# 暗号理論に置ける数論とそのアルゴリズム

Alireza Nemaney Pour(010003)

北陸先端科学技術大学院大学　情報科学研究科

2002 年 8 月 15 日

**キーワード:** Diffie-Hellman, MTI，中間攻撃, 鍵生成，検証機能.

## 1　はじめに

公開鍵配送法は，通信網の利用者が公開鍵を用いて秘密鍵を共有する方法である。秘密鍵を適用する場合，秘密鍵自体を安全でない通信路を介して配送するわけにはいかず，前もって何らかの安全な手段 (例えば，密使や書留郵便など) で通信相手と秘密鍵を共有する必要がある。ところが，公開鍵配送法を用いると，安全でない (盗聴されてもかまわない) 通信路を介して共有の秘密鍵を生成できる。公開鍵配送法では，通信相手同士が公開鍵を交換して計算した結果，この両者のみが知り得るランダムな秘密鍵の値が生成され，それを共有の秘密に用いるのである。公開鍵暗号を用いても秘密鍵の共有はもちろんできるが，公開鍵配送法は理論的にも興味深く，公開鍵暗号よりも簡単に実現できる場合があるので実用性もある。

ディフィ (Diffie) とヘルマン (Hellman) は，1976 年の有名な公開鍵暗号の論文“ *New Directions in Cryptography* ”[3] において公開鍵暗号の原理と共に現在 Diffie-Hellman 鍵配送 (Diffie-Hellman Key Distribution) と呼ばれる鍵配送方式を発表した。彼らの方式は離散対数問題に基づく初めての暗号方式である。

## 2　目的

本研究は下記の特徴をもつような公開鍵配送方式の提案を目的にしている。

1. 中間攻撃に対して安全な共通鍵の生成。
2. Diffie-Hellman の問題の難しさに基づいている方式。
3. 共通鍵の検証機能を備えもっている方式。

共通鍵が中間攻撃に対して安全であれば交信されるメッセージの守秘が守られる。また，検証機能は正しい鍵をもっているかどうか共通鍵を受け取る利用者を安心をさせるための

機能である。この検証機能によって利用者は中間攻撃の被害にあっているかどうか確認できるのである。

# 3 公開鍵配送法

## 3.1 Diffie-Hellman 鍵配送方式

システムは，素数 $p$ を生成し，乗法群 $\mathbb{Z}_p^*$ での原始根 $g$ を求め，これらの値をシステム共通のパラメータとして公開する。

以下の手続きにより，盗聴されてもよい通信路を使って利用者 Alice と利用者 Bob の間で鍵を共有する。

1. Alice は $[1, p-1]$ の間の整数 $x$ を選び，$X \equiv g^x \ (mod\ p)$ を計算する。Alice は $X$ を Bob に送る。
2. Bob は $[1, p-1]$ の間の整数 $y$ を選び，$Y \equiv g^y \ (mod\ p)$ を計算する。Bob は $Y$ を Alice に送る。
3. Alice は $K \equiv Y^x = (g^y)^x = g^{xy} \ (mod\ p)$ を計算し，$K$ を Bob とのあいだの共通鍵とする。
4. Bob は $K' \equiv X^y = (g^x)^y = g^{xy} \ (mod\ p)$ を計算し，$K'$ を Alice とのあいだの共通鍵とする。

明らかに，$K = K'$ であるため，Alice，Bob 間での鍵の共有が可能となる。

この方式では，通信している相手を確認することができないため，Alice と Bob の間に攻撃者 Lucy が通信を介在すれば，暗号鍵を共有できる。つまり，Lucy は Alice と Bob の間に入り，Alice に対しては Bob になりすまし，Bob に対しては Alice になりすますことができる。下記の図はこの攻撃を表したものである。

$$Alice \xrightarrow{g^x} Lucy \xrightarrow{g^{x'}} Bob$$
$$Alice \xleftarrow{g^{y'}} Lucy \xleftarrow{g^y} Bob$$

このとき，Lucy は Alice-Lucy 間で鍵 $g^{xy'}$ を共有し (Alice はそれを $g^{xy}$ だと信じている)，Bob-Lucy 間で鍵 $g^{x'y}$ 共有する。当然，Lucy は平文の内容をすべて解読できる。このような中間攻撃を防ぐためには，認証機能を伴用すればよい。

## 3.2 MTI/C1 鍵配送法

ここで，利用者 Alice と利用者 Bob はそれぞれ秘密鍵 $x$ と $y$ を保持し，公開鍵 $X \equiv g^x \ (mod\ p)$ と $Y \equiv g^y \ (mod\ p)$ は認証されて登録されているとする。また，素数 $p$ とその原始根 $g$ は公開されている。

