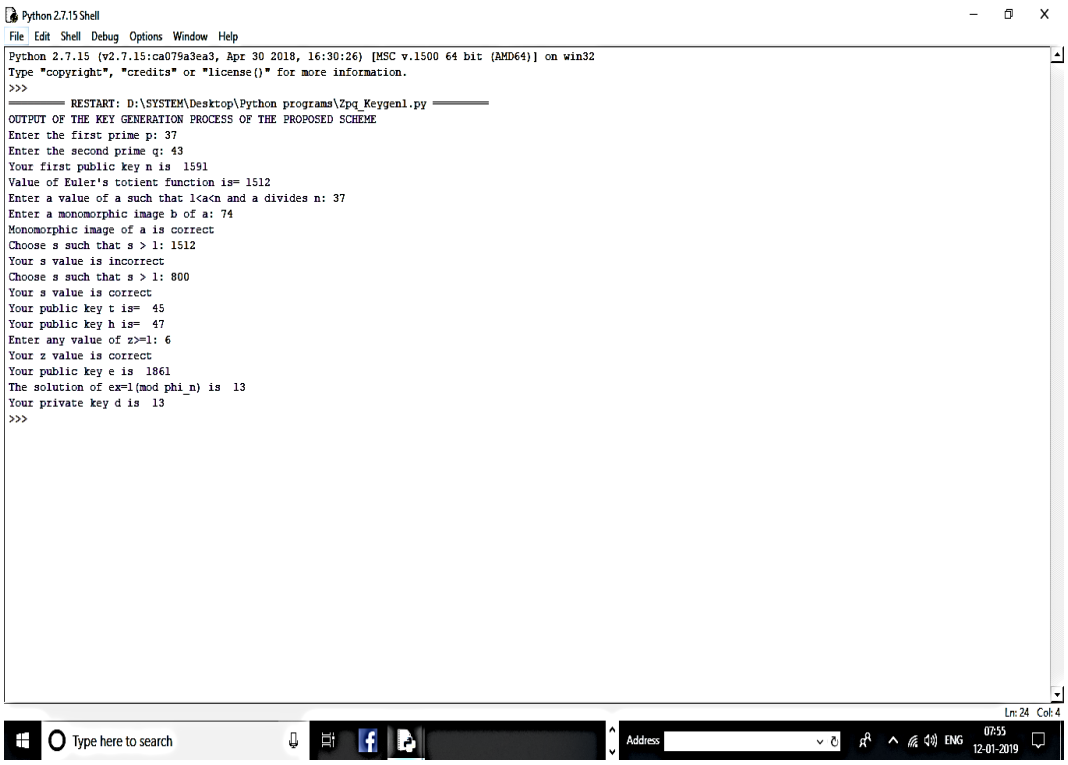
Encryption
The plaintext space is Z_n. Suppose another user Y wants to send a message $\bar{m} \in Z_n$ to X using $X's$ public key then Y will have to do the following steps:-
1. Choose integer k such that t^k is not congruent to $1(mod\ n)$
2. Compute $r \equiv t^k(mod\ n)$.
3. Compute $c = h^k m^e(mod\ n)$
Y sends to X the encrypted message (r,c)

