サイエンス・パートナーシップ・プロジェクト

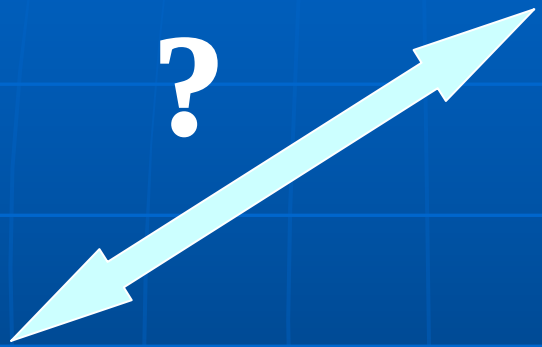
暗号の基礎から実用まで

第3部：公開鍵暗号の基礎

高知大学 理学部 応用理学科
塩 田 研 一
mail: shiota@is.kochi-u.ac.jp
http://lupus.is.kochi-u.ac.jp/~shiota/

2009年9月7日

前回の復習



- 四則演算
- べき乗計算
- 最大公約数
- てんびんクイズ
- 素因数分解
- 素数判定

- 当たり前に高速にできる計算
- 工夫をすれば高速にできる計算
- どんなに工夫しても高速にはならない計算

前回の復習

- 当たり前に高速にできる計算
  - 四則演算
- 工夫をすれば高速にできる計算
  - 最大公約数
  - てんびんクイズ
  - 素数判定
  - べき乗
- どんなに工夫しても高速にはならない計算
  - 素因数分解

今日は

- 当たり前に高速にできる計算
- 工夫をすれば高速にできる計算
- どんなに工夫しても高速にはならない計算

を組み合わせて暗号を作りましょう。

目　次

- 法演算
- フェルマの小定理
- 法べき乗暗号
- 公開鍵暗号方式
- 法べき乗暗号は公開鍵暗号ではない
- RSA暗号
- RSA暗号は公開鍵暗号である

法演算とは

- 「法」と呼ぶ数 n を決めて
- n で割った余りに置き換えて計算すること

法＝7 の例

$$5 + 6 \equiv 4 \pmod 7$$
$$2 - 6 \equiv 3 \pmod 7$$
$$3 \times 4 \equiv 5 \pmod 7$$
$$3 \div 5 \equiv 2 \pmod 7$$

練習問題

法＝2 のとき

$$1 + 1 \equiv ? \quad (\mathrm{mod}\ 2)$$
$$0 - 1 \equiv ? \quad (\mathrm{mod}\ 2)$$

法＝5 のとき

$$2 + 3 \equiv ? \quad (\mathrm{mod}\ 5)$$
$$2 - 3 \equiv ? \quad (\mathrm{mod}\ 5)$$
$$2 \times 3 \equiv ? \quad (\mathrm{mod}\ 5)$$

練習問題

法＝2 のとき

$$1 + 1 \equiv 0 \pmod 2$$
$$0 - 1 \equiv 1 \pmod 2$$

法＝5 のとき

$$2 + 3 \equiv 0 \pmod 5$$
$$2 - 3 \equiv 4 \pmod 5$$
$$2 \times 3 \equiv 1 \pmod 5$$

実　習

サンプルプログラム「フェルマの小定理」を実行してみよう

1. Macintosh HD をダブルクリック
2. 家の絵のアイコンをクリック
3. 03_Shiota をクリック
4. フェルマの小定理 をダブルクリック
5. ↑キーと return で再実行

フェルマの小定理

こんな法則がみつかりましたか？

法 n が素数ならば、任意の整数 x に対して

$$x^n \equiv x \pmod{n}$$

が成り立つ。

Q & A

ご質問、ご意見ありましたら

練習問題

$n = 7$ のとき

$$3^{100} \equiv ? \quad (\mathrm{mod}\ 7)$$

解

フェルマの小定理より

$$3^{100} \equiv 3^7 \times 3^{93} \pmod 7$$
$$\equiv 3 \times 3^{93} \pmod 7$$
$$\equiv 3^{94} \pmod 7$$