1. Alice は $[1, p-2]$ の間の整数 $r$ をランダムに選び，$Z \equiv Y^{rx} = g^{rxy} \ (mod\ p)$ を計算する。Alice は $Z$ を Bob に送る。
2. Bob は $[1, p-2]$ の間の整数 $r'$ をランダムに選び，$Z' \equiv X^{r'y} = g^{r'xy} \ (mod\ p)$ を計算する。Bob は $Z'$ を Alice に送る。
3. Alice は配送情報 $Z'$ より共有鍵 $K$ を次のように生成する。

$$K \equiv Z'^{r} = g^{xyrr'} \ (mod\ p).$$

4. Bob は配送情報 $Z$ より共有鍵 $K'$ を次のように生成する

$$K' \equiv Z^{r'} = g^{xyrr'} \ (mod\ p).$$

なお，MTI/C1 の手順は $g^{xy} \ (mod\ p)$ をいったん，Diffie-Hellman 型公開鍵配送法で共有してから，それぞれ $(g^{xy})^{r} \ (mod\ p)$，$(g^{xy})^{r'} \ (mod\ p)$ を計算して $Z$ と $Z'$ を求めている。結果的には同じ共有鍵が得られます。

## 4 公開鍵配送方式の提案

この方式は三つの段階; 登録, 交換，鍵の生成の段階である。鍵の生成と同時に鍵の検証も行われる。

### 4.1 登録段階

ここで，利用者 Alice と利用者 Bob はそれぞれ秘密鍵 $x$ と $y$ を $2 \leq x, y \leq p-2$ の間から選び，公開鍵 $X \equiv g^{x} \ (mod\ p)$ と $Y \equiv g^{y} \ (mod\ p)$ は認証されて公開ファイルに登録されているとする。また，素数 $p$ とその原始根 $g$ は公開されている。

### 4.2 交換，鍵の生成段階と鍵の検証機能

1. Alice は $r$ を $[\,2\,, p-2]$ の間からランダムに選ぶ。
2. Alice は共通鍵として $K \equiv Y^{rx} = g^{rxy} \ (mod\ p)$ を計算する。
3. Bob は $gcd(r', p-1) = 1$ の条件を満たすような整数 $r'$ を $[\,2\,, p-2]$ の間からランダムに選ぶ。また，Bob は $r'$ の逆元 $\overline{r'}$ を次の式から計算する。 $r'\overline{r'} \equiv 1 \ (mod\ p-1)$.
4. Bob は $Z' \equiv X^{r'y} = g^{r'xy} \ (mod\ p)$ と $v' \equiv g^{r'} \ (mod\ p)$ を計算してから $(Z', v')$ を Alice に送る。
5. Alice は $Z \equiv Z'^{r} = g^{rr'xy} \ (mod\ p)$ と $v \equiv X^{r} \cdot v'^{x} = g^{x(r+r')} \ (mod\ p)$ を計算してから $(Z, v)$ を Bob に送る。
6. Bob は

$$K' \equiv Z^{\overline{r'}} = g^{r(r'\overline{r'})xy} = g^{rxy} \ (mod\ p).$$

と

$$K' \equiv v^y \cdot X^{-r'y} = g^{rxy} \ (mod\ p).$$

を計算して，求まった値 $Z^{\overline{r'}} = v^y \cdot X^{-r'y}$ が等しいかどうか検証を行う。 もし同じ値が得られたら，生成された鍵は受理され，そうでなければ受理されない。

## 5 成果および今後の課題

本研究から下記のような成果が得られている。

1. 生成された共通鍵は中間攻撃に対して安全である。
2. この方式は Diffie-Hellman 問題の難しさに基づいている。
3. 鍵の検証機能は鍵を受け取る利用者に正しい鍵を持っているかどうか安心させる。
4. 鍵は毎回ランダム数によって更新されるため，鍵の生成は非決定的である。

今後の課題として，この方式を 3 人以上の間に拡張が必要である。もしこの方式不特定多数の間で利用できるように拡張可能であれば，会議鍵配送方式としても利用可能になる。また，この方式は ElGamal 暗号と MTI/C1 の機能を同時に備えもっているため，Elgamal 暗号のように利用可能である。しかし，そのとき，ElGamal 暗号のように中間攻撃に対してその安全性が失われる。

## 参考文献


[1] Neal Koblitz,“*A Course in Number Theory and Cryptogaphy* ”, Second Edition, Springer, (1994).

[2] 遠山 啓,“初等整数論 ”, 日評数学選書 : 日本評論社, (1992).

[3] Whitfield Diffie and Martin E. Hellman,“*New Directions in Cryptography* ” Invited Paper, (1976).

[4] Tsutomu Matsumoto, Youichi Takashima, and Hideki Imai,“*On seeking Smart Public-Key-Distribution Systems* ” The Transactions of the IECE of Japan, Vol. E **69**, No. 2, (1986).

[5] Simon Blake-Wilson, Don Johnson, Alfred Menezes,“*Key Agreement Protocols and their Security Analysis* ” (1997).