IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 11, Issue 5 Ver. III (Sep. - Oct. 2015), PP 32-35
www.iosrjournals.org

A Digital Signature and a New Public Key Cryptosystem Based on Discrete Logarithm Problem Over Finite Extension Field of the Field F_p

Saju M.I.[1], Lilly P.L.[2]

1. Assistant Professor, Department of Mathematics, St. Thomas' College, Thrissur, India
2. Associate professor, Department of Mathematics, St. Joseph's College, Irinjalakuda, India

***Abstract**: In this paper we developed a new way of construction of digital signature and its verification. A new public key cryptosystem is also developed in this paper. All these public systems are based on discrete logarithm problem over finite extension field of the field F_p. These cryptosystems have all features of public key cryptosystems. The securities of these systems are based on the difficulty of finding discrete logarithms over F_{p^n} with sufficiently large n.*

***Keywords**: Digital Signature, Discrete Logarithm Problem, Hash Function,, Polynomials over Finite Fields, Primitive Polynomial, Public key cryptosystem.*

I. Introduction

A signature scheme cannot be unconditionally secure, since the enemy can test all possible signatures for a given message, using the public algorithms, until she finds a valid signature. Hence given sufficient time, the enemy can always forge the signature on any message. Signature schemes are almost always used with in conjunction with a very fast public cryptographic hash functions. The hash function will take a message of long length to a small specified size.

We have to careful that the use of a hash function does not weaken the security of the signature scheme, for it is the message digest that is signed, not the message. It is necessary for hash function to satisfy certain properties in order to prevent various attacks.

There are public key cryptosystems and digital signature systems based on the discrete logarithm problem (DLP) such as Digital Signature Standard (DSS)[1], ElGamal cryptosystem and Diffie-Hellman key exchange system. In our papers [2] [3] [4], we design cryptosystems which worked on the basis of discrete logarithm problem. For the security of these systems we need digital signature. Digital signature and its security have an important role in the construction of cryptosystems. The easiness of verification of signature is an important factor of digital signature. In our digital signature process the verification of signature is faster than other signatures. In the following scheme we use a sequence of signatures for the purpose of security, it is not compulsory but if you need more security we recommend that use two or more signature at a time. We randomly select a hash function which has an important role in this system. In order to construct digital signature it is necessary to use public key cryptography. The security of these systems is based on DLP [5] [6]. In this paper we also generalize the cryptosystem of [3]. In this system we construct a sequence of keys for the security.

II. Digital Signature

Digital Signature Generation:

1) In this system we take the field $F_p(\alpha) \cong \frac{F_p\,[x]}{(f(x))}$, where f(x) is a primitive irreducible polynomial of degree n over F_p and $f(\alpha) = 0$.
Let k be a number between 1 and $p^n - 1$, and $g.c.d.(k, p^n - 1) = 1$.
Let $f_k(x)$ be the primitive polynomial with $f_k(\alpha^k) = 0$. Compute k^{-1} modulo $p^n - 1$.
So $kk^{-1} \equiv 1 \pmod{p^n - 1}$. Here, k is the secret number and the polynomials f(x) and $f_k(x)$ be public polynomials of the system.
Select a hash function h.
Let P be the plain text and $h(P) = h(x)$ be the polynomial after hashing the text P.
2) The digital signature is $h_k(x) = (h(x^{k^{-1}}))^k$.

Digital Signature Verification:

Find t such that $x^t \equiv h(x)(\mathrm{mod} f(x))$ (1)
$x^t \equiv h_k(x)(\mathrm{mod} f_k(x))$ (2)

From (1) and (2), $\left(f_k(x)+f(x)\right)x^t \equiv [h(x)f_k(x)+h_k(x)f(x)](\mathrm{mod}f(x)f_k(x))$

$$x^t \equiv [h(x)f_k(x)+h_k(x)f(x)]\left(f_k(x)+f(x)\right)^{-1}(\mathrm{mod}\, f(x)f_k(x))$$

$$x^t \equiv r(x)(\mathrm{mod}\, f(x)f_k(x))$$

Also from (1) and (2) $r(x) \equiv h(x)(\mathrm{mod}f(x))$ and $r(x) \equiv h_k(x)(\mathrm{mod}f_k(x))$
Then, $\left(r(x)-h(x)\right)(r(x)-h_k(x)) \equiv 0(\mathrm{mod}f(x)f_k(x))$ and
$r^2(x)-\left(h(x)+h_k(x)\right)r(x)+h(x)h_k(x) \equiv 0(\mathrm{mod}f(x)f_k(x))$ (3)
The signature verification we have to show that (1) and (2). I.e. $h(x)$ and $h_k(x)$ have same exponent t modulo $f(x)$ and $f_k(x)$ respectively.
The signature $h_k(x)$ is verified if (3) is satisfied.

