Malaya Journal of Matematik, Vol. 8, No. 2, 459-463, 2020

https://doi.org/10.26637/MJM0802/0022

A design of public key Cryptosystem in an algebraic extension field over a finite field using the difficulty of solving DLP

M. I. Saju[1*], Renjith Varghese[2] and E.F. Antony John[3]

Abstract

Through this research paper, authors construct a public key cryptosystem which works in the finite algebraic extension field $\mathbb{F}_{p^n}$ of the finite field $\mathbb{F}_p$. The security of this system is based on difficulty of solving DLP in $\mathbb{F}_{p^n}{}^*$. The primitive polynomials are used in the construction of algebraic extension fields. In this system all users select commonly a primitive polynomial $f(x)$ of degree n over the finite field $\mathbb{F}_p$.The prime number p, the primitive polynomial $f(x)$, encryption rule and decryption rule are given to the public, and all other features kept secret. In this system each character is treated as a polynomial of degree less than n over $\mathbb{F}_p$. After the encryption the character divided into two parts. The first part is sent to the other and the second part is used for the decryption. In this system we use similar procedure of ElGamal Exchange Cryptosystem. But our system has used more parameters than the ElGamal Exchange Cryptosystem. Hence our proposed system is more secure than ElGamal Exchange PKC.

Keywords

Cryptosystem, Cyclic Group, Discrete Logarithm Problem, Extension Field, Primitive Polynomial, Sub-exponential Algorithms.

AMS Subject Classification

35R11, 93E24, 65H20.

[1,2,3]*Department of Mathematics, St. Thomas' College, Calicut, Thrissur, Kerala, India.*

*****Corresponding author**: [1] sajumambilly@gmail.com; [2]renjithvarghese8@gmail.com; [3]antonyjohnef@gmail.com

Article History: Received **25** November **2019**; Accepted **06** March **2020**

Contents

1. Introduction

In 1976, Diffie and Hellman published their new famous paper[1] entitled 'New Directions in Cryptography'. In this paper then formulated the concept of the public key cryptography and made several ground-breaking contributions to this new field. The Diffie-Hellman publication was an extremely important event- it set forth the basic definitions and goals of a new field of mathematics/computer science. The public key cryptosystems are based on hard mathematical problems like factorization problem, DLP, Knapsack problem *etc*.

The components of PKC are one-way functions and trapdoor information. A one-way function is an invertible function that is easy to compute, but whose inverse is difficult to compute. Secure PKCs are built using one-way functions that have a trapdoor. The trapdoor is a piece of auxiliary information that allows the inverse to be easily computed. In this system the classical mathematical one way problem DLP is used.[2]

The extensively used asymmetric cryptography techniques *viz.* RSA (Rivest Shamir and Adleman) signature sending cryptosystem, Diffie-Hellman key exchange cryptosystem, DSA (Digital Signature Algorithm), ECC (Elliptic curve cryptography), ElGamal and Momusi Amere cryptosystem are also reviewed before proposing this system.[2]

In this study, the authors propose a novel cryptosystem, which works in the finite extension field of $\mathbb{F}_p$. In the first section, we explain mathematical prerequisite to appreciate the current study and section II narrates the designs of the system. Section III design the system with more than two primitive polynomials, section IV deals with results and discussion of the proposed work and finally, section V wraps up the study with a conclusion.

