Institute of Advanced Engineering and Science

International Journal of Information & Network Security (IJINS)
Vol.2, No.2, April 2013, pp. 154~159
ISSN: 2089-3299

PKC Scheme Based on DDLP

Chandrashekhar Meshram* and Suchitra A. Meshram**
* Department of Applied Mathematics, Shri Shankaracharya Engineering College, Junwani, Bhilai (C.G.), India
** Department of Mathematics, R.T.M. Nagpur University (M.S.), India

Article Info

Article history:

Received Nov 5th, 2012
Accepted Dec 10th, 2012

Keyword:

Cryptography
Public key cryptosystem (PKC)
Discrete logarithm problem
DDLP

ABSTRACT

This paper introduces the concept of public key cryptosystem, whose security is based on double discrete logarithm problem (DDLP) with distinct discrete exponents in the multiplicative group of finite fields. The adversary has to solve distinct discrete logarithm problems simultaneously in order to recover a corresponding plaintext from the received cipertext. Therefore, this scheme is expected to gain a higher level of security. We next show that, the newly developed scheme is efficient with respect to encryption and decryption and the validity of this algorithm is proven by applying to message that are text and returning the original message in various numerical examples.

Corresponding Author:

Chandrashekhar Meshram,
Department of Applied Mathematics,
Shri Shankaracharya Engineering College,
Junwani, Bhilai (C.G.), 490020, India.
Email: cs_meshram@rediffmail.com

1. INTRODUCTION

The public key algorithms are based on mathematical function rather than substitution and permutation. More important, public key cryptography is asymmetry involving the use of two separate keys, one key for encryption and a different but related for decryption, in contrast to symmetric conventional encryption, which use only one key. Public key encryption is more secure from cryptanalysis than is conventional encryption as it requires no secure transfer of any secret key. The main requirement of public key cryptography is a trap door one way function, which is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known with this information the inverse can be calculated in polynomial time [3]. The security of public key cryptosystem depends on the intractability of a hard problem. The discrete logarithm problem depends on the El-Gamal cryptosystem. In 1976, Diffie and Hellman [2] proposed the revolutionary concept in the field of cryptography, as the public key cryptography, whose security is based on the discrete logarithm problem in the cyclic groups.

In 1985, ElGamal [1] has given thefirst real and practical public key cryptosystem, whose security is based on the difficulty of solving the discrete logarithm problem in the multiplicative group of thefinite fiel d. After the discrete logarithm problem based on several public key cryptosystems came in the existence in the field of secure and practical public key cryptography, some of those are fulfill the standard criteria of public key cryptography and rest are only just review and again review of the original public key cryptosystem.

The proposed algorithms are new techniques that depend on the double discrete logarithm that is more difficult than a single discrete logarithm problem and therefore increases the security of cryptosystem.

2. PRELIMINARIES

2.1 Discrete logarithm problem

Let p be the large prime number, The finite field Z_P= (0, 1, 2, 3, ..., p − 1) (mod p).
Z_p^*= (1, 2, 3, ..., p−1) (mod p)= The multiplicative group of the finite field Z_P .
α = the primitive element.
If

$$Z_p^* = (\alpha^0, \alpha^1, \alpha^2, \dots \dots, \alpha^{P-2}) \text{ (mod p)}$$

Select any element of Z_p^* , i.e

$$\alpha \equiv \beta \ (mod\ p)$$

Then the problem of computing the value of the index x_i is called the discrete logarithm problem of β at the base α under modulo p in the multiplicative group of Z_p^* of the finite field Z_P of order p − 1 and it's denoted mathematically as $x = log_\alpha(\beta)(mod\ p)$.

2.2 Double Discrete logarithm problem

Let p be the large prime number, the finite field Z_P= (0, 1, 2, 3... p − 1) (mod p).
Z_p^*= (1, 2, 3,…….. ,p−1) (mod p) = The multiplicative group of the finite field Z_P .
If $\gamma \equiv \alpha^a \beta^b \ (mod\ p)$ in the multiplicative group of finite field Z_p^* of order $p - 1$ such that $\alpha \neq \beta^i$ and $a \neq b^i$ where α and β are two primitive elements under modulo p,$\gamma \in Z_p^*$, a and b be two distinct random integer.

