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

The Role of Primitive Polynomials in the Construction of Public Key Cryptosystems

M. I. SAJU[1], P. L. LILLY[2]
[1]Assistant Professor, Department of Mathematics, St. Thomas' College, University of Calicut, Thrissur, India
[2]Associate professor, Department of Mathematics, St. Joseph's College,University of Calicut, Irinjalakuda, India

ABSTRACT

One of the classical problems in mathematics is the Discrete Logarithm Problem (DLP).The difficulty and complexity for solving DLP is used in most of the cryptosystems. In this paper we design a public key system using a set of primitive polynomials over the field F_2 . The security of the system is based on the difficulty of solving discrete logarithms over the function field F_{2^n} with sufficiently large n.

Keywords

Discrete Logarithm Problem, Cryptosystem, Public Primitive Polynomial, Extension Field, Polynomial Congruence

1. INTRODUCTION

The public key cryptosystems firstly introduced by Diffie and Hellmann in 1976. After that in 1978, the RSA public key cryptosystem was introduced by Rivest, Shamir and Adlemann. The public key cryptosystem are based on the difficulties of solving classical problems like factorization problem, Discrete Logarithm Problem, Knapsack Problem etc. Public key cryptography draws on many areas of mathematics, including Abstract Algebra, Number Theory, Information Theory and Probability. There are many cryptosystems based on Discrete Logarithm Problem (DLP). The Diffie-Hellman key exchange, ElGamal Cryptosystem, Massey-Omura Cryptosystem are examples of cryptosystems based on DLP. The idea behind a public key cryptosystem is that it might be possible to find a cryptosystem where it is computationally infeasible to determine the deciphering key from the given enciphering key. The advantage of a public key system is that Shine (or anyone else) can send an encrypted message to Saju (without the prior communication of a shared secret key) by using the public encryption rule.

The cryptosystem in this paper is also based on DLP. In the papers [1][2][3][4][5], We use a pair of primitive polynomials over F_2, but here we use a finite set of primitive polynomials of same degree over F_2.

1.1[6] Definition

If G is finite Group, b is an element of G, and y is an element of g which is a power of b, then the discrete logarithm of y to the base b is any integer x such that $y = b^x$.

1.1.1 Example

In $F_{3^2}{}^*$ with α a root of $x^2 + 2x + 2$, the discrete logarithm of -1 to the base α is 4.

1.2 [6] [7] Definition

A polynomial $f \in F_q[x]$ of degree $d \geq 1$ is called a primitive polynomial over F_q if it is the minimal polynomial over F_q of a primitive element of F_{q^d}.

1.3 [6][7] Definition

Let $f \in F_q[x]$ be a nonzero polynomial. If $f(0) \neq 0$, then the least positive integer t for which $f(x)$ divides $x^t - 1$ is called the order of f and denoted by $ord(f) = ord(f(x))$

1.3.1 Example

The polynomials x^3+x^2+1 and x^3+x+1 are primitive polynomials over F_2 of degree 3.

1.4 [6][7] Theorem

Let $f \in F_q[x]$ be a primitive polynomial of degree d, then $ord(f)$ is equal to q^d-1.

1.5 [6][7] Theorem

Let f be a primitive polynomial in $F_q[x]$ of degree d, then f has a root α in F_{q^d}. Furthermore, all the roots of f are simple and are given by the d distinct elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$ of F_{q^d}.

1.5.1[6][7] Corollary

Any two primitive polynomials in $F_q[x]$ of the same degree have isomorphic splitting fields.

1.6 [6][7] Definition

Let F_{q^d} be an extension of F_q and let $\alpha \in F_{q^d}$. Then the elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$ are called the conjugates of α with respect to F_q.

1.7 [7] Theorem

Let $f(x)$ be a monic irreducible polynomial in $F_2[x]$ of degree d. Let $\alpha \in F_{p^d}$ be a root of $f(x)$, and for $k \in N$, let $f_k(x)$ be the characteristic polynomial of $\alpha^k \in F_{p^d}$ over F_p. Then $f_k(\alpha^k) = (-1)^{n(k+1)} \prod_{j=1}^{k} f(\omega_j x)$, where $\omega_1, \omega_2, \ldots, \omega_k$ are the k^{th} roots of unity over F_p counted according to multiplicity.

1.7.1 Example

Let $f(x) = x^4+x+1$ in $F_2[x]$ and $f(\alpha)=0$. To calculate $f_3(x^3) = (-1)^{16} \prod_{j=1}^{3} f(\omega_j x)$, where ω_j is the cube root of unity. $f_3(x^3) = (x^4+x+1)(x^8+x^4+x^2+x+1) = x^{12}+x^9+x^6+x^3+1$.

