群と暗号：Diffie Hellman鍵交換

松本　眞:m-mat @ math.sci.hiroshima-u.ac.jp

平成21 年4 月9 日

1　暗号

- A さんがB さんに、秘密の文字の列を通信路経由で送りたい。
- 通信路を流れる情報は、知られたくないC さんに漏洩してしまう。
- A さんは送りたい文字の列を暗号化してから通信し、B さんは受け取ってから復号化する。

簡単のため、仮定：

1. 文字はひらがななど、１００種類未満とする
2. 00-99 の数と、一文字を対応させる：

   00-あ、01-い、02-う、. . . 45-ん、. . .。
3. 送りたい文字はちょうど４文字。⇒ １０進で８桁

   あいたい↦00 01 15 01 = 00011501

この数と文字の対応は、C さんも知っているとする。

1.1　共有鍵暗号

- A さんとB さんがあらかじめ会って、１０進で８桁の秘密の鍵を打ち合わせておく。

  例:31415926
- A さんの暗号化：

  $00011501 + 31415926 \mod 100000000 = 31427427$ の下８桁を、暗号として送る

- B さんの復号化：

  $31427427 - 31415926 \mod 100000000 = 00011501$

- C さんは、鍵が 31415926 だとは知らないので復号できない。

2　会わずに行う鍵の交換

A さんと B さんが直接会ったりせずに、C さんに見られている通信路を使って鍵を共有することはできないか？

⇒ Diffie Hellman 暗号系

p を 100000000 より大きい整数とする。以下の計算は $\mathbb{Z}/p$ の中で行う。

1. $a \in \mathbb{Z}/p$ を決めて、a, p をみんなに公開する。
2. A さんは $n \in \mathbb{Z}/p$ をでたらめに選ぶ (だれにも教えず記録しておく)
3. B さんは $m \in \mathbb{Z}/p$ をでたらめに選ぶ (だれにも教えず記録しておく)
4. A さんは、a^n を計算して通信路で B さんに送る
5. B さんは、a^m を計算して通信路で A さんに送る
6. A さんは、受け取った数を n 乗して結果を鍵とする
7. B さんは、受け取った数を m 乗して結果を鍵とする

事実：p が大きいとき、$a \in \mathbb{Z}/p$ に対して a^n を計算することは計算機を使えば容易だが、a と a^n が与えられて n を求めることは計算が著しく難しい

1. C さんが見られる情報：a, a^n, a^m
2. A さんだけが持っている情報 n
3. B さんだけが持っている情報 m
4. B さんが送ってきたものを n 乗すれば A さんは $(a^m)^n$ を得る
5. A さんが送ってきたものを m 乗すれば B さんは $(a^n)^m$ を得る

$\mathbb{Z}/p$ では $(a^m)^n = (a^n)^m$。これにより、A さんと B さんが秘密の共有鍵をもつことができる。(上の 31415926 の代わりに使う。)

レポート問題 2.1. 上の「$\mathbb{Z}/p$ では $(a^m)^n = (a^n)^m$」を示せ。

一般に、a が半群の元なら $(a^m)^n = (a^n)^m$ となることを証明せよ。

結合法則が成り立たない場合には、これが成立しない例があることを示せ。

上の通信方法では、$(\mathbb{Z}/p, \times, 1)$ が半群だということしか使っていない。したがって、半群があれば Diffie Hellman 暗号系をつくることができる。

問題は、「a^n, a から n を求めるのが困難」なのはどんな半群なのか、よくわかっていないことである。$(\mathbb{Z}/p, \times, 1)$ ではある種の素数 p が有望である。他に、楕円曲線を用いてつくった大きな群が有望とされている。

レポート問題 2.2. もし、半群として $(\mathbb{Z}/p, \times, 1)$ ではなく $(\mathbb{Z}/p, +, 0)$ を用いたら、共有鍵 $(nm)a$ は C さんにより比較的容易に見破られてしまう。これについて考察せよ。