

# 鍵配送方式

環境情報学部 4年 石原和音

学籍番号 70050607

[t00069ki@sfc.keio.ac.jp](mailto:t00069ki@sfc.keio.ac.jp)

2006年5月4日

## 1. 鍵配送方式が必要となる背景

共通鍵暗号方式とは、暗号の送信者と受信者が、同じ鍵を使って暗号通信をする方式である。すなわち、共通鍵暗号においては、通信相手(送信者もしくは受信者)と必ず同じ鍵を持っていないてはならない。また、他の利用者による盗聴傍受を防ぐためには、それぞれの通信相手について、異なる鍵を利用しなければならない。よって、共通鍵暗号方式では、おおまかに言って、利用者の数の自乗の共通鍵が必要となる。

この条件の下で、古くからの方法と鍵配送方式を比較する。

### 古くからの方法    あらかじめ鍵を共有しておく方式

鍵配送方式以前の古くからの方法では、通信相手と同じ鍵を持つということは、各利用者が、通信相手となりうる利用者全員と鍵をあらかじめ共有していかないてはならない、ということである。たとえば100人の利用者を相手に暗号通信するためには、100種類の鍵をあらかじめ交換しておくことになる。100人程度の小規模なネットワークならば、この方法も現実的な方法であろう。

しかし、通信ネットワーク<sup>1</sup>が発達した現在、暗号通信の利用者となりうる相手は100人、というわけにはいかない。たとえば、1万人の暗号通信利用者のいる会社組織において、それぞれが1万人の利用者を相手に暗号通信をするためには、それぞれが1万種類の鍵をあらかじめ交換しておく必要がある。1万×1万の1億種類の鍵が必要であり、それぞれに管理のコストがかかる。利用者が1万人ならば、まだ辛うじて可能かもしれない。しかし、たとえば商用の通信などで、全人類が暗号通信の対象となりうる<sup>2</sup>とすれば、各利用者は訳60億の共通鍵を管理しなくてはならないことになる。共通鍵の総数は60億×60億=3600京が必要である。3600京の共通鍵それぞれに管理コストが発生する。しかも、新しい人間がどんどん産まれてくる。暗号通信の前にあらかじめ鍵を共有しておくためには、世界中の新生児と暗号鍵を交換してまわらなくてはならない。これは言うまでもなく非現実的である。

### 新しい方法    鍵配送方式

鍵配送方式とは、公開された通信経路<sup>2</sup>を使っていながら、秘密裏に共通鍵を共有することのできる方法である。鍵配送方式を用いれば、共通鍵が必要になった時にはじめて、共通鍵を「配送」すればよい。オン・デマンドで共通鍵を交換するわけである。暗号通信をする可能性のある相手が60億人居たとしても、実際に暗号通信が必要となるのはそのうちのごく一部である。このように、オン・デマンドで共通鍵を共有できれば、鍵管理のコストは劇的に低くなる。また、暗号通信をする利用者が新しく出てきても、鍵を共有することが出来る。何らかの理由で共通鍵を更新する必要が出て、新しい共通鍵を「配送」できれば、鍵の管理にかかるコストはぐっと安くなる。

1 インターネットに代表される

2 通信は盗聴されると仮定する

## 2.鍵配送方式

### 古い鍵配送方式 共通鍵による3者モデル

素朴な鍵配送の実現方法として、共通鍵暗号を利用した3者モデルがある。双方の利用者が信頼する共通鍵配送者に、共通鍵を中継・配送してもらう方法である。共通鍵配送者との間の共通鍵はあらかじめ共有しておく。この方法は比較的小規模なネットワークにおいては実用されている。<sup>3</sup>しかし、大規模なネットワークには「双方の利用者が信頼できる共通の共通鍵配送者」は存在しないと考えたほうがよい。また、少数の共通鍵配送者で全利用者間の共通鍵の中継をこなすことは、負荷の点からも不安が残る。また、ネットワーク的にも脆弱である<sup>4</sup>。このように、3者モデルによる鍵配送方式には問題点がある。

### より新しい鍵配送方式

公開鍵暗号を使った鍵配送方式のプロトコルは、以下のような関数  $F$  があれば実現できる。利用者 A は秘密鍵  $a$  となる乱数を、利用者 B は秘密鍵  $b$  となる乱数を持っているとする。以下の条件を満たす関数  $F$  <sup>5</sup>