$f_3(x^3) = x^4+x^3+x^2+x+1$.

1.7.2 Example

We compute the minimal polynomials over F_2 of all elements of F_{16}. Let $\alpha \in F_{2^4}$ be a root of the primitive polynomial x^4+x+1 over F_2. The elements of $F_{2^4}{}^*$ are in Table 1. The generators of $F_{2^4}{}^*$ are $\alpha, \alpha^2, \alpha^4, \alpha^7, \alpha^8, \alpha^{11}, \alpha^{13}, \alpha^{14}$. Here x^4+x+1 and x^4+x^3+1 are primitive polynomials of degree 4 over F_2.

2. A PUBLIC KEY CRYPTOSYSTEM

In a public key cryptosystem, there are three public algorithms, the key generation algorithm, the encryption algorithm and the decryption algorithm. This system works on the base of "Strong Discrete Logarithm Assumption". Under the strong discrete logarithm assumption there will be a strong one way function, namely, "Exponentiation Modulo a Prime p".

2.1 Key generation algorithm

Let $f(x)$ be a primitive polynomial of degree n over F_2 and α be a root of $f(x)$. So we have a finite extension field $F_2(\alpha) = \frac{F_2[x]}{(f(x))} = F_{2^n}$.

Let $f_{k_1}(x), f_{k_2}(x), \ldots\ldots, f_{k_r}(x)$ be primitive polynomials of degree n over F_2, $\alpha^{k_i}, i = 1,2,\ldots,r$ be the roots of $f_{k_i}(x)$ and $k_1, k_2, \ldots., k_r$ are relatively prime to 2^n-1 and $1 \le r \le \frac{\varphi(2^n-1)}{n}$. The α^{k_i} is a polynomial in α, $g_i(\alpha)$. The DLP is to find k_i, such that $\alpha^{k_i} = g_i(\alpha)$. The sequence of integers $(k_1, k_2, \ldots., k_r)$ be the secrete key of this system. Compute the sequence of integers $({k_1}^{-1}, {k_2}^{-1}, \ldots\ldots, {k_r}^{-1})$ for the purpose of decryption process. Here, both sequences of integers are secret. The public parameters are the field $\frac{F_2[x]}{(f(x))}$, the primitive polynomials $f_{k_1}(x), f_{k_2}(x), \ldots\ldots, f_{k_r}(x)$ and the polynomials $g_i(\alpha)$, $= 1,2,\ldots,r$.

2.2 Encryption algorithm

Let N be a $n-bit$ number and consider the following system of polynomial congruence

$$x^N \equiv T(x)\left(mod f(x)\right)$$
$$x^N \equiv T_{k_1}(x)\left(mod f_{k_1}(x)\right)$$
$$x^N \equiv T_{k_2}(x)\left(mod f_{k_2}(x)\right) \qquad (2.1)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x^N \equiv T_{k_r}(x)\left(mod f_{k_r}(x)\right)$$

Then, we have,

$$T(x) \equiv \left[T_{k_1}(x^{k_1})\right]^{{k_1}^{-1}}\left(mod f(x)\right)$$
$$T(x) \equiv \left[T_{k_2}(x^{k_2})\right]^{{k_2}^{-1}}\left(mod f(x)\right) \qquad (2.2)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$T(x) \equiv \left[T_{k_r}(x^{k_r})\right]^{{k_r}^{-1}}\left(mod f(x)\right)$$

Also, we have,

$$T_{k_1}(x) \equiv \left[T(x^{{k_1}^{-1}})\right]^{k_1}(mod f_{k_1}(x))$$
$$T_{k_2}(x) \equiv \left[T(x^{{k_2}^{-1}})\right]^{k_2}(mod f_{k_2}(x)) \qquad (2.3)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$T_{k_r}(x) \equiv \left[T(x^{{k_r}^{-1}})\right]^{k_r}(mod f_{k_r}(x))$$

Let $M(x)$ be the plain text. Then compute $(M(x)(T(x))^{-r}, T_{k_1}(x^{k_1}), T_{k_2}(x^{k_2}), \ldots, T_{k_r}(x^{k_r}))$ (2.4), this $r+1-tuple$ will be the cipher text.

Or compute

$$\left(M(x)(T_{k_1}(x))^{-1}(T_{k_2}(x))^{-1}\ldots.(T_{k_r}(x))^{-1}, \atop T(x^{k_1{}^{-1}}), T(x^{k_2{}^{-1}}), \ldots, T(x^{k_r{}^{-1}})\right)..$$

(2.5), this $r+1-tuple$ will be the cipher text.