2. Mathematical Prerequisite

A field $\mathbb{F}$ is a commutative ring with unity without zero divisors and every nonzero element has multiplicative inverse in it. A finite field is a field with finite number of elements. The characteristic of a field is a smallest positive integer m such that $ma = 0$, for all $a \in \mathbb{F}$. The characteristic of a finite field is a prime number. For a prime number p, there is a field having p elements, this field is denoted by $\mathbb{F}_p$. If $f(x)$ is an irreducible polynomial of degree n over the finite field $\mathbb{F}_p$, then the quotient ring $\frac{\mathbb{F}_p[x]}{(f(x))}$ is a finite field with p^n elements. For each natural number $n > 1$ and a prime p, there is a finite field having p^n elements and this field is a finite extension field of $\mathbb{F}_p$. If $f(x)$ is a primitive polynomial over $\mathbb{F}_p$, then it is an irreducible polynomial and its roots generate the finite field $\frac{\mathbb{F}_p[x]}{(f(x))}$. This extension field is known as algebraic extension field over the finite field $\mathbb{F}_p$ with single parameter x and it is denoted by $\mathbb{F}_{p^n}$[3]. There are $\frac{\varphi(p^n-1)}{n}$ primitive polynomials over the finite field $\mathbb{F}_p$ of degree n, where φ is Euler's totient function [4]. If α is one of the roots of the primitive polynomial $f(x)$ then its other roots are $\alpha^{p^1}, \alpha^{p^2}, \alpha^{p^3}, \ldots, \alpha^{p^{n-1}}$. If α is a root of the primitive polynomial $f(x)$ in the extension field $\frac{\mathbb{F}_p[x]}{(f(x))}$, then it can be observed that there exist another primitive polynomial $f_k(x)$ such that α^k will be its root where $\gcd(p^n-1,k) = 1$ and α^k is not a root of $f(x)$. Choose a random n-bit number N and divide x^N by $f(x)$ and $f_k(x)$. The remainders are *viz.* $T(x)$ and $T_k(x)$ respectively, then

$$T(x) \equiv \left(T_k\left(x^k\right)\right)^{k^{-1}} (\bmod f(x)) \text{ and}$$
$$T_k(x) \equiv \left(T\left(x^{k^{-1}}\right)\right)^{k} (\bmod f_k(x)) .[5]$$

Let α be a primitive root for $(\mathbb{F}_{p^n})^* = \left(\frac{\mathbb{F}_p[x]}{(f(x))}\right)^*$ and $t(x)$ be a nonzero polynomial in $\mathbb{F}_{p^n}$. The DLP is the problem to finding an exponent k such that $\alpha^k \equiv t(x)(\bmod f(x))$. This problem is difficult because there are infinitely many values for k. [6][7][8][9][10]

No efficient general method for computing discrete logarithms on conventional computers is known till date and authors are of the view that implementing this concept in the proposed algorithms in public-key cryptography enhances its security on the assumption that the discrete logarithm problem over carefully chosen groups has no efficient solution because it works in the cyclic subgroup of an acyclic group. [11][12]

3. Designing the exchange Cryptosystem

Alice wants to send a message or key for use in symmetric cipher to Bob, but they knew that, every piece of information that they exchange is observed by their adversary Eve. How is it possible for Alice to send a key or message without making it available to Eve?

Here, there is a method, which is based on the difficulty of solving the DLP in $\mathbb{F}_{p^n}$.

The first step is for Alice and Bob to agree on a large prime p and a primitive polynomial $f(x) \in \mathbb{F}_p[x]$ of degree n. Alice and Bob make the prime p and the primitive polynomial $f(x)$ public knowledge.

The next step is for Alice to pick a secret number k_A such that $\gcd(p^n-1,k_A) = 1$. Also find a primitive polynomial $f_{k_A}(x)$ of degree n such that α^{k_A} is a root of $f_{k_A}(x)$.

Choose an n-bit number N_A and compute the following

$$x^{N_A} \equiv T_A(x)(\bmod f(x))$$
$$x^{N_A} \equiv T_{k_A}(x)\left(\bmod f_{k_A}(x)\right)$$

Then we have,

$$T_A(x) \equiv \left(T_{k_A}\left(x^{k_A}\right)\right)^{k_A^{-1}} (\bmod f(x)) \qquad (2.1)$$

$$\text{and } T_{k_A}(x) \equiv \left(T_A\left(x^{k_A^{-1}}\right)\right)^{k_A} \left(\bmod f_{k_A}(x)\right) \qquad (2.2)$$

Similarly, Bob picks a number k_B such that $\gcd(p^n-1,k_B) = 1$. Also find a primitive polynomial $f_{k_B}(x)$ of degree n such that α^{k_B} is a root of $f_{k_B}(x)$.

