International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 6 Issue 9|| September 2017 || PP. 50-53

Design of a Discrete Logarithmic Problem Based Exchange Public Key Cryptosystem in the Finite Algebraic Extension Field of a Finite Field

*M. I. Saju[1], P. L. Lilly[2]
[1]*(Assistant Professor, Department of Mathematics, St. Thomas' College, University of Calicut, Thrissur, Kerala, India)*
[2]*(Associate Professor, Department of Mathematics, St. Joseph's College,University of Calicut, Thrissur, Kerala, India)*
Corresponding Author: M. I. Saju

***Abstract**: Every user, while communicating privately over a public channel, wish for a trusted channel to communicate securely thus eliminating the least chance of the intruder getting access to it, either at transit or in store. Cryptography - the most popular technique to provide secure data communication is hence studied extensively from the middle of 1970's. Even though there exists few limitations, cryptography is here to stay primarily because it has played a key role in providing strong, reliable, and robust network data security thus safeguarding users' privacy. Through this research paper, authors propose a public key cryptosystem, which works in an algebraic extension field over a finite field. In the construction the authors use primitive polynomials over the finite field. In this system each user encrypted his text into two parts and sends the first part to the one. The receiver also encrypted the received text into two parts and sends the first part to the sender. This process can be repeated a finite number of times. The proposed system has all the major features of the popular exchange public key cryptosystem and the security of the system is as good as the difficulty of solving discrete logarithm problem (DLP) over the finite field. Proposed system is implemented and tested in Mat lab to verify its potential for implementation in the Open Systems.*

***Keywords**: Algebraic Extension Field, Discrete Logarithm Problem, Exchange Cryptosystem, Finite Field, Primitive Polynomial*

Date of Submission: 20-09-2017 Date of acceptance: 30-09-2017

I. INTRODUCTION

The birth of modern cryptography is a great deal of fascinating mathematics some of which has been developed for cryptographic applications but much of which is taken from the classical canons. The three main algorithms in a public key cryptosystem are Key Creation Algorithm, the Encryption Algorithm and the Decryption Algorithm[1]. The security of the system depending on the difficulties of solving classical problems *viz.* Factorization problem, the Discrete Logarithm Problem and Knapsack problem[2].

The main prerequisites for the construction of the public key cryptosystem are prime numbers, irreducible polynomial over a finite field of finite degree. The generation of a strong prime is an important role in the design of the system. The Gordon's algorithm is used for generating a strong prime[3].

If $f(x)$ is an irreducible polynomial of degree n over the finite field $\mathbb{F}_p$ then the quotient ring $\mathbb{F}_q = \frac{\mathbb{F}_p[x]}{(f(x))}$ is a finite field with $q = p^n$ elements [4]. If $f(x)$ is a primitive polynomial over $\mathbb{F}_p$, then it is an irreducible polynomial and its roots generate the group $\mathbb{F}_q^*$. The number of primitive polynomials of degree n over the field $\mathbb{F}_p$ is$\frac{\varphi(p^n-1)}{n}$[5][6].

1.1. Example The number of primitive polynomials of degree 6 over the field $\mathbb{F}_2$ is given by $\frac{\varphi(2^6-1)}{6} = 6$. They are $x^6 + x^5 + x^4 + x + 1$, $x^6 + x^5 + x^3 + x^2 + 1$, $x^6 + x^5 + x^2 + x + 1$, $x^6 + x^5 + 1$, $x^6 + x^4 + x^3 + x + 1$ and $x^6 + x + 1$.

If $f(x)$ be a primitive polynomial of degree n over the field $\mathbb{F}_p$, $f(\beta) = 0$, β^r be a root of another primitive polynomial $f_r(x)$ such that r and $p^n - 1$ are relatively prime and let k be a random $n - bit$ number with

$x^k \equiv g(x)(mod f(x))$ and $x^k \equiv g_r(x)(mod f_r(x))$, then $g(x) \equiv \left(g_r(x^r)\right)^{r^{-1}} (mod f(x))$ and $g_r(x) \equiv \left(g\left(x^{r^{-1}}\right)\right)^r (mod f_r(x))$[7][8][9][10].

