# 公開鍵暗号とその仕組み～補足資料～

慶應義塾大学理工学部情報工学科 2 年　新行内 浩輔 *

2016 年 5 月 22 日

# RSA 暗号

## 1　RSA 暗号の概要

RSA 暗号とは，Ronald Linn Rivest，Adi Shamir，Leonard Max Adleman の 3 人が発明した公開鍵暗号の一つである．この暗号は，巨大な素数を素因数分解することが困難であることを安全性の根拠としている．

## 2　仕組み

ここでは，平文 P を暗号化して，正しく復号化するまでの仕組みを説明していく．

### 2.1　事前準備

以下に登場する文字についてまとめておこう．

P: 平文 (plane text)

C: 暗号文 (cryptogram)

$p, q$: 300 桁以上の素数 (これらは受信者のみが知っている 秘密鍵)

$m$: $p$ と $q$ の積 (公開鍵)

$e$: 後に説明するが，うまく調整された数 (公開鍵)

$d$: これも後に説明する，秘密の数

*shingyo_do_the_likeliest@yahoo.co.jp

## 2.2　暗号化・復号化のメカニズム

はじめに，受信者側が $[e, m]$ のセットを公開鍵として公開する．これをみた送信者は，平文 P を $e$ 乗する．これが，暗号文 C である．

$$\mathrm{C} \equiv \mathrm{P}^e \pmod{m} \tag{1}$$

暗号文 C を受信した正当な受信者は秘密の数 $d$ を用いて，復号化することができる．

$$\mathrm{P} \equiv \mathrm{C}^d \equiv (\mathrm{P}^e)^d \pmod{m} \tag{2}$$

## 2.3　d の求め方

ここで重要なのが，$d$ である．$d$ は，正当な受信者のみが簡単に求められるが，それ以外の人にとっては求めることができない，という不思議な数である．では，$d$ がどのような数なのかより具体的に探っていこう．

オイラーの定理

$m$ を自然数，$a$ を $m$ と互いに素な整数としたとき，$a^{\phi(m)} \equiv 1 \pmod{m}$
ここで，$\phi(n)$ は，1 から $n$ までの自然数のうち，$m$ と互いに素なものの個数のことである．

オイラーの定理を利用すると，

$$P^{\phi(m)} \equiv P^{\phi(m)v} \equiv 1 \pmod{m} \quad , \quad v \in \mathbb{Z} \tag{3}$$

となるので，

$$P^{\phi(m)v+1} \equiv P \pmod{m} \tag{4}$$

(2) と (4) より，

$$ed = \phi(m)v + 1 \tag{5}$$

この式を満たすような，$d$，$v$ を求めてやればよい．(5) は一次不定方程式である．ここで次の定理を参考にしたい．

一次不定方程式の整数解の存在性

$x$，$y$ に関する二元一次不定方程式 $ax + by = c$ が整数解を持つことと，$c$ が $a, b$ の最大公約数の倍数であることは同値である．
特に，$ax + by = 1$ が整数解を持つことと，$a$ と $b$ が互いに素であることは等しい．

この定理から，$e$ と $\phi(m)$ が互いに素であれば，(5) は整数解 $d$，$v$ を持つことが導

かれる．
ちなみに，$\phi(m)$ は $m = pq$ であるため，次のようにかける．

$$\phi(m) = pq - p - q + 1 = (p-1)(q-1) \tag{6}$$

$p, q$ を知っている人，つまり正当な受信者は簡単に $\phi(m)$ を計算することができる．一方で，不正に暗号文を入手したとしても公開鍵 $e$ と $m$ しか分からず，$p, q$ は求められないため $\phi(m)$ を計算することはできない．これが，冒頭に述べた「RSA 暗号が巨大な素数を素因数分解することが困難であることを安全性の根拠としている」という意味である．

さて，$d$ の存在は示すことができた．だが，実際に求めることはできるのだろうか？また，はたして d は正の整数解を持つのだろうか？

最後に，$d$ が正の整数解を必ず持つということを示すことにする．
整数解の組 $(d_0, v_0)$ が見つかったとする．$(d_0 < 0)$
つまり，

$$ed_0 - \phi(m)v_0 = 1 \tag{7}$$

である．ここで整数 $k$ を用いて，

$$e(d_0 + \phi(m)k) - \phi(m)(v_0 + ek) = 1 \tag{8}$$

も成立する．これより，$(d_0 + \phi(m)k, v_0 + ek)$ も (5) の解の一つであり，$k$ を適当に選ぶことで，$d_0 + \phi(m)k > 0$ とすることができる．これで，$d$ が正の整数解をもつことが示された．

$\phi(m)$ を求め，(5) を導出さえできれば，$d$ を求めることは容易である．おなじみ，ユークリッドの互除法の出番である．この方法についてはここでは割愛する．どうしても知りたいという人は青チャートを紐解いてみることをお勧めする．

# 参考文献


[1] John MacCormick. (長尾高弘訳) 世界でもっとも強力な 9 のアルゴリズム. 日経 BP 社. 2012.

[2] 一松 信. 暗号の数理. 改訂新板. ブルーバックス. 講談社. 2005.

[3] 今井秀樹監修. トコトンやさしい暗号の本. 今日からもの知りシリーズ. B & T ブックス. 日刊工業新聞社. 2010.

[4] 結城 浩. 暗号技術入門 第 3 版: 秘密の国のアリス. SB クリエイティブ. 2015.