3. THE ALGORITH FOR COMPUTING THE DISCRETE LOGARITHM PROBLEM

3.1 Baby step giant step (see [5]):

Input: A generator a of a cyclic group G of order n, and element$b \in G$.
Output: the discrete logarithm $x = log_a b$.

```
1.  Set $m \leftarrow \lceil\sqrt{n}\rceil$.
2.  Construct a table with entries $(j, a^j)$ for $0 \le j < m$.
    Sort this table by the second component.
3.  Compute $a^{-m}$ and set $c \leftarrow b$.
4.  For $i$ from 0 to $m - 1$do the following :
    4.1  Check if $c$ the second component of some entry in the table is.
    4.2  If $c = a^j$ then return $(x = im + j)$.
    4.3  Set $c = c\, a^{-m}$.
```

3.2 The pollards rho algorithm for logarithms (see [6]):

Input: A generator a of a cyclic group G of prime order n, and an element $b \in G$.
Output: the discrete logarithm $x = log_a b$.

```
1.  Set $x_0 \leftarrow 1, a_0 \leftarrow 1, b_0 \leftarrow 1$.
2.  For $i = 0,1,2,3\dots$ do the following:
    2.1  Using the quantities $x_{i-1}$, $a_{i-1}$, $b_{i-1}$ and $x_{i-2}$, $a_{i-2}$, $b_{i-2}$, compute previously, compute $x_{2i}$, $a_{2i}$,
         $b_{2i}$using some equations.
    2.2  If $x_i = x_{2i}$ ,then do the following:
         2.2.1  Set $r \leftarrow b_i - b_{2i} mod\ n$.
         2.2.2  If $r = 0$ then terminate the algorithm with failure; else
         2.2.3  Compute $x = r^{-1}(a_{2i} - a_i) mod\ n$.
3.  Return $x$.
```

3.3 The Pohlig-Hellman algorithm (see [7]):

Input: A generator a of a cyclic group G of order n, and an element $b \in G$.
Output: the discrete logarithm $x = log_a b$.

```
1.  Find the prime factorization of $n$: $n = P_1^{e_1} P_2^{e_2} P_3^{e_3} \dots\dots . P_r^{e_r}$, where $e_i \geq 1$.
2.  For $i$ from 1 to $r$ do the following
    2.1  Set $q \leftarrow p_i$ and $e \leftarrow e_i$.
    2.2  Set $c \leftarrow 1$ and $l_{-1} \leftarrow 0$.
    2.3  Compute $\bar{a} \leftarrow a^{n/q}$.
    2.4  For $j$ from 0 to $e - 1$ do the following:
         Compute $c \leftarrow c a^{l_{j-1} q^{j-1}}$ and $\bar{b} \leftarrow (bc^{-1})^{n/q^{j+1}}$.

       Compute$l_j = log_{\bar{a}} \bar{b}$.
    2.5  set $x_i \leftarrow l_0 + l_1 q + l_2 q^2 + \cdots \dots . . + l_{e-1} q^{e-1}$
3.  Use Gauss's algorithm to compute the integer $x, 0 \leq e \leq n - 1$,such that $x \equiv x_i \; mod \; P_i^{e_i}$ for
    $1 \leq i \leq r$.
4.  Return $(x)$.
```

3.4 **The index calculus algorithm**

The index calculus algorithm which was discovered or rediscovered by several authors, Adleman **(see [9]):** or Hellman and Reyneri. **(see [8]):**

Input: A generator a of a cyclic group G of order n, and an element $b \in G$.
Output: the discrete logarithm $x = log_a b$.

```
1.  (select a factor base S)Choose a subset $S = p_1 p_2 p_3 \dots \dots p_t$ of $G$ such that a significant proportion of all
    elements in $G$ can be efficiently expressed as a product of elements from S.
2.  (Collect linear relations involving logarithms of elements in S)
    2.1  Select a random integer $k, 0 \leq k \leq n - 1$, and compute$a^k$.
    2.2  Try to write $a^k$ as a product of elements in $S$: $a^k = \prod_{i=1}^{t} p_i^{c_i}, c_i \geq 0$.
         If successful, take logarithm of both sides of equation to obtain a linear relation:
                 $$k \equiv \sum_{i=1}^{t} c_i log_a p_i mod \; n.$$
    2.3  Repeat step 2.1 and 2.2 until $t + c$ relations of the above form are obtained.
3.  (Find the algorithms of elements in $S$ ) Working $modulo \; n$, solve the linear system of $t + c$
    equations(in $t$ unknowns ) collected in step 2 to obtain the values of $log_a p_i, 1 \leq i \leq t$.
4.  Compute $x$.
    4.1  Select a random integer $k, 0 \leq k \leq n - 1$, and compute $ba^k$.
    4.2  Try to write $ba^k$ as a product of elements in $S$:
                 $$ba^k = \prod_{i=1}^{t} p_i^{d_i}, d_i \geq 0$$
                 $$x = \left(\sum_{i=1}^{t} d_i log_a p_i - k\right) mod \; n.$$
```