2.3 Decryption algorithm

We compute the following

$[T_{k_r}(x^{k_r})]^{k_r{}^{-1}}, [T_{k_{r-1}}(x^{k_{r-1}})]^{k_{r-1}{}^{-1}}, \ldots, [T_{k_1}(x^{k_1})]^{k_1{}^{-1}}$ and multiply each result with the first part of the cipher text (3.1), and then we get the plain text $M(x)$.

Or compute $[T(x^{k_r{}^{-1}})]^{k_r}, [T(x^{k_{r-1}{}^{-1}})]^{k_{r-1}}, \ldots\ldots, [T(x^{k_1{}^{-1}})]^{k_1}$ and multiply each result with the first part of the cipher text (3.2), and then we get the plain text $M(x)$. Here we use the results (2.2) and (2.3) In the first case $(k_1{}^{-1}, k_2{}^{-1}, \ldots\ldots, k_r{}^{-1})$ and in the second case $(k_1, k_2, \ldots\ldots, k_r)$ be used as deciphering keys.

3. EXAMPLE

Take $f(x) = x^5 + x^2 + 1$, it is a primitive polynomial of degree 5 over F_2 and let α be a root of $f(x)$. So we have a finite extension field $F_2(\alpha) = \frac{F_2[x]}{(f(x))} = F_{2^5}$. The other roots of $f(x)$ are $\alpha^2, \alpha^4, \alpha^8, \alpha^{16}$. There are six primitive polynomial of degree 5 over F_2. See the table 2.

Take N=15, we have

$$x^{15} \equiv x^4 + x^3 + x^2 + x + 1 (mod x^5 + x^2 + 1)$$

$$x^{15} \equiv x^4 + x^3 + x + 1 (mod x^5 + x^4 + x^3 + x^2 + 1)$$

$$x^{15} \equiv x^4 + x^2 + 1 (mod x^5 + x^4 + x^2 + x + 1) \quad (3.1)$$

$$x^{15} \equiv x^4 + x^3 (mod x^5 + x^3 + x^2 + x + 1)$$

$$x^{15} \equiv x^3 + x^2 (mod x^5 + x^4 + x^3 + x + 1)$$

$$x^{15} \equiv x^2 + x (mod x^5 + x^3 + 1)$$

In this case $T(x) = x^4 + x^3 + x^2 + x + 1$, $T_3(x) = x^4 + x^3 + x + 1$, $T_5(x) = x^4 + x^2 + 1$, $T_7(x) = x^4 + x^3$, $T_{11}(x) = x^3 + x^2$ and $T_{15}(x) = x^2 + x$. Then, compute $T_3(x^3) = x^4 + x^3 + x^2 + 1$, $T_5(x^5) = x^4 + x^3 + x^2$, $T_7(x^7) = x^3 + x^2 + x$, $T_{11}(x^{11}) = x^4 + 1$ and $T_{15}(x^{15}) = x^3 + x^2 + 1$.

But from the above congruence (3.1), we get

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

$$x^4 + x^3 + x^2 + x + 1 \equiv (x^4 + x^3 + x^2)^{25} (mod x^5 + x^2 + 1)$$

$$x^4 + x^3 + x^2 + x + 1 \equiv (x^3 + x^2 + x)^9 (mod x^5 + x^2 + 1) \quad (3.2)$$

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

$$x^4 + x^3 + x^2 + x + 1 \equiv (x^3 + x^2 + 1)^{29} (mod x^5 + x^2 + 1)$$

And also have

$$x^4 + x^3 + x + 1 \equiv (x^{84} + x^{63} + x^{42} + x^{21} + 1)^3 (mod x^5 + x^4 + x^3 + x^2 + 1)$$

$$x^4 + x^2 + 1 \equiv (x^{100} + x^{75} + x^{50} + x^{25} + 1)^5 (\mathrm{mod} x^5 + x^4 + x^2 + x + 1)$$

$$x^4 + x^3 \equiv (x^{36} + x^{18} + x^{18} + x^9 + 1)^7 (mod x^5 + x^3 + x^2 + x + 1) \quad (3.3)$$

$$x^3 + x^2 \equiv (x^{68} + x^{51} + x^{34} + x^{17} + 1)^{11} (mod x^5 + x^4 + x^3 + x + 1)$$

$$x^2 + x \equiv (x^{116} + x^{87} + x^{58} + x^{29} + 1)^{15} (\mathrm{mod} x^5 + x^3 + 1)$$

Then also compute $(T(x))^{-1} = x^4 + x^3 + x + 1$, $(T_3(x))^{-1} = x^4 + x^3 + x^2 + x + 1$, $(T_5(x))^{-1} = x^4 + x^3 + x$, $(T_7(x))^{-1} = x^4 + 1$, $(T_{11}(x))^{-1} = x^2 + x + 1$ and $(T_{15}(x))^{-1} = x^3 + x^2 + x$.