この計算を続けると

$$3^{100} \equiv 3^{94} \equiv 3^{88} \equiv \cdots \equiv 3^4$$
$$\equiv 81 \equiv 4 \pmod 7$$

法則

解を一般化すると

法 n が素数ならば、

$$x \equiv x^{n} \equiv x^{2n-1} \equiv x^{3n-2} \equiv \cdots \pmod{n}$$

が成り立つ。

n に色々な素数を入れてみると

$$x \equiv x^5 \equiv x^9 \equiv x^{13} \equiv x^{17} \cdots \pmod 5$$

$$x \equiv x^7 \equiv x^{13} \equiv x^{19} \equiv x^{25} \cdots \pmod 7$$

$$x \equiv x^{11} \equiv x^{21} \equiv x^{31} \equiv x^{41} \cdots \pmod{11}$$

etc.

その中で…

$$x \equiv x^{9} \quad (\bmod 5)$$

$$x \equiv x^{25} \quad (\bmod 7)$$

$$x \equiv x^{21} \quad (\bmod 11)$$

のような式に着目

それをこう書き換える:

$$x \equiv (x^3)^3 \pmod 5$$

$$x \equiv (x^5)^5 \pmod 7$$

$$x \equiv (x^3)^7 \pmod{11}$$

法べき乗

こんな法則が見えてきましたね。

法 n が素数、e, d が

$$ed \equiv 1 \pmod{n-1}$$

を満たす数ならば、

$$y \equiv x^e \pmod{n}$$

$$\Leftrightarrow \quad x \equiv y^d \pmod{n}$$

が成り立つ。

証　明

$$x \equiv (x^e)^d \pmod{n}$$

が成り立つので、これに $y \equiv x^e \pmod{n}$

を代入すると $x \equiv y^d \pmod{n}$

逆に

$$y \equiv (y^d)^e \pmod{n}$$

も成り立つので、これに $x \equiv y^d \pmod{n}$

を代入すると $y \equiv x^e \pmod{n}$

Q & A

ご質問、ご意見ありましたら

法べき乗暗号のアイデア

$$y \equiv x^e \pmod{n}$$
$$\Leftrightarrow \quad x \equiv y^d \pmod{n}$$

の法則の意味:

$\mathbf{mod}\ n$ で数を e 乗すると
d 乗で元へ戻る

法べき乗暗号

- 暗号化:

$$y = f(x) = \mathrm{MOD}(x^e, n)$$

- 復号化:

$$g(y) = \mathrm{MOD}(y^d, n)$$

ただし $\mathrm{MOD}(x,n)$ は x を n で割った余り

e : 暗号化指数, d : 復号化指数 と呼ぶ

実習（鍵生成）

1. 「法べき乗暗号の鍵生成」をダブルクリック
2. 64ビット位で実行してみましょう
3. 03_Shiota のウィンドウをクリックすると
   - 「暗号化指数」のファイル　MPEK.txt
   - 「復号化指数」のファイル　MPDK.txt

   ができているはずです。

実習（暗号化）

「やぎさんゆうびん」の歌詞を暗号化してみましょう

1. YagisanYuubin.txt のアイコンを「法べき乗暗号暗号化」のアイコンへドラッグ&ドロップ
2. MPCYagisanYuubin.txt というファイルができているはず

実習（復号化）

MPCYagisanYuubin.txt を復号化してみましょう

1. MPCYagisanYuubin.txt のアイコンを「法べき乗暗号復号化」のアイコンへドラッグ&ドロップ
2. MPDYagisanYuubin.txt というファイルができているはず

実習（ 画像ファイルの暗号化 ）

今度は猫の絵を暗号化・復号化してみましょう

1. 2006_3_3s.gif のアイコンを「法べき乗暗号暗号化」のアイコンへドラッグ&ドロップ
2. MPC2006_3_3s.gif というファイルができているはず
3. MPC2006_3_3s.gif のアイコンを「法べき乗暗号復号化」のアイコンへドラッグ&ドロップ