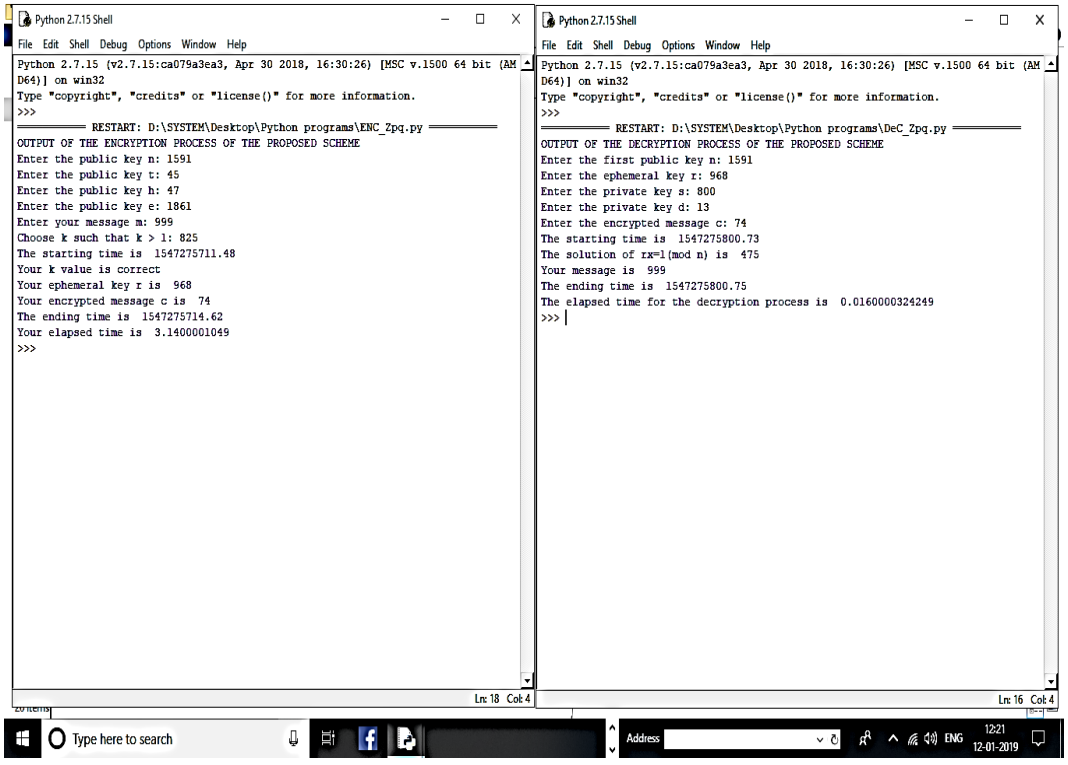
Decryption
For the decryption of the message c, X should compute $m \equiv c^d(r^{-1})^{sd}(mod\ n)$, using private keys s and d.
Thus, X recovers the encrypted message $\overline{m}$.
Let us take an example of p and q, as taken in [5], to see how the algorithm is implemented.

Example 2.7. *Suppose $p = 37, q = 43$ then $n = 1591$ and $\phi(n) = 36 \times 42 = 1512$. Suppose $a = 37$, $b = 74$ then $37^2 = 1369 \nmid 1591 + 74 = 1665$ and therefore, $t = 45$. Since $gcd(t,n) = 1$, by [10], there exists an integer z such that $(n+tz, \phi(n))$=1. Choose $z = 6$ then $e = n+tz = 1861$, which is relatively prime to 1512. Using Euclidean Extended algorithm to solve for $1861d \equiv 1(mod\ 1512)$, we get $d = 13$. Now taking $s = 800$, we get $h = 47$.*
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.