Choose an n-bit number N_B and compute the following

$$x^{N_B} \equiv T_B(x)(\bmod f(x))$$
$$x^{N_B} \equiv T_{k_B}(x)(\bmod f_{k_B}(x))$$

Then we have,

$$T_B(x) \equiv \left(T_{k_B}\left(x^{k_B}\right)\right)^{k_B^{-1}} (\bmod f(x)) \qquad (2.3)$$

and

$$T_{k_B}(x) \equiv \left(T_B\left(x^{k_B^{-1}}\right)\right)^{k_B} (\bmod f_{k_B}(x)) \qquad (2.4)$$

Table 1.1

Alice	**Bob**
Suppose Alice want to send the message $M(x)$ to Bob. For this compute $M(x)(T_A(x))^{-1}$ or $M(x)\left(T_{k_A}(x)\right)^{-1}$ and send this to Bob	
	Bob computes $M(x)(T_A(x))^{-1}(T_B(x))^{-1}$ or $M(x)\left(T_{k_A}(x)\right)^{-1}(T_{k_B}(x))^{-1}$ and send back to Alice
Alice computes $M(x)(T_A(x))^{-1}(T_B(x))^{-1}\left(T_{k_A}\left(x^{k_A}\right)\right)^{k_A^{-1}} =$ $M(x)(T_B(x))^{-1}$ or $M(x)\left(T_{k_A}(x)\right)^{-1}(T_{k_B}(x))^{-1}\left(T_A\left(x^{k_A^{-1}}\right)\right)^{k_A} =$ $M(x)(T_{k_B}(x))^{-1}$ and send this to Bob.	
	Bob Computes $M(x)(T_B(x))^{-1}\left(T_{k_B}\left(x^{k_B}\right)\right)^{k_B^{-1}} = M(x)$ or $M(x)(T_{k_B}(x))^{-1}\left(T_B\left(x^{k_B^{-1}}\right)\right)^{k_B} = M(x),$ Bob receives the message $M(x)$.

4. Design the exchange message Cryptosystem with more than two primitive polynomials

Alice chooses numbers k_{A_i} such that $\gcd\left(p^n-1,k_{A_i}\right)=1$ and $\alpha^{k_{A_i}}$ be the root of the primitive polynomial $f_{k_{A_i}}(x)$ of degree n where $i=1,2,\ldots,r_A$. Choose an n-bit number N_A and compute the following

$$x^{N_A} \equiv T_A(x)(\bmod f(x))$$
$$x^{N_A} \equiv T_{k_{A_i}}(x)\left(\bmod f_{k_{A_i}}(x)\right), i=1,2,\ldots,r_A$$

Then we have,

$$T_A(x) \equiv \left(T_{k_{A_i}}\left(x^{k_{A_i}}\right)\right)^{k_{A_i}^{-1}} (\bmod f(x)), i=1,2,\ldots,r_A \qquad (3.1)$$

and

$$T_{k_{A_i}}(x) \equiv \left(T_A\left(x^{k_{A_i}^{-1}}\right)\right)^{k_{A_i}} \left(\bmod f_{k_{A_i}}(x)\right), i=1,2,\ldots r_A \qquad (3.2)$$

Multiplying the congruences (3.1), we have

$$(T_A(x))^{r_A} = \left(T_{k_{A_1}}\left(x^{k_{A_1}}\right)\right)^{k_{A_1}^{-1}} \left(T_{k_{A_2}}\left(x^{k_{A_2}}\right)\right)^{k_{A_2}^{-1}} \ldots$$
$$\left(T_{k_{A_{r_A}}}\left(x^{k_{A_{r_A}}}\right)\right)^{k_{A_{r_A}}{}^{-1}} (\bmod f(x)) \ (3.3)$$

Similarly, Bob chooses numbers k_{B_i} such that $\gcd\left(p^n-1,k_{B_i}\right)=1$ and $\alpha^{k_{B_i}}$ be the root of the primitive polynomial $f_{k_{B_i}}(x)$ of degree n , $i=1,2,\ldots,r_B$. Choose an n-bit number N_B and compute the following

$$x^{N_B} \equiv T_B(x)(\bmod f(x))$$
$$x^{N_B} \equiv T_{k_{B_i}}(x)\left(\bmod f_{k_{B_i}}(x)\right), i=1,2,\ldots,r_B$$

Then we have,

$$T_B(x) \equiv \left(T_{k_{B_i}}\left(x^{k_{B_i}}\right)\right)^{k_{B_i}^{-1}} (\bmod f(x)), i=1,2,\ldots,r_B \ (3.4)$$

and

$$T_{k_{B_i}}(x) \equiv \left(T_A\left(x^{k_{B_i}^{-1}}\right)\right)^{k_{B_i}} \left(\bmod f_{k_{B_i}}(x)\right), i=1,2,\ldots r_B \qquad (3.5)$$