Example: Digital Signature Generation: 1) n this system we take the field $F_2(\alpha) \cong \frac{F_2\,[x]}{(f(x))}$, where $f(x) = x^3 + x^2 + 1$ is a primitive irreducible polynomial of degree 3 over F_2 and $f(\alpha) = 0$.
Take $k = 3$ and $g.c.d.(3, 2^3 - 1) = 1$.
Then $f_3(x) = x^3 + x + 1$ be the primitive polynomial with $f_3(\alpha^3) = 0$. Compute 3^{-1} modulo $2^3 - 1$ and we get $3^{-1} \equiv 5(\mathrm{mod}7)$.
Here, $k = 3$ is the secret number.
Select a hash functionh.
Let P be the plain text and $h(P) = h(x) = x + 1$ be the polynomial after hashing the text P.
2) The digital signature is $h_3(x) = (h(x^5))^3 \equiv x^2 + x + 1(\mathrm{mod}x^3 + x + 1)$.
Digital Signature Verification: Find t such that
$x^t \equiv (x+1)(\mathrm{mod}x^3 + x^2 + 1)$ (4)
$x^t \equiv (x^2 + x + 1)(\mathrm{mod}x^3 + x + 1)$ (5)
From (4) and (5),

$$(x^2+x)x^t \equiv [(x+1)(x^3+x+1)+(x^2+x+1)(x^3+x^2+1)]\mathrm{mod}(x^3+x^2+1)(x^3+x+1)$$

$$x^t \equiv (x^5+x^4+x^3+x^2+x)(x^2+x)^{-1}(\mathrm{mod}\, x^6+x^5+x^4+x^3+x^2+x+1)$$

$$x^t \equiv (x^5+x^4+x^3+x^2+x)(x^4+x^2+1)(\mathrm{mod}\, x^6+x^5+x^4+x^3+x^2+x+1)$$

$x^t \equiv x^5(\mathrm{mod}x^6+x^5+x^4+x^3+x^2+x+1\,)$
For the signature verification, we have to verify (4) and (5),
I.e. $x^5 \equiv (x+1)(\mathrm{mod}x^3+x^2+1)$ and $x^5 \equiv (x^2+x+1)(\mathrm{mod}x^3+x+1)$

Digital Signature Generation with more than one key:

1) In this system we take the field $F_p(\alpha) \cong \frac{F_p\,[x]}{(f(x))}$, where $f(x)$ is a primitive irreducible polynomial of degree n over F_p and $f(\alpha) = 0$.
Let $k_1, k_2, \ldots\ldots, k_r$ be the numbers between 1 and $p^n - 1$, and $g.c.d.(k_i, p^n - 1) = 1, i = 1$ to r.
Let $f_{k_i}(x)$ be the primitive polynomial with $f_{k_i}(\alpha^{k_i}) = 0, i = 1\ to\ r$. Compute ${k_i}^{-1}$ modulo $p^n - 1$.
So $k_i{k_i}^{-1} \equiv 1\ (mod\ p^n - 1)$. Here, $(k_1, k_2, \ldots\ldots, k_r)$ be the secret sequence.
Select a hash function$h$.
Let P be the plain text and $h(P) = h(x)$ be the polynomial after hashing the text P.
2) Compute $h_{k_i}(x) = (h\left(x^{{k_i}^{-1}}\right))^{k_i}$, i=1 to r.
The signature is $(h_{k_1}(x), h_{k_2}(x), \ldots\ldots\ldots, h_{k_r}(x))$.

Digital Signature Verification: Find t such that

$$x^t \equiv h(x)\left(modf(x)\right),$$
$$x^t \equiv h_{k_1}(x)(modf_{k_1}(x))$$
$$\ldots\ldots\ldots. \qquad (6)$$
$$\ldots\ldots\ldots..$$
$$x^t \equiv h_{k_r}(x)(modf_{k_r}(x)$$

From the above system (6),
$x^t \equiv r(x)(mod\ f(x)f_{k_1}(x)f_{k_2}(x) \ldots f_{k_r}(x))$.
Also from the system $r(x) \equiv h(x)(modf(x))$ and $r(x) \equiv h_{k_i}(x)\left(modf_{k_i}(x)\right), i = 1\ to\ r$, then
$\left(r(x)-h(x)\right)\left(r(x)-h_{k_1}(x)\right)\ldots.(r(x)-h_{k_r}(x)) \equiv 0(modf(x)f_{k_1}(x)f_{k_1}(x)\ldots.f_{k_r}(x))$ (7)
The signature verification we have to show the system (6). I.e. $h(x)$ and $h_{k_i}(x), i = 1\ to\ r,$ have same exponent t modulo $f(x), f_{k_1}(x), f_{k_2}(x), \ldots., f_{k_r}(x)$ respectively.