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

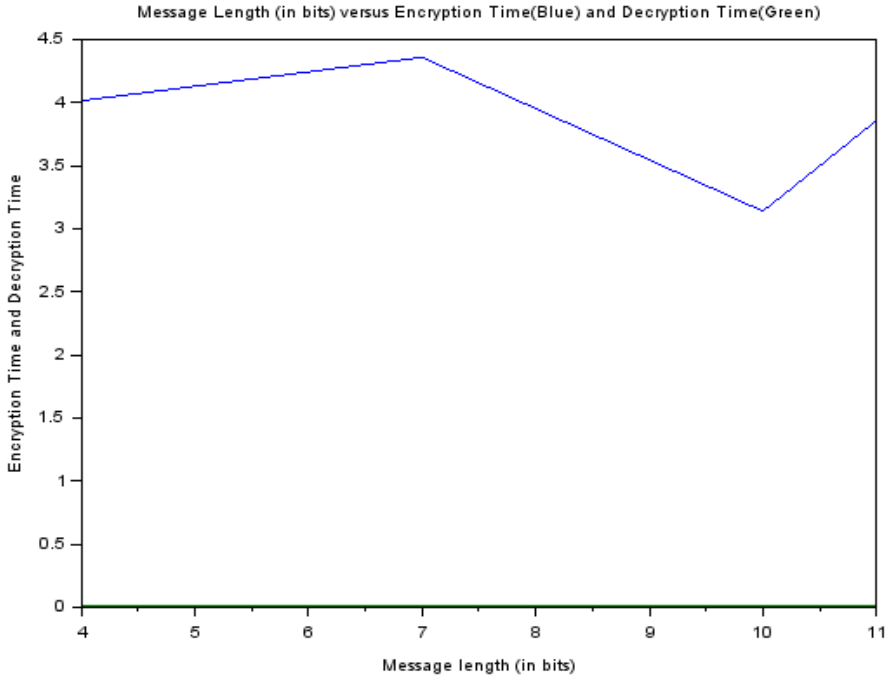
RECORDS OF ELAPSED TIMES





The given table shows that there is a difference between the encryption time and decryption time. The encryption time is a bit lengthy because the one who encrypts the message has to check that the ephemeral key r is not equal to 1 modulo n. The decryption time is almost negligible. With the increase in the message length, the decryption time goes on increasing but nothing can be said about the encryption time as it keeps on fluctuating. This can be seen clearly seen in the given graph. The graph also shows that the curve of the decryption process is almost coinciding with the X-axis.

Message(m)	Length(in bits)	Encrypted Message(c)	Encryption time(in ms)	Decryption time(in ms)
9	4	423	4.01600003242	0.0149998664856
99	7	1434	4.35899996758	0.0150001049042
999	10	74	3.1400001049	0.0160000324249
1590	11	591	3.85899996758	0.0160000324249



3. Security of the scheme

The security of this proposed scheme is based on integer factorization problem and Discrete Logarithm Problem, particularly CDH. The encryption and decryption of the scheme is partly based on the Elgamal Encryption scheme using DLP([12],[17]). An adversary who tries to find the private key d will have to find $\phi(n)$ first, which is an impossible task, for a large n, unless he/she knows the factors of n. Again, the private key s has been chosen randomly which is another disadvantage to the adversary and thus increases the security of the scheme. The size of n chosen for the proposed scheme should be a minimum of 2048 bits (617 decimal digits) as choosing size of n of at least 1024 bits could retrieve the factors of n in the near future. So, depending on the size of n, the size of p and q should be at least 1024 bits long. Also, taking a large n can somewhat delay the time of factorizing it via, Polland Rho method or the New Factorization (NF) method[13]. Moreover, larger size of n can also resist brute force attack. Again, p and q are to be taken in such a way that they do not permit the applications of known algorithms like the number field sieve method and that they do not give rise to the use of Euclidean Extended algorithm to solve for d in the congruence $ed \equiv 1(mod\ \phi(n))$. If $d < n^{0.5}$ then there is a chance of retrieving d[14]. So, the value of e should be such that the value of d is greater than $n^{0.5}$. Even though t and n are public but this will not reveal the factors of n because the equation $t = \frac{n}{a} + \frac{b}{a}$ contains two unknowns and so is difficult to solve. In the key generation process, s should be chosen in such a way that it does not take any value which is the order of t modulo n or any multiple of the order of t modulo n otherwise, the value of h will be 1 and the whole problem will be reduced to just one hard problem. The same applies to k in the encryption process. Again, taking large n can also resist attacks on the Discrete Logarithm problem used in this paper. Such attacks are the brute force attack, Shank's Baby-step Giant-step, Pollard's Rho method, Index Calculus Method [16]. Suppose a sender wants to find m directly then he/she will have to compute $h^{k^{-1}}$ modulo n which is an impossible task because k is not revealed to anyone except to the sender of the message. But even if $h^{k^{-1}}$ is known then also an attacker has to find d to know m. So, this scheme is semantically secured]. Hence, this scheme is equally secured as the other schemes based on RSA cryptosystem and the discrete logarithm problem. Since the parameter k is chosen by the sender, so for sending different messages $c_1 = h^k m_1^e (modn)$ and $c_2 = h^k m_2^e (modn)$, even if the same k is used, the above

two problems reduce to $m_2^e \equiv c_2^{-1} c_1 m_1^e (mod n)$, which does not give the value of m_2 even if m_1 is known to the attacker because the private key d is unknown to him/her. So the sender can safely use the same parameter k unlike in [7].