Multiplying the congruences (3.4), we have

$$(T_B(x))^{r_B} = \left(T_{k_{B_1}}\left(x^{k_{B_1}}\right)\right)^{k_{B_1}^{-1}} \left(T_{k_{B_2}}\left(x^{k_{B_2}}\right)\right)^{k_{B_2}^{-1}} \ldots$$
$$\left(T_{k_{B_{r_B}}}\left(x^{k_{B_{r_B}}}\right)\right)^{k_{B_{r_B}}{}^{-1}} (\bmod f(x)) \ (3.6)$$

Table 1.2

Alice	Bob
Suppose Alice want to send the message $M(x)$ to Bob. For this compute $M(x)\left(T_A(x)\right)^{-r_A}$ and send this to Bob.	
	Bob computes $M(x)\left(T_A(x)\right)^{-r_A}\left(T_B(x)\right)^{-r_B}$ and send back to Alice.
Alice computes $M(x)\left(T_A(x)\right)^{-r_A}\left(T_B(x)\right)^{-r_B}\left(T_{k_{A_1}}\left(x^{k_{A_1}}\right)\right)^{k_{A_1}^{-1}}$ $\left(T_{k_{A_2}}\left(x^{k_{A_2}}\right)\right)^{k_{A_2}^{-1}}\ldots\left(T_{k_{A_{r_A}}}\left(x^{k_{A_{r_A}}}\right)\right)^{k_{A_{r_A}}{}^{-1}}$ $=M(x)\left(T_B(x)\right)^{r_B}$, by the result (3.3) and send this to Bob.	
	Bob Computes $M(x)\left(T_B(x)\right)^{r_B}\left(T_{k_{B_1}}\left(x^{k_{B_1}}\right)\right)^{k_{B_1}^{-1}}$ $\left(T_{k_{B_2}}\left(x^{k_{B_2}}\right)\right)^{k_{B_2}^{-1}}\ldots$ $\left(T_{k_{B_{r_B}}}\left(x^{k_{B_{r_B}}}\right)\right)^{k_{B_{r_B}}{}^{-1}}$, by the result (3.6) Bob receives the message $M(x)$.

5. Results and Discussions

5.1 Example

Suppose the primitive polynomial $f(x)=x^6+x^5+x^4+x+1\in\mathbb{F}_2[x]$ be the public parameter of the system.
Alice takes a number $k_A=29$, then the second primitive polynomial $f_{29}(x)=x^6+x^5+x^3+x^2+1$ and $k_A^{-1}=50$. She takes a 6-bit number $N_A=43$ and computes the following

$$x^{43}\equiv x^5+x^4(\bmod f(x)) \text{ and } x^{43}\equiv x^5+x^3+x^2\,(\bmod f_{29}(x))$$

Where $T_A(x)=x^5+x^4, T_{29}(x)=x^5+x^3+x^2, (T_A(x))^{-1}=x^5+x^4+x^2+1$ and $(T_{29}(x))^{-1}=x^4$

Suppose Alice wants to send the message
$M(x)=x^5+x^3+x+1$ to Bob.
For this Alice computes

$$\left\{M(x)\left(T_A(x)\right)^{-1}, T_{29}\left(x^{29}\right)\right\}=\left\{x^4+x^2, x^4+x^3+x+1\right\}$$

Alice sends $M_A(x)=x^4+x^2$ to Bob.
In the similar manner Bob takes the secret number $k_B=47$, then the second primitive polynomial
$f_{47}(x)=x^6+x^5+x^2+x+1$ and $k_B^{-1}=59$. He takes a 6-bit number $N_B=61$ and computes the following

$$x^{61}\equiv x^5+x^2+1(\bmod f(x)) \text{ and}$$
$$x^{61}\equiv x^5+x^3+x\,(\bmod f_{47}(x))$$

Where
$T_B(x)=x^5+x^2+1, T_{47}(x)=x^5+x^3+x, (T_B(x))^{-1}=x^2$ and $(T_{47}(x))^{-1}=x^4+x^3+x^2+x$
Bob computes

$$\left\{M_A(x)\left(T_B(x)\right)^{-1}, T_{47}\left(x^{47}\right)\right\}=$$
$$\left\{x^5+x+1, x^5+x^4+x^2+x+1\right\}$$

Bob sends $M_B(x)=x^5+x+1$ to Alice.
Alice Computes
$\left(x^5+x+1\right)\left(x^4+x^3+x+1\right)^{50}=x^5+x^4+x^3+1$
Bob computes
$\left(x^5+x^4+x^3+1\right)\left(x^5+x^4+x^2+x+1\right)^{59}=x^5+x^3+x+1$
and Bob receive the original message.

