JOURNAL OF THEORETICAL PHYSICS & CRYPTOGRAPHY
www.IJTPC.org/Publications

Exchange Message Cryptosystem Based On Discrete Logarithm Problem over the Extension Field $\mathbb{F}_{p^n}$ of the Finite Field $\mathbb{F}_p$

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.

Abstract

Through this research paper, authors construct a public key cryptosystem which works in the finite extension function field of the finite field $\mathbb{F}_p$. The security of this system is based on difficulty of solving DLP in $\mathbb{F}_{p^n}{}^*$. 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. Each user select a private secret number k, which is less than $p^n - 1$ and relatively prime to $p^n - 1$. Also, computes $k^{-1}(mod p^n - 1)$. Each user has to compute another primitive polynomial $f_k(x)$ of degree n over $\mathbb{F}_p$, such that α^k be its root and $f(\alpha) = 0$. Also each user can randomly chosen an ephemeral number N and find remainders $T(x)$ and $T_k(x)$, when x^N is divided by $f(x)$ and $f_k(x)$ rspectively. Let $T_A(x)$,$T_{k_A}(x)$ be the remainders of 'A' and $T_B(x)$,$T_{k_B}(x)$ be the remainders of 'B'. Suppose 'A' wants to send a message $M(x)$ to 'B'. Then, 'A' computes $M(x)\left(T_A(x)\right)^{-1}$ and send to 'B', but 'B' has no idea about $\left(T_A(x)\right)^{-1}$, so 'B' computes $M(x)\left(T_A(x)\right)^{-1}\left(T_B(x)\right)^{-1}$ and send back to 'A'. Then, 'A' releases $\left(T_A(x)\right)^{-1}$ from the text and again send to 'B', then 'B' releases $\left(T_B(x)\right)^{-1}$ from the text and releases the message $M(x)$.

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 groundbreaking 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.

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

In this study, the authors propose a novel cryptosystem, which works in the finite extension field of $\mathbb{F}_p$. In the next section, we explain mathematical prerequisite to appreciate the current study and section III narrates the designs of the system. Section IV design the system with an example, section V deals with the security of the proposed work and finally, section VI wraps up the study with a conclusion.

Mathematical Prerequisites

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 $a \in F$. 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 function field over the finite field $\mathbb{F}_p$ with single parameter$x$ and it is denoted by $\mathbb{F}_{p^n}$. 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. 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

$T(x) \equiv \left(T_k(x^k)\right)^{k^{-1}} (mod f(x))$ and $T_k(x) \equiv \left(T(x^{k^{-1}})\right)^k (mod\ f_k(x))$.

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 $\alpha^k \equiv t(x)(mod\ f(x))$. This problem is difficult because there are infinitely many values for k.

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.

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 $g.c.d.(p^n - 1, k_A) = 1$. 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

$x^{N_A} \equiv T_A(x)(mod f(x))$

$x^{N_A} \equiv T_{k_A}(x)(mod f_{k_A}(x))$

Then we have, $T_A(x) \equiv (T_{k_A}(x^{k_A}))^{k_A{}^{-1}}(mod f(x))$ (3.1) and

$T_{k_A}(x) \equiv (T_A(x^{k_A{}^{-1}}))^{k_A}(mod f_{k_A}(x))$ (3.2)

Similarly, Bob picks a number k_B such that $g.c.d.(p^n - 1, k_B) = 1$. 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

$x^{N_B} \equiv T_B(x)(mod f(x))$

$x^{N_B} \equiv T_{k_B}(x)(mod f_{k_B}(x))$

Then we have, $T_B(x) \equiv (T_{k_B}(x^{k_B}))^{k_B{}^{-1}}(mod f(x))$ (3.3) and

$T_{k_B}(x) \equiv (T_B(x^{k_B{}^{-1}}))^{k_B}(mod f_{k_B}(x))$ (3.4)

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 $M(x)\left(T_{k_A}(x)\right)^{-1}\left(T_{k_B}(x)\right)^{-1}$ and send back to Alice.