(ア)  $F(a)$  と  $b$  から、 $F(b)$  と  $a$  から、 $K$  を計算できる。

- i. Aさんの公開鍵となる  $F(a)$  と、Bさんの秘密鍵  $b$  から、共通鍵  $K$  を計算できる。
- ii. Bさんの公開鍵となる  $F(b)$  と、Aさんの秘密鍵  $a$  から、共通鍵  $K$  を計算できる。

(イ)  $F(x)$  の値から  $x$  を逆算することは困難。<sup>6</sup>

(ウ) 2つの公開鍵  $F(a)$ 、 $F(b)$  から  $K$  を計算することは困難。

この関数  $F$  をつけた鍵配送方式のプロトコルは以下のようなものである。

① 相互に公開鍵を交換する

- i. Aさんは  $F(a)$  の値をBさんに送る
- ii. Bさんは  $F(b)$  の値をAさんに送る

② 共通鍵を計算する

- i. Aさんは受け取った  $F(b)$  と  $a$  から  $K$  を計算
- ii. Bさんは受け取った  $F(a)$  と  $b$  から  $K$  を計算

③ AさんとBさんは共通鍵  $K$  を使って暗号通信をする

このプロトコルでは、通信されるデータは  $F(a)$  と  $F(b)$  のみであり、盗聴者は  $K$  を計算することが困難である<sup>7</sup>。

3 マサチューセッツ工科大学において開発された Kerberos に代表される

4 少数の「ハブ」が中継を行うスター型ネットワークは、「ハブ」が集中的に攻撃にさらされるため脆弱である

5 多数の利用者が暗号通信に使うのであるから、当然、その関数は公開されたものでなくてはならない

6  $F$  の逆関数  $F^{-1}$  の計算には莫大な時間がかかる。この性質を非対称性、強一方向性とも言う

7 関数  $F$  の条件イ・ウによりこれが言える

## 公開鍵暗号による鍵配送の具体例 DH 鍵配送方式<sup>8</sup>

DH 鍵配送方式において、関数  $F$  は  $F_{g,p}(a) = g^a \bmod p$  である。 $g$  (原始元)と  $p$  (法)を与えられると  $F$  は決まる。 $g$  と  $p$  は公開されていてよい。

この  $F$  はアの条件を満たす。

$$\begin{aligned}(F_{g,p}(a))^b \bmod p &= (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = K \\ (F_{g,p}(b))^a \bmod p &= (g^b \bmod p)^a \bmod p = g^{ba} \bmod p = g^{ab} \bmod p = K\end{aligned}$$

この  $F$  の逆関数は  $F_{g,p}^{-1}$  は離散対数問題となる。よってイの性質を満たす。すなわち、 $g^a \bmod p$  の値から  $a$  を逆算することは困難である。ただし、 $p$  や  $g$  などを適切に選ばなくてはならない。たとえば  $p$  は十分に大きくなくてはならない。