5.2. Example of Character Wise Transformation from Plain Text to Cipher Text

Key Creation Algorithm

Input

Degree of the polynomial: 8
The primitive polynomial:
$f(x) = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$
The secret key: $k = 113$.

Output

The public key is $x^{113} \equiv x^6 + x^5 + x^4 + x^3 + 1(\bmod f(x))$
The second primitive polynomial:
$f_{113}(x) = x^8 + x^6 + x^5 + x^4 + 1$
The inverse of k: $k^{-1} = 167$.

Encryption Algorithm

Input

The primitive polynomial:
$f(x) = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$
The second primitive polynomial:
$f_{113}(x) = x^8 + x^6 + x^5 + x^4 + 1$
The public key $g(x) \equiv x^6 + x^5 + x^4 + x^3 + 1(\bmod f(x))$
Ephemeral key number: $N = 123$
Plain Text: $M(x) = STJOSE$.

Output

Cipher Text: Hp :^{1} HX, X

Decryption Algorithm

Input

Cipher Text: Hp :^{1} HX, X
The inverse of k: $k^{-1} = 167$.

Output

Plain Text: $M(x) = STJOSE$

Table 1.3
Example of Character Wise Transformation from Plain Text to Cipher Text

Character	8-bit binary	M(x)	Encrypted polynomial	8-bit binary	Encrypted Character
S	01010011	$x^6 + x^4 + x + 1$	$x^6 + x^3$	01001000	H
T	01010100	$x^6 + x^4 + x^2$	$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$	11111110	p
J	01001010	$x^6 + x^2 + x$	$x^7 + x^2$	10000100	:
O	01001111	$x^6 + x^3 + x^2 + x + 1$	$x^7 + x^5 + x^4 + x^3 + 1$	10111001	^{1}
S	01010011	$x^6 + x^4 + x + 1$	$x^6 + x^3$	01001000	H
E	01000101	$x^6 + x^2 + 1$	$x^6 + x^4 + x^3$	01011000	X

5.3. Comparison of the Proposed Message Exchange Cryptosystem with ElGamal Message Exchange Public Key Cryptosystem

Table 1.4

ElGamal Message Exchange PKC	Proposed Message Exchange PKC
Alice and Bob fix a publicly known prime p and all other elements used are kept secret.	Alice and Bob fix a publicly known prime p and a primitive polynomial $f(x) \in \mathbb{F}_p[x]$ of degree n and all other numbers and polynomials used are kept secret
Alice takes her message M, and chooses a secret random exponent a such that $\gcd(a, p-1) = 1$ and sends the number $M^a(\bmod p)$ to Bob.	Alice takes her message $M(x)$ and chooses a secret number k_A such that $\gcd(p^n - 1, k_A) = 1$. Also find a primitive polynomial $f_{k_A}(x)$ of degree n such that α^{k_A} is a root of $f_{k_A}(x)$ and $f(\alpha) = 0$, Choose an n-bit number N_A and computes the following, $x^{N_A} \equiv T_A(x)(\bmod f(x))$ $x^{N_A} \equiv T_{k_A}(x)\left(\bmod f_{k_A}(x)\right)$ Computes $M(x)(T_A(x))^{-1}$ and sends this to Bob.
Bob chooses a secret random exponent b such that $\gcd(b, p-1) = 1$ and sends $(M^a)^b\,(mod p) = M^{ab}$ to Alice.	Bob picks a number k_B such that $\gcd(p^n - 1, k_B) = 1$. Also find a primitive polynomial $f_{k_B}(x)$ of degree n such that α^{k_B} is a root of $f_{k_B}(x)$. Choose an n-bit number N_B and computes the following, $x^{N_B} \equiv T_B(x)(\bmod f(x))$ $x^{N_B} \equiv T_{k_B}(x)(\bmod f_{k_B}(x))$ Computes $M(x)(T_A(x))^{-1}(T_B(x))^{-1}$ and sends this to Alice.
Alice then computes the inverse of a in modulo $p-1$ and then computes $\left(M^{ab}\right)^{a^{-1}}(mod p) = M^b$ and sends to Bob.	Alice computes $M(x)(T_A(x))^{-1}(T_B(x))^{-1}\left(T_{k_A}\left(x^{k_A}\right)\right)^{k_A^{-1}} =$ $M(x)(T_B(x))^{-1}$ and sends this to Bob.
Bob computes the inverse of b in modulo $p-1$ and then computes $\left(M^b\right)^{b^{-1}}(mod p) = M$ recovers the message of Alice.	Bob computes $M(x)(T_B(x))^{-1}\left(T_{k_B}\left(x^{k_B}\right)\right)^{k_B^{-1}} = M(x)$, recovers the message of Alice.