1.2. Example Let $f(x) = x^6 + x^5 + x^4 + x + 1$ be the primitive polynomial over $\mathbb{F}_2$, $f(\beta) = 0$ and $r = 37$.
Then, β^{37} is a root of another primitive polynomial $f_{37}(x) = x^6 + x + 1$ over $\mathbb{F}_2$, where $\gcd(37,63) = 1$. The inverse of 37 is 46.
Take $k = 53$, then we have
$x^{53} \equiv x^5 + x^4 + x^3 + x^2 + x(modf(x))$, $x^{53} \equiv x^5 + x^3 + x(modf_{37}(x))$,
$x^5 + x^4 + x^3 + x^2 + x \equiv ((x^{37})^5 + (x^{37})^3 + x^{37})^{46}(modf(x))$ and
$x^5 + x^3 + x \equiv ((x^{46})^5 + (x^{46})^4 + (x^{46})^3 + (x^{46})^2 + x^{46})^{37}(modf_{37}(x))$

II. DESIGNING THE SYSTEM

George and Joseph fix a publicly known prime p and a primitive polynomial $f(x)$ of degree n over the field $\mathbb{F}_p$ and all other elements used are kept secret. Suppose George wants to send a message $M(x)$ to Joseph. George takes a secret private key number r such that $\gcd(r, p^n - 1) = 1$ and an ephemeral key number k_1, and computes the following

$x^{k_1} \equiv g(x)(modf(x))$ and $x^{k_1} \equiv g_r(x)(modf_r(x))$, and sends the polynomial $M(x)\big(g(x)\big)^{-1}$ to Joseph. Here $f_r(x)$ be another primitive polynomial of degree n over $\mathbb{F}_p$ with $f_r(x^r) = 0$.

Joseph takes a secret private key number s such that $\gcd(s, p^n - 1) = 1$ and an ephemeral key number k_2, and computes the following $x^{k_2} \equiv h(x)(modf(x))$ and $x^{k_2} \equiv h_s(x)(modf_s(x))$, and sends the polynomial $M(x)\big(g(x)\big)^{-1}\big(h(x)\big)^{-1}$ to George. Here $f_s(x)$ is another primitive polynomial of degree n over $\mathbb{F}_p$ with $f_s(x^s) = 0$.

George computes $M(x)\big(g(x)\big)^{-1}\big(h(x)\big)^{-1}\big(g_r(x^r)\big)^{r^{-1}} = M(x)\big(h(x)\big)^{-1}$ and sends back to Joseph.

Finally, Joseph computes $M(x)\big(h(x)\big)^{-1}\big(h_s(x^s)\big)^{s^{-1}}$ and recovers the message $M(x)$ of George.

2.1 Example George and Joseph fix a publicly known primitive polynomial $f(x) = x^6 + x^5 + x^4 + x + 1$ of degree 6 over the field $\mathbb{F}_2$.
Step 1.Key creation process of George
George takes a secret number $r = 37$ with $\gcd(37,63) = 1$, computes another primitive polynomial $f_{37}(x) = x^6 + x + 1$ with $f_{37}(x^{37}) = 0$ and $37^{-1} = 46$. All these parameters are kept secret.
Step 2.Encryption process of George
Suppose George wants to send the message $M(x) = x^5 + x^4 + x^2 + 1$ to Joseph. He takes an ephemeral key number 53 and computes the following:
$x^{53} \equiv x^5 + x^4 + x^3 + x^2 + x(modf(x))$, $x^{53} \equiv x^5 + x^3 + x(modf_{37}(x))$ and $(x^5 + x^4 + x^2 +$ *1x5+x4+x3+x2+x−1=x4+1*. For the purpose of decryption he computes *x375+x373+x37=x5+x3+x*. Hence he sends $x^4 + 1$ to Joseph.
Step 3.Key creation process of Joseph
Joseph takes a secret number $s = 43$ with $\gcd(43,63) = 1$, computes another primitive polynomial $f_{43}(x) = x^6 + x^5 + x^3 + x^2 + 1$ with $f_{43}(x^{43}) = 0$ and $43^{-1} = 22$. All these parameters are kept secret.
Step 4.Encryption process of Joseph
He takes an ephemeral key number 39 and computes the following:
$x^{39} \equiv x + 1(modf(x))$, $x^{39} \equiv x^5 + x^3 + x^2 + x(modf_{43}(x))$ and
$(x^4 + 1)(x + 1)^{-1} = x^3 + x^2 + x + 1$. For the purpose of decryption he computes $((x^{43})^5 + (x^{43})^3 + (x^{43})^2 + x^{43} = x + 1$. Hence he sends back the polynomial $x^3 + x^2 + x + 1$ to George.
Step 5.Decryption process of George
George multiplying the received polynomial $x^3 + x^2 + x + 1$ with $(x^5 + x^3 + x)^{46}$
And he gets $x^4 + x + 1$, sends this to Joseph.
Step 6.Decryption process of Joseph
Joseph multiplying the received polynomial $x^4 + x + 1$ with $(x + 1)^{22}$ and gets the original message $M(x) = x^5 + x^4 + x^2 + 1$.
2.2 Example: George and Joseph fix a publicly known primitive polynomial $f(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$ of degree 8 over the field $\mathbb{F}_2$.
Step 1.Key creation process of George
George takes secret numbers $r = 37,43,103$ with these numbers are relatively prime to 255, computes primitive polynomials $f_{37}(x) = x^8 + x^5 + x^3 + x + 1$ with $f_{37}(x^{37}) = 0$, $f_{43}(x) = x^8 + x^7 + x^6 + x^5 + x^2 + x + 1$ with $f_{43}(x^{43}) = 0$ and $f_{103}(x) = x^8 + x^6 + x^5 + x^3 + 1$ with $f_{103}(x^{103}) = 0$ and $31^{-1} = 181$, $43^{-1} = 172$ and $103^{-1} = 52$. All these parameters are kept secret.
Step 2.Encryption process of George