4. Performance Analysis

The encryption algorithm of the proposed scheme requires three modular exponentiations, viz, t^k, h^k and m^e. One modular multiplication of the last two exponentiations is also required. Thus, the encryption process requires three modular exponentiations and one modular multiplication. This is more efficient than the scheme proposed in [8] which requires six modular exponentiations and four modular multiplications. The decryption process requires one application of Extended Euclidean algorithm for finding the inverse of the ephemeral key r, two modular exponentiations,viz, c^d and $(r^{-1})^{sd}$ and one modular multiplication of the two exponentiations. The decryption scheme is as efficient as the scheme proposed in [9].

5. Conclusion and Future Works

In this paper, we introduced the concept of m-injective Rings to create a Public key Cryptosystem. This property of Z_{pq} of being m-injective over itself helped in the creation of a public key t which is relatively prime to n. The idea of congruence and the application of Chinese Remainder Theorem helped in the creation of another public key e which is relatively prime to $\phi(n)$ thus making it as efficient as the RSA Cryptosystem. Again, the property of t, being relatively prime to n, created another way to the application of the Elgamal encryption scheme using Discrete Logarithm Problem. So the whole scheme involves around the idea of two hard problems, viz, RSA Cryptosystem and DLP (CDH) making the proposed scheme as efficient as the other existing schemes.

The property of Z_{pq} of being m-injective over itself paved way to the creation of this proposed scheme. Hence, our future work will include findings of more rings which are m-injective over themselves and creating public key cryptographic schemes out of them based on some other hard problems.

References

[1] R. Baer, Abelian Groups that Are Direct Summands of Every Containing Abelian Group, *Bull. Amer. Math. Soc.,* 46(1940), 800–806.

[2] C. Faith, *Algebra: Rings, Modules and Categories, I*, Berlin, p. 157, 1973.

[3] T. Y. Lam, *Lectures on Modules and Rings*, New York: Springer-Verlag, p. 63, 1999.

[4] Y. Utumi, On Continuous Rings and Self Injective Rings,1965, University of Rochester, Rochester, New York, (1965), 158–173.

[5] E. Milanov, *The RSA Algorithm*, 3 June 2009.

[6] K.S. McCurley, The Discrete Logarithm Problem, Proceedings of Symposia in Applied Mathematics, Volume 42, 1990

[7] P. Goswami, M.M.Singh, B.Bhuyan, A New Public Key Scheme based on Integer Factorization and Discrete Logarithm, *Palestine Journal of Mathematics*, 6(2)(2017), 580-584

[8] D. Poulakis, A Public Key Encryption Scheme Based on Factoring and Discrete Logarithm, *Journal of Discrete Mathematical Sciences and Cryptography*, 12:6(2009), 745–752.

[9] 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)

[10] I. Niven, H.S. Zukerman, H.L. Montgomery, *An Introduction to the Theory of Numbers*, Fifth Edition, John Wiley and Sons, Inc., p.73, 2000

[11] K.S.McCureley, A key distribution system equivalent to factoring, *Journal of Cryptography*, 1:2(1988), 95–106.

[12] T.Elgamal, A public Key Cryptosystem and a Signature scheme based on discrete Logarithms, *Journals and Magazine > IEEE Transactions on Information Theory*, 31(4)(1985), 409–472.

[13] B.R. Ambedkar, S.S. Bedi, A New Factorization Method to Factorize RSA Public Key Encryption, *IJSCI International Journal of Computer Science*, 8(6:1)(2011), 242–247.

[14] D.Boneh, G. Durfee, Cryptanalysis of RSA with Private Key d less than $N^{0.292}$, Computer Science Department, Stanford University, CA 94305-9045.

[15] W. Diffie, M. Hellman, New Directions in Cryptography, *IEEE Trans. Inform. Theory*, 22(1976), 472–492

[16] K. Rabah, Security of the Cryptographic Protocols Based on Discrete Logarithm Problem, *Journal of Applied Sciences*, 5(9)(2005), 1692–1712.

[17] F. Bao, R.H. Deng, H.Zhu, Variations of Diffie-Hellman Problem, Variations of Diffie-Hellman Problem, Infocomm Security Department, Institute for Infocomm Research. 21 Heng Mui Keng Terrace, Singapore 119613

[18] M. Kosters, *Injective Modules and the Injective Hull of a Module*, November 27, 2009.

★★★★★★★★★
ISSN(P):2319 – 3786
Malaya Journal of Matematik
ISSN(O):2321 – 5666
★★★★★★★★★