The signature $(h_{k_1}(x), h_{k_2}(x), \dots \dots \dots, h_{k_r}(x))$ is verified if (7) is satisfied.

III. Security Of The Digital Signature

The security of this digital signature is based on the difficulty of solving DLP. The random selection of the prime number and the size of the extension field are important in this signature. The complexity in computation process of the signature $h_k(x)$ from h(x) is depends upon the complexity of the DLP. The selection of the hash function is an important factor of this signature system. For a polynomial $f_k(x)$ its root as a polynomial $g(\alpha)$ can be found using the algorithm presented in [7]. The complexity of the algorithm is not more than $O(t^3)$. The process is difficult when we work in the field of size with prime extension to be equal at least to 2048. The selection of hash function is also very important. It will be necessary for hash function to satisfy certain properties in order to prevent various attacks.

IV. A Public Key Cryptosystem

In this system we take the field $F_p(\alpha) \cong \frac{F_p\,[x]}{(f(x))}$, where $f(x)$ is a primitive irreducible polynomial of degree n over F_p and $f(\alpha) = 0$.
Let $k_1, k_2, \dots \dots, k_r$ be the numbers between 1 and $p^n - 1$, and $g.c.d.(k_i, p^n - 1) = 1, i = 1\ to\ r.$
Let $f_{k_i}(x)$ be the primitive polynomial with $f_{k_i}(\alpha^{k_i}) = 0, i = 1\ to\ r.$ Compute ${k_i}^{-1}$ modulo $p^n - 1.$
So $k_i {k_i}^{-1} \equiv 1\ (mod\ p^n - 1)$. Here, $(k_1, k_2, \dots \dots, \mathrm{k}_r)$ be the secret sequence.
For a randomly generated N with n bits we compute the following system of congruence equations,

$$\begin{aligned}
&x^N \equiv T_{k_0}(x)(mod\ f(x))\\
&x^N \equiv T_{k_1}(x)(mod\ f_{k_1}(x))\\
&x^N \equiv T_{k_2}(x)(mod\ f_{k_2}(x))\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots.\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots.\\
&x^N \equiv T_{k_{r-1}}(x)(mod\ f_{k_{r-1}}(x))
\end{aligned} \tag{8}$$

Then we can compute the following equations,

$$\begin{aligned}
&T_{k_1}(x) \equiv \left(T_{k_0}\left(x^{{k_1}^{-1}}\right)\right)^{k_1} (mod\ f_{k_1}(x))\\
&T_{k_2}(x) \equiv \left(T_{k_1}\left(x^{{k_2}^{-1}}\right)\right)^{k_2} (mod\ f_{k_2}(x))\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&T_{k_{r-1}}(x) \equiv \left(T_{k_{r-2}}\left(x^{{k_{r-1}}^{-1}}\right)\right)^{k_{r-1}} (mod\ f_{k_{\mathrm{r}-1}}(x))
\end{aligned} \tag{9}$$

Encryption: Suppose we want to encrypt the message M. We can express M as a polynomial M(x) of degree n over F_p, the encryption process is the following,

$$\left\{M.(T_{k_1}(x))^{-1}.(T_{k_2}(x))^{-1} \dots \dots.\left(T_{k_{r-1}}(x)\right)^{-1}, T_{k_0}\left(x^{{k_1}^{-1}}\right), T_{k_1}\left(x^{{k_2}^{-1}}\right), \dots \dots, T_{k_{r-2}}\left(x^{{k_{r-1}}^{-1}}\right)\right\} \tag{10}$$

Decryption:- In the process of decryption, using the key$(k_1, k_2,\dots, k_{r-1})$, compute the following,

$$\begin{aligned}
&(T_{k_{r-2}}(x^{{k_{r-1}}^{-1}}))^{k_{r-1}} = T_{k_{r-1}}(x)\\
&(T_{k_{r-3}}(x^{{k_{r-2}}^{-1}}))^{k_{r-2}} = T_{k_{r-2}}(x)\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots.\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots.\\
&(T_{k_1}(x^{{k_2}^{-1}}))^{k_2} = T_{k_2}(x)\\
&(T_{k_0}(x^{{k_1}^{-1}}))^{k_1} = T_{k_1}(\mathrm{x}).
\end{aligned} \tag{11}$$