4. **THE COMPLEXITY OF DOUBLE DISCRETE LOGARITHM PROBLEM**

Theorem: 1- Double Discrete Logarithm Problem has a complexity in the form of Discrete Logarithm Problem.

Proof: We know that, the mathematical structure of DLP in the multiplicative group of the finite field Z_p^* of order $p - 1$ is defined as follows:

$$\alpha^a = \beta \; mod \; p$$

Taking logarithm of both side of the above equation to the base α:

$$\log \alpha \, (\beta \; mod \; p) \equiv a \tag{1}$$

Now, the mathematical structure of DDLP in the multiplicative group of the finite field Z_p^* of order $p - 1$ is defined as follows:

$$\alpha^a \beta^b \equiv \gamma \; mod \; p \tag{2}$$

Taking logarithm of both side of above equation to the base α, we have,

$$log_{\alpha}(\alpha^{a}\beta^{b}) \equiv log_{\alpha}(\gamma \; mod \; p)$$
$$\Rightarrow \; log_{\alpha}(\alpha^{a}) + log_{\alpha}(\beta^{b}) \equiv log_{\alpha}(\gamma \; mod \; p)$$
$$\Rightarrow \; a \, log_{\alpha} \alpha + b \, log_{\alpha} \beta \equiv \; log_{\alpha}(\gamma \; mod \; p)$$
$$\Rightarrow \; a + \; b \, log_{\alpha} \beta \equiv log_{\alpha}(\gamma \; mod \; p)$$
$$\Rightarrow \; a \equiv log_{\alpha}(\gamma \; mod \; p) - b \, log_{\alpha} \beta$$
$$\Rightarrow \; a \equiv log_{\alpha}(\gamma \; mod \; p) - log_{\alpha}(\beta^{b})$$
$$\Rightarrow \; a \equiv log_{\alpha}\left(\frac{\gamma}{\beta^{b}} \; mod \; p\right) \qquad (3)$$

Again, taking logarithm of both the side of equation (2) to the base β:

$$log_{\beta}(\alpha^{a}\beta^{b}) \equiv log_{\beta}(\gamma \; mod \; p)$$
$$\Rightarrow \; log_{\beta}(\alpha^{a}) + log_{\beta}(\beta^{b}) \equiv log_{\beta}(\gamma \; mod \; p)$$
$$\Rightarrow \; a \, log_{\beta} \alpha + b \, log_{\beta} \beta \equiv \; log_{\beta}(\gamma \; mod \; p)$$
$$\Rightarrow a \, log_{\beta}\alpha + b \; \equiv log_{\beta}(\gamma \; mod \; p)$$
$$\Rightarrow b \; \equiv log_{\beta}(\gamma \; mod \; p) - a \, log_{\beta}\alpha$$
$$\Rightarrow b \; \equiv log_{\beta}(\gamma \; mod \; p) - log_{\beta}(\alpha^{a})$$
$$\Rightarrow \; b \equiv log_{\beta}\left(\frac{\gamma}{\alpha^{a}} \; mod \; p\right) \qquad (4)$$

Equation (1) represents DLP where as equation (2) and (3) represents DDLP involving two distinct discrete logarithm problems in the form of DLP and making the computation of DDLP more difficult.

5. THE PROPOSED PUBLIC KEY ENCRYPTION SCHEME

In this section, we introduce some notations and parameters which will be used throughout this paper: A large number p is safe prime. An integers α and β are two primitive elements of multiplicative group Z_{p}^{*} and element γ of Z_{p}^{*}. Two integers a and b are safe and set $1 \leq a \; b \leq p-2$.