3.1 Encryption

Let $M(x)$ be the plain text. The cipher text is

$\left\{M(x)(T(x))^{-5}, T_3(x^3)\right), T_5(x^5), T_7(x^7), T_{11}(x^{11}), T_{15}(x^{15})\}$

$= \{M(x)(x^4 + x^3 + x + 1)^{-5}, x^4 + x^3 + x^2 + 1, x^4 + x^3 + x^2, x^3 + x^2 + x, x^4 + 1, x^3 + x^2 + 1\}$ (3.4)

Or

$\{M(x)(T_3(x))^{-1})(T_5(x))^{-1}(T_7(x))^{-1}(T_{11}(x))^{-1}$

$(T_{15}(x))^{-1}, T(x^{21}), T(x^{25}), T(x^{9}), T(x^{17}), T(x^{29})\}$
$=\{M(x)(x^4+x^3+x^2+x+1)(x^4+x^3+x)(x^4+1)(x^2+x+1)(x^3+x^2+x),$
$.x^{84}+x^{63}+x^{42}+x^{21}+1,\ x^{100}+x^{75}+x^{50}+x^{25}+1,\ x^{36}+x^{18}+x^{18}+x^{9}+1,\ x^{68}+x^{51}+x^{34}+x^{17}+1, x^{116}+x^{87}+x^{58}+x^{29}+1\}$
(3.5)

3.2 Decryption

In the first case using the decryption key $(21, 25, 9, 17, 29)$, compute the following $(x^4+x^3+x^2+1)^{21}$, $(x^4+x^3+x^2)^{25}$, $(x^3+x^2+x)^9$, $(x^4+1)^{17}$ and $(x^3+x^2+1)^{29}$.

From (3.2) each of the above term is $x^4+x^3+x^2+x+1$, so multiply five times the first part of the cipher text (3.4) by this polynomial, we can release the plain text $M(x)$.

In the second case using the decryption key $(3, 5, 7, 11, 15)$, compute the following $(x^{84}+x^{63}+x^{42}+x^{21}+1)^3$, $(x^{100}+x^{75}+x^{50}+x^{25}+1)^5$, $(x^{36}+x^{18}+x^{18}+x^9+1)^7$, $(x^{68}+x^{51}+x^{34}+x^{17}+1)^{11}$ and $(x^{116}+x^{87}+x^{58}+x^{29}+1)^{15}$.

Multiply each of the above results with the first part of the cipher text (3.5), we can release the plain text $M(x)$, here we use the result (3.3).

4. SECURITY

The security of the above system is based on DLP. In the system we use different set of primitive polynomials. There are $\frac{\varphi(2^n-1)}{n}$ primitive polynomials available, select randomly a finite set of primitive polynomials for the key generation algorithm process. When we take a Galois Field of size at least 2^{2048} the system will more secure.

5. REFRENCES

[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 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

Table:1

j	α^j	j	α^j
0	1	8	α^2+1
1	α	9	$\alpha^3+\alpha$
2	α^2	10	$\alpha^2+\alpha+1$
3	α^3	11	$\alpha^3+\alpha^2+\alpha$
4	$\alpha+1$	12	$\alpha^3+\alpha^2+\alpha+1$
5	$\alpha^2+\alpha$	13	$\alpha^3+\alpha^2+1$
6	$\alpha^2+\alpha^3$	14	α^3+1
7	$\alpha^3+\alpha+1$		

Table: 2

Primitive polynomial	Roots of the polynomial	k	k^{-1}
$f_3(x)=x^5+x^4+x^3+x^2+1$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}$	3	21
$f_5(x)=x^5+x^4+x^2+x+1$	$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18}$	5	25
$f_7(x)=x^5+x^3+x^2+x+1$	$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{25}, \alpha^{19}$	7	9
$f_{11}(x)=x^5+x^4+x^3+x+1$	$\alpha^{11}, \alpha^{22}, \alpha^{13}, \alpha^{26}, \alpha^{21}$	11	17
$f_{15}(x)=x^5+x^3+1$	$\alpha^{15}, \alpha^{30}, \alpha^{29}, \alpha^{27}, \alpha^{23}$	15	29