6. Conclusion

Strength of the cryptographic system solely depends on the underlying mathematical complexity and, many a times, it is not fully understood or appreciated by its typical users for varying reasons. Through the current study, authors studied commonly used Cryptosystems to propose a mathematical model that allows stealth security which is the need and demand of the hour. It was all the major features of the popular public key cryptosystem and the security of the system is as good as solving DLP over the finite field $\mathbb{F}_{p^n}$, hence the difficulty and complexity of the mathematical problem applies here too. The proposed system will secure the communication provided the degree of the primitive polynomial is sufficiently large and it also depends on selection of the ephemeral number and the prime number. The algorithms used here is sub-exponential and all the entries are polynomials, which add to the stealth of the system. Expected running time of these sub-exponential algorithms are of the form $O\left[\exp(c + o(1))(\ln q)^{\alpha}(\ln\ln q)^{1-\alpha}\right]$ where c is a positive constant and α is a constant satisfying $0 < \alpha < 1$. Our proposed system is secure when works in the field of size at least 2^{2048}. It is implemented and tested in mat lab to verify its potential for implementation in the open systems.
The following parameters are very important for the security of our proposed systems.

1. The size of the prime p is at least 2^{2048}.
2. The factors of $p-1$ contains large primes.

3. Different random ephemeral keys are used to encrypt different plain texts.

4. The size of the degree of the primitive polynomials used.

5. The intractability of the DLP in the multiplicative group $(\mathbb{F}_{p^n})^*$.

References

[1] Whitfield Diffie and Martin Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, 22(1976), 644–654.

[2] Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1994.

[3] Neal Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics, 3, 1998.

[4] Rudolf Lidl and Harald Niederreiter, *Finite Fields*, Cambridge University Press, 1997.

[5] MI Saju and PL Lilly, A method of designing a publickey cryptosystem based on discrete logarithm problem, *International Research Journal of Pure Algebra*, 4(2014), 628–630.

[6] MI Saju and PL Lilly, Application of function fields in a public key cryptosystem, *Journal of Theoretical and Computational Mathematics*, 1(2015), 52–55.

[7] MI Saju and PL Lilly, A digital signature and a new public key cryptosystem based on discrete logarithm problem over finite extension field of the field Fp, *International Organization of Science and Research Journal of Mathematics*, 11(2015), 32–35.

[8] MI Saju and PL Lilly, A method of designing block cipher involves a key bunch matrix with polynomial entries over F2, *International Organization of Science and Research Journal of Mathematics*, 11(2015), 1–4.

[9] MI Saju and PL Lilly, A public key cryptosystem based on discrete logarithm problem over finite fields Fpn , *International Organization of Science and Research Journal of Mathematics*, 11(2015), 1–3.

[10] MI Saju and PL Lilly, The role of primitive polynomials in the construction of public key cryptosystems, *Journal of Theoretical Physics and Cryptography*, 11(2016), 1–4.

[11] MI Saju and PL Lilly, Design of a discrete logarithm problem based exchange public key cryptosystem in the finite algebraic extension filed of a finite field, *International Journal of Engineering Science Invention*, 6(2017), 50–53.

[12] MI Saju and PL Lilly, Exchange message cryptosystem based on discrete logarithm problem over extension field Fpn of the finite field Fp, *Journal of Theoretical Physics and Cryptography*, 14(2017), 8–11.

⋆⋆⋆⋆⋆⋆⋆⋆⋆
ISSN(P):2319 − 3786
Malaya Journal of Matematik
ISSN(O):2321 − 5666
⋆⋆⋆⋆⋆⋆⋆⋆⋆