The algorithm consists of three sub algorithms: key generation, encryption and decryption.

1. Key Generation:-

   The key generation algorithm runs as follows:

   1.1 Pick randomly a large prime p and two generators α and β of Z_{p}^{*} .

   1.2 Select two random integer a and b such that $1 \leq a \; b \leq p-2$.

   1.3 Compute $\alpha^{a} mod(\,p)$ and $\beta^{b} mod(\,p)$.

The public key is formed by $(p, \alpha, \beta, \alpha^{a}, \beta^{b})$ and the corresponding secret key is given by (a, b).

2. Encryption:-

   An entity Bob to encrypt a message m to another Alice should do the following:

   2.1 Alice obtain authentic public key $(p, \alpha, \beta, \alpha^{a}, \beta^{b})$.

   2.2 Message $m \in [0, p-1]$.

   2.3 Select two random integer i and j such that $1 \leq i \; j \leq p-2$.

   2.4 Compute $C_1 \equiv \alpha^{i} mod \; (p)$ and $C_2 \equiv \beta^{j} mod \; (p)$.

   2.5 Compute $\gamma = m(\; C_1^{a} C_2^{b} \;) mod \; (p)$.

The cipher text is given by $C = (C_1, \; C_2, \gamma)$.

3. Decryption:-

   To recover the plaintext m from the cipher text

   Alice should do the following:

   3.1 Compute $C_1^{(p-1)-a} mod \; (p) = C_1^{-a} mod \; (p)$ and $C_2^{(p-1)-b} mod \; (p) = C_2^{-b} mod \; (p)$.

   3.2 Recover the plaintext m by computing $(C_1^{-a}, C_2^{-b}, \gamma) mod(p)$.

   3.3 Return the plaintext m.

6. CONSISTENCY OF ALGORITHM

We validate our new scheme by proving the following theorem.

Theorem 2: If the algorithms of key generation and encryption run smoothly then the decryption of the encrypted message in decryption is correct.

Proof: The algorithm above is true for all encrypted message.
Then, in encryption algorithm,

$$C_1 \equiv \alpha^i mod\ (p)$$
$$C_2 \equiv \beta^j mod\ (p)$$
$$\gamma = m(\ C_1^a C_2^b\ )mod\ (p)$$

In Decryption algorithm,

$$C_1^{(p-1)-a} mod\ (p) = C_1^{-a} mod\ (p)$$
$$C_2^{(p-1)-b} mod\ (p) = C_2^{-b} mod\ (p).$$

Then

$$\begin{aligned}(C_1^{-a}, C_2^{-b}, \gamma)mod(p) &= (C_1^{-a} C_2^{-b} m\ C_1^a C_2^b)mod\ (p)\\ &= (C_1^{-a} C_2^{-b}\ C_1^a C_2^b m)mod\ (p)\\ &= m\ mod(p)\end{aligned}$$

7. SECURITY ANALYSIS

The security of cryptosystem based on the intractability of double discrete logarithm problem as an opponent should solve a discrete logarithm problem twice to obtain the private key given the public as following:

In this encryption the public key is given by $(p, \alpha, \beta, \alpha^a, \beta^b)$ and the corresponding secret key is given by (a, b).

To obtain the private key (a) he should solve the DLP

$$a \equiv log_\alpha(\alpha^a)mod\ (p)$$

To obtain the private key (b) he should solve the DLP

$$b \equiv log_\beta(\beta^b)mod\ (p)$$

So, the proposed algorithm is more secure.

Discrete log attack

Say that attacker is able to obtain the secret integer i and j from $C_1 \equiv \alpha^i mod\ (p)$ and $C_2 \equiv \beta^j mod\ (p)$. He could derive the plaintext m if and only if he manages to get $m\ C_1^a C_2^b$.

8. CONCLUSION

In this present paper, we present public key encryption scheme based on double discrete logarithm problem with distinct discrete exponents in the multiplicative group of finite fields. This kind of scheme definitely provides a new scheme with a longer and higher level of security than that based on a double discrete logarithm problem with distinct discrete exponents. The proposed scheme also requires minimal operations in encryption and decryption algorithms and thus makes it is very efficient. The present paper provides the special result from the security point of view, because we face the problem of solving double and triple distinct discrete logarithm problem at the same time in the multiplicative group of finite fields as compared to the other public key cryptosystem, where we face the difficulty of solving the traditional discrete logarithm problem in the common groups.

