高校生のための現代数学講座　　東京大学
「素数」　　玉原国際セミナーハウス
講義 (2)　高木　俊輔　　2012 年 7 月 28 日

「ＲＳＡ暗号」

暗号とは, 秘密裏に通信するために当事者間でのみ了解されるように決めた特殊な記号, あるいは特殊な方法によって通信しようとする文書に変形を加えることである. 通信しようとする文章を**平文**（ひらぶん）といい, 変形した文章を**暗号文**という. 暗号文を平文に戻す道具を**鍵**という. かつては, 暗号は戦争で敵に知られず連絡したり, 国家の機密を通信で打ち合わせたりするのが主要な用途であったが, インターネットの発達した現代においては人々の生活に密着したものとなっている. 実際, 日常生活で用いられる通信のセキュリティーを守るために暗号はなくはならないものである. 電子マネー, 電子署名, 電子投票などでも暗号は用いられている.

現代ではコンピュータが発達しているので, 単純な暗号は直ちに解読されてしまう. そのため, 様々な解読の難しい暗号が考案されている. 1977 年, アメリカ商務省標準局は, 暗号化のアルゴリズムは公開するが暗号化のための鍵は公開しないタイプの暗号方式を商業用として採用した. この **DES** (data encryption standard) と呼ばれる暗号方式は実際に用いられたが, コンピュータの発達によってこれも安全性の保証がなくなったため, **AES**(advanced encryption standard) の公募がなされ, 2002 年にはベルギーの研究者が提案した**ラインドール** (Rijndael) が商業用の次期暗号システムとして採用されるに至っている.

以上の暗号は, 暗号化の鍵と解読するための鍵を, 発信者と受信者が共有して用いる方式である. この方式の暗号を**共通鍵暗号**という. これに対し, ディフィー (W. Diffie) とヘルマン (M. Hellman) は, 1976 年, 暗号化の鍵を公開しても, 多数の人の中で不特定の 2 人が暗号通信を行うことが可能であるということを見出した. これが**公開鍵暗号**と呼ばれる暗号方式である. たとえ強力なコンピューターを用いても計算を完了するためには途方もない時間がかかり, 事実上解読できないというのがその原理である. 公開鍵暗号方式の構成には, 次のいずれかに基づくものが代表的である.

(i) 素因数分解問題の難しさに基づくもの

(ii) 離散対数問題の難しさに基づくもの

この講義では (i) について解説する. まず、公開鍵暗号の解説をするための数学的準備を行う. p, q を相異なる 2 つの素数とし, $\mathbf{Z}/pq\mathbf{Z}$ を考える.

$$(\mathbf{Z}/pq\mathbf{Z})^* = \{\bar{a} \mid a \in \mathbf{Z},\ a \text{ は } pq \text{ と互いに素 } \}$$

この集合は

$$ab \equiv 1 \pmod{pq} \text{ となる整数 } b \text{ が存在する}$$

ような a が属する剰余類の集合と言い換えてもよい. すなわち, $\mathbf{Z}/pq\mathbf{Z}$ の元のうち, 乗法に関する逆元を有するもの全体の集合である.

$$ab \equiv 1 \pmod{pq},\ a'b' \equiv 1 \pmod{pq}$$

ならば,

$$aa'bb' \equiv 1 \pmod{pq}$$

だから,

$$\bar{a},\ \bar{a'} \in (\mathbf{Z}/pq\mathbf{Z})^* \implies \bar{a}\bar{a'} \in (\mathbf{Z}/pq\mathbf{Z})^*$$

となる. すなわち, $(\mathbf{Z}/pq\mathbf{Z})^*$ は乗法に関して閉じている. $\mathbf{Z}/pq\mathbf{Z}$ は

$$\bar{0},\ \bar{1},\ \bar{2},\ \cdots,\ \overline{pq-2},\ \overline{pq-1}$$

からなり, その元の個数は pq 個である. そのうち, $(\mathbf{Z}/pq\mathbf{Z})^*$ に入る元の個数は $0 \leq a \leq pq-1$ なる整数 a で pq と互いに素なものの数に等しいから

$$(p-1)(q-1)$$

個である. このことから, フェルマーの小定理の一般化として次の結果を得る.

補題 0.1 $a \in (\mathbf{Z}/pq\mathbf{Z})^*$ ならば,

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

が成り立つ.

例 0.2 $p = 41, q = 47$ とし, $n = pq = 1927$ を考える. このとき, $(p-1)(q-1) = 1840$. $a = 192$ をとれば, 192 は 41, 47 で割り切れないから $192 \in (\mathbf{Z}/1927\mathbf{Z})^*$ である. このとき

$$192^{1840} \equiv 1 \pmod{1927}$$

を得る.

それでは, 公開鍵暗号の代表的な例である **RSA 暗号**の紹介をしよう. この暗号は 1978 年にリヴェスト (R. Rivest), シャミア (A. Shamir), アドルマン (L. N. Adleman) によって発表された. RSA 暗号は, ２つの大きな素数の積を素因数分解することが困難であることに基づく公開鍵暗号である. ユーザー B が暗号を送信し, ユーザー A が受信し秘密情報を得るという設定である.

まず最初に，ユーザー A は相異なる大きな素数 $p,\ q$ を選び，$n\ =\ pq$ とおく．$\mathbf{Z}/(p-1)(q-1)\mathbf{Z}$ の元 e で

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

となる元 d が存在するものをランダムに選ぶ．そして，n, e を公開する．

$$\text{公開} : n, e$$

ユーザー A は p, q, d を秘密鍵として，秘匿しておく．

ユーザー B がユーザー A に平文 $M \in (\mathbf{Z}/n\mathbf{Z})^*$ を送信するために，

$$M^e \pmod{n}$$

を計算し暗号化する．n の素因数分解が困難であるため，第三者は d を計算できず，$M^e \pmod{n}$ から M を復元できない．一方，ユーザー A は n の素因数分解 $n = pq$ を知っているため d を計算でき，$(M^e)^d \equiv M \pmod{n}$ によって，平文 M を復元できるのである．

実際に復元できていることをチェックしておこう．補題 0.1 から

$$M^{(p-1)(q-1)} \equiv 1 \pmod{n}.$$

$ed \equiv 1 \pmod{(p-1)(q-1)}$ だから，ある整数 s があって

$$ed = (p-1)(q-1)s + 1$$

となる．したがって，

$$\begin{aligned} M^{ed} \pmod{n} &\equiv M^{(p-1)(q-1)s+1} \pmod{n} \\ &\equiv (M^{(p-1)(q-1)})^s M \pmod{n} \\ &\equiv M \pmod{n} \end{aligned}$$

となる．

例 0.3 例 0.2 と同じく，$p = 41, q = 47$ の場合を考える．$n = pq = 1927$ である．このとき，$(\mathbf{Z}/1927\mathbf{Z})^*$ の元の個数は $(p-1)(q-1) = 1840$．$e = 17$ とすれば，ユークリッドの互除法を用いて，

$$1840 = 108 \times 17 + 4,\ 17 = 4 \times 4 + 1$$

から，

$$4 \times 1840 + 1 = 433 \times 17$$

を得る．よって，$d = 433$ とすれば，

$$ed = 17 \times 433 \equiv 1 \pmod{1840}$$

となる．平文 $M = 192$ をこのシステムで暗号化すれば，

$$M^e = 192^{17} \equiv 873 \pmod{1927}$$

ユーザー B は暗号文 873 をユーザー A に送る．ユーザー A は

$$873^d = 873^{433} \equiv 192 \pmod{1927}$$

によって平文 $M = 192$ を復元する．