Suppose George wants to send a message $M(x) = x^7 + x^5 + x^3 + x + 1$ to Joseph. He takes the ephemeral key numbers 113,123,171 and computes the following,

$x^{113} \equiv x^7 + x^6 + x^5 + x^3 + x^2 + 1(modf(x))$

$x^{113} \equiv x^3 + x^2 + 1(modf_{37}(x))$

$x^{123} \equiv x^7 + x^5 + x^3 + x^2 + x + 1(modf(x))$

$x^{123} \equiv x^7 + x^6 + x^3 + x^2 + x(modf_{43}(x))$

$x^{171} \equiv x^7 + x^5 + x^4 + x^3(modf(x))$

$x^{171} \equiv x^7 + x^6 + x^5 + x^4 + x^3 + x^2(modf_{103}(x))$, then computes

$(x^7 + x^5 + x^3 + x + 1)\ (x^7 + x^6 + x^5 + x^3 + x^2 + 1)^{-1}$

$(x^7 + x^5 + x^3 + x^2 + x + 1)^{-1}\ \ (x^7 + x^5 + x^4 + x^3)^{-1} = x^7 + x^6 + x^3 + x^2 + x + 1,$

$(x^{37})^3 + (x^{37})^2 + 1 = x^7 + x^6 + 1$

$(x^{43})^7 + (x^{43})^6 + (x^{43})^3 + (x^{43})^2 + x^{43} = x^7 + x^4 + x^3 + x^2$

$(x^{103})^7 + (x^{103})^6 + (x^{103})^5 + (x^{103})^4 + (x^{103})^3 + (x^{103})^2 = x^7 + x^5.$

The four parts of the encrypted text are

$x^7 + x^6 + x^3 + x^2 + x + 1, x^7 + x^6 + 1, x^7 + x^4 + x^3 + x^2, x^7 + x^5$

The first part sends to Joseph and the remaining three parts kept secret for the process of decryption.

Step 3.Key creation process of Joseph

Joseph takes secret numbers $s = 41,73,139$ with these numbers are relatively prime to 255, computes the primitive polynomials $f_{41}(x) = x^8 + x^5 + x^3 + x + 1$ with $f_{41}(x^{41}) = 0$, $f_{73}(x) = x^8 + x^5 + x^3 + x + 1$ with $f_{73}(x^{73}) = 0$ and $f_{139}(x) = x^8 + x^7 + x^2 + x + 1$ with $f_{139}(x^{139}) = 0$. Then computes $41^{-1} = 56$, $73^{-1} = 7$ and $139^{-1} = 244$. All these parameters are kept secret.

Step 4.Encryption process of Joseph

He takes the ephemeral key numbers 121,137,143 and computes the following,

$x^{121} \equiv x^7 + x^5 + x^3 + x^2(modf(x))$

$x^{121} \equiv x^7 + x^6 + x^5 + x^4 + x^2(modf_{41}(x))$

$x^{137} \equiv x^4 + x^3(modf(x))$

$x^{137} \equiv x^6 + x^4 + x^3 + x^2 + x(modf_{73}(x))$

$x^{143} \equiv x^5 + 1(modf(x))$

$x^{143} \equiv x^6 + x^2(modf_{139}(x))$,

and take the received polynomial $x^7 + x^6 + x^3 + x^2 + x + 1$ and computes

$(x^7 + x^6 + x^3 + x^2 + x + 1)(x^7 + x^5 + x^3 + x^2)^{-1}(x^4 + x^3)^{-1}(x^5 + 1)^{-1}$

$= x^7 + x^6 + x^5,$

$(x^{41})^7 + (x^{41})^6 + (x^{41})^5 + (x^{41})^4 + (x^{41})^2 = x^7 + x^5 + x^4 + x^3 + x^2,$

$(x^{73})^6 + (x^{73})^4 + (x^{73})^3 + (x^{73})^2 + x^{73} = x^7 + x^6 + x^5 + x^3$

$(x^{139})^6 + (x^{139})^2 = x^6 + x^5 + x^2.$

The four parts of the encrypted text are

$x^7 + x^6 + x^5, x^7 + x^5 + x^4 + x^3 + x^2, x^7 + x^6 + x^5 + x^3, x^6 + x^5 + x^2$

The first part sends to George and the remaining three parts kept secret for the process of decryption.

