高校生のための現代数学講座　　東京大学
「数論と暗号」　　玉原国際セミナーハウス
講義 (2)　桂　利行　　2005 年 8 月 19 日

# 「暗号のいろいろ」

**暗号の種類**

(i) 共通鍵暗号
(ii) 公開鍵暗号

**公開鍵暗号**

公開鍵暗号の提案：W. Diffie, M. Hellman (1976 年)

公開鍵暗号の原理

(i) 素因数分解問題の困難に基づくもの（RSA 暗号）
(ii) 離散対数問題の困難に基づくもの（ElGamal 暗号）

**RSA 暗号**

Rivest, Shamir, Adleman (1977 年)

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 A

(1) $p$, $q$ を大きな素数とし, $n = pq$ とおき, $\mathbf{Z}/(p-1)(q-1)\mathbf{Z}$ の $(p-1)(q-1)$ と互いに素な自然数 $e$ をランダムに選ぶ．

(2) $ed \equiv 1 \bmod (p-1)(q-1)$ となる元 $d$ を計算する．

公開：$n, e$
秘密鍵：$p, q, d$

(3) 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, $M^e \bmod n$ によって暗号化する．

(4) 第三者は $d$ を計算できないため, $M^e \bmod n$ から $M$ を復元できないが,
ユーザー A は
$(M^e)^d \equiv M \bmod n$
によって, 平文 $M$ を復元できるのである．

**ElGamal 暗号**

T. ElGamal (1985 年)

ElGamal 暗号は, $\mathbf{Z}/p\mathbf{Z}$ から 0 を除いた集合 $\mathbf{F}_p^*$ に乗法を考え、その離散対数を用いるものである.

$p$ を大きな素数, $g$ を $\mathbf{F}_p^*$ の原始元とする. すなわち, $g$ を何乗かすれば $\mathbf{F}_p^*$ の任意の元が得られるとする.

ユーザー A

(1) $0 \leq x \leq p-2$ なる整数 $x$ をランダムに選び, 秘密鍵とする.

(2) $g^x \mod p \equiv y$ を計算し, $y$ を公開する.

公開：$p, y$

秘密鍵：$x$

ユーザー B

(3) ユーザー A に平文 $M \in \mathbf{Z}/p\mathbf{Z}$ を送信するために, 乱数 $r$ を選ぶ.

(4) $c_1 = g^r \mod p$ および $c_1 = y^r M \mod p$ によって暗号化し, $(c_1, c_2)$ のペアをユーザー A に送る.

(5) 第三者は $y$ から $x$ を計算できないために暗号を解読できないが,

ユーザー A は,

$M \equiv c_2/c_1^x \mod p$

によって, 平文 $M$ を復元できるのである.

**参考文献**

[1] 太田和夫・國廣昇著, ほんとうに安全? 現代の暗号, 岩波科学ライブラリー 102, 岩波書店, 2005.

[2] 辻井重男著, 暗号, 講談社, 1996.