参考URL

授業で使用した猫の絵は

ドンゴラスけ林のフリー素材
http://dongorasu.hp.infoseek.co.jp/osouzai.htm

のページから拝借致しました。

Q & A

ご質問、ご意見ありましたら

昔ながらの暗号は

暗号の送信者と受信者が同じ「鍵」を使う

⇒　ネット時代では不都合が

1. 膨大な個数の「鍵」が必要
2. 「鍵」の打ち合わせが不可能

公開鍵暗号方式とは

送信者は「錠前」を

受信者は「鍵」を

公開鍵暗号方式

- 暗号化関数 $f(x)$ を公開
- 復号化関数 $g(y)$ は自分だけの秘密
- 自分への暗号文を $f(x)$ で作ってもらって $g(y)$ を使って読む

- 大事なこと:

  $f(x)$ からは $g(y)$ が計算できないこと

法べき乗暗号は公開鍵暗号ではない

- 錠前: n と e
- 鍵: d
- d の計算方法:

  e と n-1 をてんびんプログラムに入力

  ⇒ 出力:

  $e\,u + (n\text{-}1)\,v = 1$ を満たす u, v

  ⇒ この u が d

高速!!

Q & A

ご質問、ご意見ありましたら

RSA暗号とは

- 1977年、世界初の公開鍵方式の暗号
- 法べき乗暗号をもうひとひねり：

  n を、素数ではなく、

  二つの素数の積にする

  $$n = p \times q$$

RSA暗号の変換式

は法べき乗暗号と同じく

- 暗号化:

$$y = f(x) = \mathrm{MOD}(x^{e}, n)$$

- 復号化:

$$g(y) = \mathrm{MOD}(y^{d}, n)$$

RSA暗号の復号化指数 d

- d の計算方法:

n の素因数 p, q が必要!!

e と $(p\text{-}1)(q\text{-}1)$ をてんびん

プログラムに入力

⇒ 出力: $e\,u + (p\text{-}1)(q\text{-}1)\,v = 1$ を満たす u, v

⇒ この u が d

RSA暗号の安全性

- 復号化指数 d の計算には素因数分解が必要

… 事実上実行不可能 !!

Q & A

ご質問、ご意見ありましたら

実習（鍵生成）

1．「RSA暗号の鍵生成」をダブルクリック

2．64ビット位で実行してみましょう

3．03_Shiota のウィンドウをクリックすると

- 「錠前」のファイル　RSAP.txt
- 「鍵」のファイル　RSAS.txt

ができているはずです。

実習（暗号化）

さっきと同様に「やぎさんゆうびん」の歌詞を暗号化してみましょう

1. YagisanYuubin.txt のアイコンを「RSA暗号化」のアイコンへドラッグ&ドロップ
2. RSACYagisanYuubin.txt というファイルができているはず

実習（復号化）

RSACYagisanYuubin.txt を復号しましょう

1. RSACYagisanYuubin.txt のアイコンを「RSA復号化」のアイコンへドラッグ&ドロップ
2. RSADYagisanYuubin.txt というファイルができているはず

実習（画像ファイルの暗号化）

同様に猫の絵も暗号化してみましょう

1. 2006_3_3s.gif のアイコンを「RSA暗号化」のアイコンへドラッグ&ドロップ
2. RSAC2006_3_3s.gif というファイルができているはず
3. RSAC2006_3_3s.gif のアイコンを「RSA復号化」のアイコンへドラッグ&ドロップ

Q & A

ご質問、ご意見ありましたら

まとめ

- 公開鍵暗号で大事なこと:

  暗号化関数からは復号化関数が計算できないこと

- RSA暗号の正規ユーザが使う計算
  - 鍵生成: 素数判定、てんびんプログラム
  - 変換式: 法べき乗　… 全て高速
- RSA暗号への攻撃者が使う計算
  - 素因数分解　… 天文学的時間が掛かる

Q & A

ご質問、ご意見ありましたら

今日の後半は

実用の暗号ツールを使う実習です。