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

Example

Take the primitive polynomial $f(x) = x^5 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$, $k_A = 23$, $k_A{}^{-1} = 27$, $f_{23}(x) = x^5 + x^3 + x^2 + x + 1$, $N_A = 21$ and compute the following,

$x^{21} \equiv x^2 + x(modx^5 + x^4 + x^3 + x^2 + 1$

$x^{21} \equiv x^4 + x^3 + 1(modx^5 + x^3 + x^2 + x + 1)$

Where $T_A(x) = x^2 + x$, $T_{23}(x) = x^4 + x^3 + 1$, $\left(T_A(x)\right)^{-1} = x^3 + x$, $(T_{23}(x))^{-1} = x^3$.

Let $M(x) = x^4 + x^2 + 1$.

Alice computes $\left\{M(x)\left(T_A(x)\right)^{-1}, T_{23}(x^{23})\right\}$ = $\{x^3 + x^2,\ x^4 + 1\}$

Alice sends $M_A(x) = x^3 + x^2$ to Bob.

Bob takes the secret number $k_B = 19$, then $k_B{}^{-1} = 18$ and

$f_{19}(x) = x^5 + x^4 + x^3 + x + 1$.

Also Bob takes a 5-bit number $N_B = 17$ and computes the following

$x^{17} \equiv x^4 + x^2 + x(modx^5 + x^4 + x^3 + x^2 + 1)$

$x^{17} \equiv x^3 + x + 1(modx^5 + x^4 + x^3 + x + 1)$

Where $T_B(x) = x^4 + x^2 + x$, $T_{19}(x) = x^3 + x + 1$, $\left(T_B(x)\right)^{-1} = x^4 + x + 1$, $(T_{19}(x))^{-1} = x^4 + x^3 + x + 1$.

Bob Computes $\left\{M_A(x)\left(T_B(x)\right)^{-1}, T_{19}(x^{19})\right\}$ = $\{x^4 + x^3 + x^2 + 1, x^4 + x^2 + x + 1\}$

Bob sends $M_B(x) = x^4 + x^3 + x^2 + 1$ to Alice.

Alice Computes $(x^4 + x^3 + x^2 + 1)(x^4 + 1)^{27} = x^3 + 1$.

Bob Computes $(x^3 + 1)(x^4 + x^2 + x + 1)^{18} = x^4 + x^2 + 1$.

Security of the proposed 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 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. It is implemented and tested in mat lab to verify its potential for implementation in the open systems.

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] Lilly P.L., Saju M.I., A Method of Designing a Public-Key Cryptosystem Based on Discrete Logarithm Problem, International Journal of Pure Algebra, 4(11), 2014, pp628-630(3)

[2] Saju M.I., Lilly P.L., A Public-Key Cryptosystem Based on Discrete Logarithm Problem over Finite Fields $\mathbb{F}_{p^n}$ International Organization of Science and Research Journal of Mathematics, 11(1), 2015, pp01-03(3)

[3] Saju M. I., Lilly P.L., A Method of Designing Block Cipher which Involves a Key Bunch Matrix With

Polynomial Entries over F_2 , International Organization of Science and Research Journal of Mathematics, 11(2), 2015, pp01-04

[4] Saju M. I., Lilly P.L., Applications of Function Field in a Public Key Cryptosystem, Journal of Theoretical and Computational Mathematics, Vol.1(1), 2015, pp:52-55.

[5] Saju M. I., Lilly P.L., A Digital Signature and a new Public Key Cryptosystem Based on Discrete Logarithm Problem Over Finite Extension of the Field F_2 , , International Organization of Science and Research Journal of Mathematics, 11(5), 2015, pp32-35

[6] Lidi R., Miederreiter H., Finite Fields.

[7]Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, an Introduction to Mathematical Cryptography, Springer.