Journal of Modern Mathematics and Statistics 2 (1): 28-29, 2008
ISSN: 1994-5388
© Medwell Journals, 2008

A PKC Based on Discrete Logarithms in Metacyclic Groups

Sunil Kumar Kashyap, Birendra Kumar Sharma and Amitabh Banerjee
School of Studies in Mathematics, Pt. Ravishankar Shukla University,
Raipur, Chhattisgarh-492010, India

Abstract: We design a Public Key Cryptosystem (PKC), whose security is based on the Discrete Logarithm Problem (DLP) in the Metacyclic Groups. Mathematics Subject Classification Number: 94A60.

Key words: Public Key Cryptosystem (PKC), Discrete Logarithm Problem (DLP), Metacyclic Groups

INTRODUCTION

In this study, we design a public key cryptosystem, whose security is based on the difficulty of solving the discrete logarithm problem in the metacyclic groups.

PRELIMINARIES

Discrete logarithm problem:
Let,

p = The large prime number,
Z_p = $\{0, 1, 2, 3, \ldots, p\text{-}1\}$ mod p = The finite field,
Z_p^* = $\{1, 2, 3, p\text{-}1\}$ mod p = The multiplicative group of the finite field Zp,
α = The primitive element,

If,
$Z_p^* = \{\alpha^0, \alpha^1, \alpha^2, \alpha^3, \ldots, \alpha^{p-2}\}$ mod p,
Select any element of Z_p^*, i.e., $\alpha^x \equiv \beta$ mod p,

Then, the problem of computing the value of the index x, is called the discrete logarithm problem of β at the base α under modulo p in the multiplicative group Z_p^* of the finite field Z_p of the order p-1 and it is denoted mathematically as, $x \equiv \log_\alpha (\beta \bmod p)$.

Metacyclic groups: Let $C_p = \langle a \rangle$ and $C_q = \langle b \rangle$ be (multiplicative cyclic groups of prime orders p and q, respectively such that p<q and q|p-1. Lets be an integer such that $s \neq 0$ (mod p).

There is such an s exists:

- The map $\alpha : C_p \to C_q$ given by $a^i \mapsto a^{si}$ is an automorphism.
- The map $\theta : C_q \to \mathrm{Aut}C_p$ given by $\theta(b^i) = \alpha^i$(α as in part (a)) is homomorphism ($\alpha^O = 1_{cp}$).
- If we write a for (a, e) and b for (e, b), then the group $C_p \times_\theta C_q$ is a group of order pq. Generated by a and b subject to the relations: $|a| = p$, $|b| = q$, $ba = a^s b$, where $s \neq 1(\bmod p)$ and $s^q \equiv 1(\bmod p)$. The group $C_p \times_\theta C_q$ is called the Metacyclic group.

THE DISCRETE LOGARITHMS IN METACYCLIC GROUPS

In this study, we show the discrete logarithms in the metacyclic groups with the help of our following theorem.

Theorem: There exist the two distinct discrete logarithms in the Metacyclic Group $C_p \times_\theta C_q$, which can be represented as follow:

- The computing the value of s from the relation: $|a| = p$, $|b| = q$,$ba = a^s b$
- The computing the value of q from the relation: $s^q \equiv 1$ (mod p).

Proof: We know that, by definition of metacyclic groups: Let $C_p = \langle a \rangle$ and $C_q = \langle b \rangle$ be (multiplicative cyclic groups of prime orders p and q, respectively, such that p<q and q|p-1. Let s be an integer such that $s \neq 0(\bmod p)$.

If, we write a for (a, e) and b for (e, b), then the group $C_p \times_\theta C_q$ is a group of order pq. Generated by a and b subject to the relations: $|a| = p$,$|b| = q$, $ba = a^s b$, where $s \neq 1$ (mod p) and $s^q \equiv 1(\bmod p)$.
Now we study the 2 cases,

Case-1: First we took the relation; $|a| = p$, $|b| = q$, $ba = a^s b$, Here, the problem of computing the value of s is the discrete logarithm problem in the metacyclic groups.

Case-2: Now we study the second relation; $s^q \equiv 1$ (mod p).

Corresponding Author: Sunil Kumar Kashyap, School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur, Chhattisgarh-492010, India

Here, the problem of computing the value of q is the discrete logarithm problem in the metacyclic groups.

Therefore, we can say that after the study of case 1, 2.

There exist the 2 distinct discrete logarithms in the Metacyclic Group $C_p \times_\theta C_q$, which can be represented as follow:

- The computing the value of s from the relation: $|a| = p$, $|b| = q$, $ba = a^s b$.
- The computing the value of q from the relation: $s^q \equiv 1 (\mathrm{mod}\ p)$.

This completes the proof.

THE PROPOSED PUBLIC KEY CRYPTOSYSTEM

In this part of study, we design a public key cryptosystem, whose security is based on the difficulty of computing the proposed discrete logarithms in the metacyclic groups.

The key generation

- Select the metacyclic group.
- Select the public keys, $(a,b,e,C_p,C_q,C_p \times_\theta C_q)$,
- Select the private keys, (s, q).

The encryption

- Select the message, $[m = m_1+m_2]$,
- The ciphertext, $[c_1,c_2,c_3,c_4]$,

where,

$c_1 = (a^k)$

$c_2 = (s^l)$

$c_3 = m_1 (a^s)^k$

$c_4 = m_2 (s^q)^l$

The decryption

- The Plaintext, $[m = m_1+m_2]$,

where,

$m_1 = (c_3).(c_1)^{-s}$,

$m_2 = (c_4).(c_2)^{-q}$

CONCLUSION

In the year 1976, Diffie and Hellman (1976) 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.

But, Elgamal (1985) was given the first real and practical public key cryptosystem, whose security is based on the difficulty of solving the discrete logarithm problem in the multiplicative group of the finite field.

Then after the discrete logarithm problem based several public key cryptosystems came in the existence in the field of secure and practical public key cryptography, but some of those are full fill the standard criteria of public key cryptography, rest are only just review and again review of the original public key cryptosystems.

In present proposed public key cryptosystem, security is based on a very special type of finite cyclic groups, i.e. metacyclic groups, thus our scheme provides the special result as the security point of view, because we face the double trouble of solving the two distinct discrete logarithm problem at the same time in the metacyclic groups as compare to the other public key cryptosystem, where we face the difficulty of solving the traditional discrete logarithm problem in the common groups.

REFERENCES

Diffie, W. and M.E. Hellman, 1976. New directions in cryptography. Transac. Information. Theory, 22: 644-654.

Elgamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transac. Information Theory, 31: 469-472.