REFERENCES

[1] T. ElGmal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Trans. Inform. Theory*, vol. 31, pp 469-472, 1995.

[2] W. Diffie, and Hellman M.E., "New direction in Cryptography", *IEEE Trans.Inform.Theory*, vol. 22, pp 644-654, 1976.

[3] S. William, “Cryptography and Network Security: Principles and Practice”, Second ed.Prentice Hall, Upper Saddle River, NWW Jerswy, 1998.

[4] H. K. Rosen, “Elementary Number Theory and its Application” 1984 .

[5] D. E. Knuth, “The Art of Computer Programming-Sorting and Searching”, Addison-Wesley, Reading, Massachusetts, vol. 3, 1973.

[6] J.M. Pollard, “Monte, Carlo methods for index computation (mod p)”, *Mathematics of Computation* vol. 32, pp 918-924, 1978.

[7] S.C. Pohling and M.E. Hellman, “An improved algorithm for computing logarithm over GF (p) and its cryptographic significance”, *IEEE Transactions on Information Theory*, vol. 24, pp 106-110, 1978.

[8] M.E. Hellman and J.M. Reyneri, “Fast computation of discrete logarithms in GF(q)”, *Advanced in Cryptology-Proceedings of Crypto*, vol. 82, pp 3-13, 1983.

[9] L.M. Adleman, “A subexponential algorithm for discrete logarithm problem with applications to cryptography”, Proceedings of the IEEE 20th Annual Symposium on Foundation of Computer Science, pp 55-60, 1979.

BIOGRAPHY OF AUTHORS

Chandrashekhar Meshram received the M.Sc and M.Phil degrees, from Pandit Ravishankar Shukla University, Raipur (C.G.) in 2007 and 2008, respectively and pursuing PhD from R.T.M. Nagpur University, Nagpur (M.S.) India. Presently he is teaching as an Assistant Professor in Department of Applied Mathematics, Shri Shankaracharya Engineering College, Junwani, Bhilai, (C.G.) India. His research interested in the field of Cryptography and its Application, Boundary value problem, Statistics, Raga (Music and Statistics), Neural Network , Ad hoc Network, Number theory, Environmental chemistry, Mathematical modeling, Thermo elasticity, Solid Mechanics and Fixed point theorem. He is a member of International Association of Engineers (IAENG), Hong Kong, World Academy of Science, Engineering and Technology (WASET), New Zealand , Computer Science Teachers Association (CSTA), USA, Association for Computing Machinery (ACM), USA, International Association of Computer Science and Information Technology(IACSIT), Singapore, European Association for Theoretical Computer Science (EATCS), Greece, International Association of Railway Operations Research (IAROR), Netherland, International Association for Pattern Recognition (IAPR), New York , International Federation for Information Processing (IFIP) ,Austria, Association for the Advancement of Computing in Education (AACE),USA, International Mathematical Union (IMU) Berlin, Germany, European Alliance for Innovation (EAI), International Linear Algebra Society (ILAS) Haifa, Israel, Science and Engineering Institute (SCIEI), Machine Intelligence Research Labs (MIR Labs) , USA, Society: Intelligent Systems, KES International Association, United Kingdom, Universal Association of Computer and Electronics Engineers (UACEE), The Society of Digital Information and Wireless Communications (SDIWC) and Life –time member of Internet Society (ISOC),USA ,Indian Mathematical Society , Cryptology Research Society of India and Ramanujan Mathematical Society of India (RMS) and editor in chief of IJRRWC, UK and managing editor of IJCMST, India. He is regular reviewer of thirty International Journals and International Conferences.

Dr. (Mrs) Suchitra A. Meshram received the MSc, M.Phil and PhD degrees, from R.T.M. Nagpur University, Nagpur (M.S.) India. Presently she is teaching as Associate Professor in Department of Mathematics and is having 27 years of teaching experience postgraduate level in University. She is carrying out her research work in the field of Thermo elasticity, Solid Mechanics, Cryptography and its Application. Dr. Meshram published eighteen research papers in National and International Journals.