Step 5.Decryption process of George

Using the polynomials $x^7 + x^6 + 1, x^7 + x^4 + x^3 + x^2, x^7 + x^5$, the secret numbers 52,172,193 and the received polynomial $x^7 + x^6 + x^5$ computes the following,

$(x^7 + x^6 + x^5)(x^7 + x^5)^{52} = x^7 + x^6 + x^2$

$(x^7 + x^6 + x^2)(x^7 + x^4 + x^3 + x^2)^{172} = x^6 + x^4 + x^2 + x$

$(x^6 + x^4 + x^2 + x)(x^7 + x^6 + 1)^{193} = x^7 + x^6 + x^4 + x^2 + x + 1.$

Then the polynomial $x^7 + x^6 + x^4 + x^2 + x + 1$ sends to Joseph.

Step 6. Decryption process of Joseph

Using the polynomials $x^7 + x^5 + x^4 + x^3 + x^2, x^7 + x^6 + x^5 + x^3, x^6 + x^5 + x^2$, the secret numbers 244,7,56 and the received polynomial $x^7 + x^6 + x^4 + x^2 + x + 1$ computes the following,

$(x^7 + x^6 + x^4 + x^2 + x + 1)(x^6 + x^5 + x^2)^{244} = x^7 + x^5 + x^3 + x^2$

$(x^7 + x^5 + x^3 + x^2)(x^7 + x^6 + x^5 + x^3)^7 = x^3$

$(x^3)(x^7 + x^5 + x^4 + x^3 + x^2)^{56} = x^7 + x^5 + x^3 + x + 1 = M(x)$

III. SECURITY OF THE SYSTEM

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 numbers and the prime numbers. In this system the finite algebraic field $\mathbb{F}_{p^n}$ given to the public and all other parameters are kept secret. The algorithms used here is sub-exponential and all the entries are polynomials, which add to the stealth of the system. It is implemented and tested in mat lab to verify its potential for implementation in the open systems. The selection of the prime number is an important factor of this system. For the security select the size of the field is at least 2^{2048}.

IV. 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.

REFERENCES

[1] A. Menezes, P. C. Van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography (CRC Press,1996)

[2] D. R. Stinson, Cryptography theory and practice (Second Edition, Chapman and Hall/CRC., 2002, 339pp.)

[3] J.A. Gordon, Strong Primes are Easy to Find Advances in Cryptology, Proceedings of Eurocrypt 84, Springer, 1985, 216-223.

[4] J Fraleigh, A First Course in Abstract Algebra (Addison Welsley, Seventh edition 2002)

[5] R. Lidl and H. Niederreiter, Finite Fields (Cambridge University Press, 2nd ed., 1997)

[6] D.S. Dummit and R.M. Foote, Abstract Algebra (John Wiley and Sons Inc., Hoboken, NJ, Third Edition.2004)

[7] Saju M.I. and Lilly P.L., A Method of Designing a Public-Key Cryptosystem Based on Discrete Logarithm Problem, International Research Journal of Pure Algebra, 4(11), 2014, 628-630.

[8] Saju M.I. and Lilly P.L., A Public-Key Cryptosystem Based on Discrete Logarithm Problem over Finite Fields F_p^n, International Organization of Science and Research Journal of Mathematics, 11(1), 2015, 01-03.

[9] Saju M.I. and Lilly P.L., A digital signature and a new public key cryptosystem based on discrete logarithm problem over finite extension field of the field $F_{p,}$ International Organization of Science and research Journal of mathematics, 11(5), 2015, 32-35.

[10] Saju M.I. and Lilly P.L.,The Role of Primitive Polynomials in the Construction of Public Key Cryptosystems, Journal of Theoretical Physics and Cryptography, 11, 2016, 01-04.

International Journal of Engineering Science Invention (IJESI) is UGC approved Journal with Sl. No. 3822, Journal no. 43302.

M. I. Saju. "Design of a Discrete Logarithmic Problem Based Exchange Public Key Cryptosystem in the Finite Algebraic Extension Field of a Finite Field." International Journal of Engineering Science Invention(IJESI), vol. 6, no. 9, 2017, pp. 50–53.