ウの性質については、残念ながら調査することができなかった。

### DH 鍵配送方式の数値による具体例

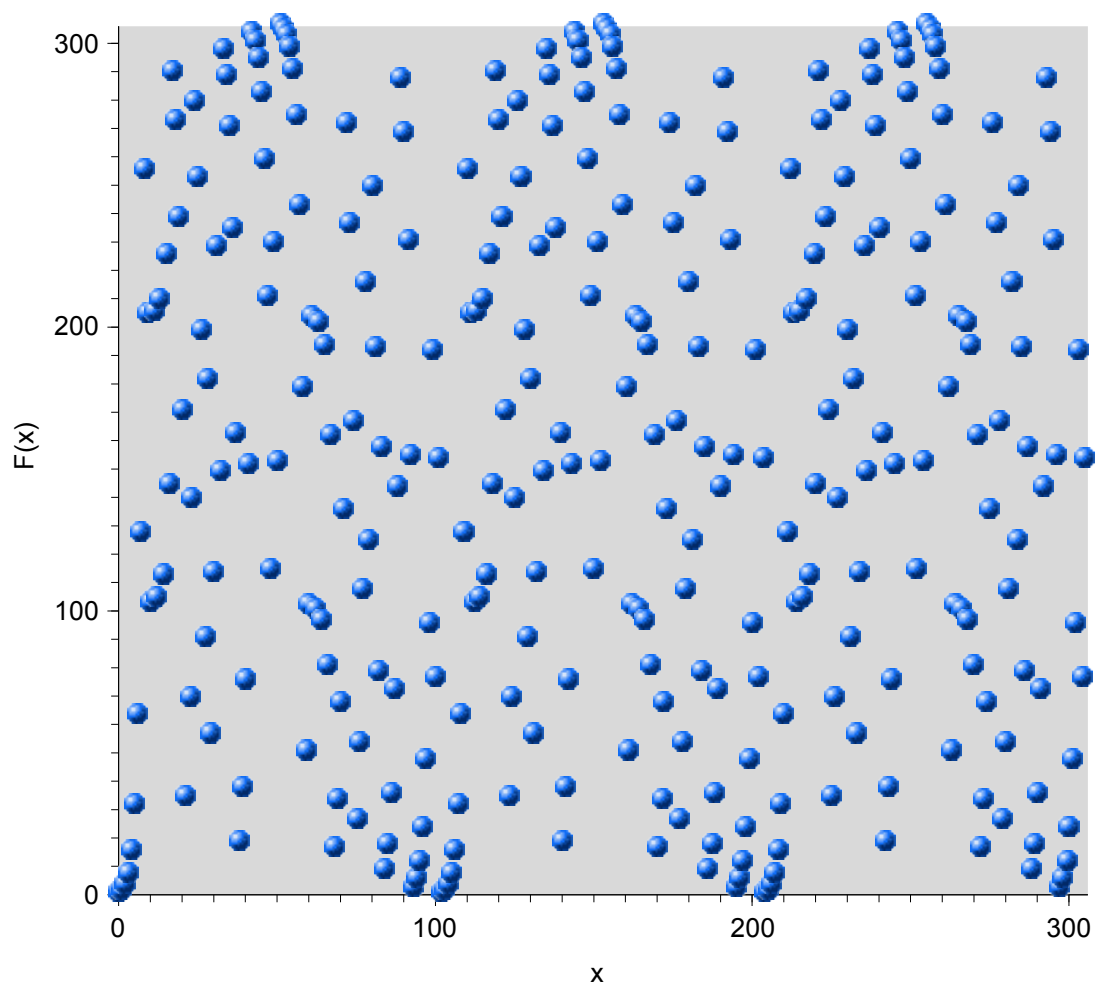
$p=307$  とする。 $g=2$  とする。

$F = F_{2,307}(x) = 2^x \bmod 307$  である。

Aさんは秘密鍵  $a=213$  を作る。

Bさんは秘密鍵  $b=132$  を作る。

- ① 相互に公開鍵を交換する
  - i. Aさんは公開鍵  $2^{213} \bmod 307 = 205$  をBさんに送る。
  - ii. Bさんは公開鍵  $2^{132} \bmod 307 = 114$  をAさんに送る。
- ② 共通鍵を計算する
  - i. Aさんは  $114^{213} \bmod 307 = 81$  を計算し、 $K=81$  を得る。
  - ii. Bさんは  $205^{132} \bmod 307 = 81$  を計算し、 $K=81$  を得る。
- ③ AさんとBさんは共通鍵  $K=81$  を使って暗号通信をする



## 補足と考察

- $2^{102} \bmod 307 = 1$   $2^{204} \bmod 307 = 1$  となるので、 $g=2$  は原始元ではない。このため、 $F = F_{2,307}(x) = 2^x \bmod 307$  の値域の要素数は(原始元であった場合の)3分の1に減少している。3回の重複が生じているということである。上のグラフを見ても明らかにパターンが見て取れる。これが暗号の強度低下に結びつくのであろう。これを避けるために、 $g$  に原始元を選ぶことが求められるのだらう。
- $g'=5$   $g''=13$  などならば原始元であったようだ。先にこれを計算しておかなかったことが悔やまれる。
- もちろん  $2^{307-1} \bmod 307 = 1$  となり、フェルマーの小定理が成立する。
- 以上の計算には表計算ソフトウェア OpenOffice.org Calc を用いた。