And can get M by multiplying the respective element with the first part of the encrypted message.
Or,
From the system (1) we can compute the following,

$$\begin{aligned}
&T_{k_0}(x) \equiv (T_{k_1}(x^{k_1}))^{{k_1}^{-1}}(mod\ f(x))\\
&T_{k_1}(x) \equiv (T_{k_2}(x^{k_2}))^{{k_2}^{-1}}(mod\ f_{k_1}(x))\\
&T_{k_2}(x) \equiv (T_{k_3}(x^{k_3}))^{{k_3}^{-1}}\left(mod\ f_{k_2}(x)\right)\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots
\end{aligned} \tag{12}$$

$T_{k_{r-2}}(x) \equiv (T_{k_{r-1}}(x^{k_{r-1}}))^{{k_{r-1}}^{-1}}(mod\, f_{k_{r-2}}(x))$

Encryption: Suppose M is the message, then the encryption process is the following,

$$\{M.(T_{k_0}(x))^{-1}.(T_{k_1}(x))^{-1} \ldots\ldots (T_{k_{r-2}}(x))^{-1}, T_{k_1}(x^{k_1}), T_{k_2}(x^{k_2}), \ldots\ldots T_{k_{r-1}}(x^{k_{r-1}})\} \quad (13)$$

Decryption:- In the process of decryption, using the key$(k_1, k_2, \ldots, k_{r-1})$, compute the following,

$$(T_{k_{r-1}}(x^{k_{r-1}}))^{{k_{r-1}}^{-1}} = T_{k_{r-2}}(x)$$
$$(T_{k_{r-2}}(x^{k_{r-2}}))^{{k_{r-2}}^{-1}} = T_{k_{r-3}}(x)$$
……………………………. (14)
…………………………….
$$(T_{k_2}(\mathrm{x}^{\mathrm{k}_2}))^{{\mathrm{k}_2}^{-1}} = \mathrm{T}_{\mathrm{k}_1}(\mathrm{x})$$
$$(\mathrm{T}_{\mathrm{k}_1}(\mathrm{x}^{\mathrm{k}_1}))^{{\mathrm{k}_1}^{-1}} = \mathrm{T}_{\mathrm{k}_0}(\mathrm{x}).$$

And can get M by multiplying the corresponding element with the first part of the encrypted message.

V. Security Of The New Cryptosystem

This system is secure provided that the discrete logarithm problem is intractable. In this system the secret key has more than one parameter. The selection of the prime number, the size of the extension field and primitive polynomials are very important in this system. The security of this system depends upon the size of the characteristic of the base field.

VI. Conclusion

In this paper we developed a digital signature and a new cryptosystem based on DLP. The security of these systems is based on the selection of the extension field. All public key operations of these systems can be implemented virtually with the same complexity compared with existing systems. In the presented digital signature the verification part is very easy. The selection of hash function, the prime number, the primitive polynomial and the extension field are very careful in these systems.

References

[1]. Digital Signature Standard, Federal Information Processing Standards Publication 186, May 1994.

[2]. Lilly P.L., Saju M.I., A method of designing a public- key cryptosystem based on discrete logarithm problem, IRJPA-4(11), 2014, 628-630.

[3]. Saju M.I., Lilly P.L., A public key Cryptosystem based on discrete logarithm problem over finite fields $\mathrm{F}_{\mathrm{p}^{\mathrm{n}}}$, IOSR Journal of Mathematics(IOSR-JM)-Vol.11(1), 2015, 01-03.

[4]. Saju M.I., Lilly P.L., A method of designing block cipher involves a key bunch matrix with polynomial entries over F_2, IOSR Journal of Mathematics(IOSR-JM)-Vol.11(2), 2015, 01-04.

[5]. Odlyzko A.., Discrete logarithms: The past and the future; Designs, Codes and Cryptography, (2000), 129-145.

[6]. McCurley K., The discrete logarithm problem, Proceedings of Symposia in Applies Mathematica, Vol.42, 1990, 49-74.

[7]. Taher ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE, Transactions on Information Theory, Vol. IT-31, n.4, 1985, 469-472, also in CRYPTO 84, 10-18, Springer- verlag.