現代数学への流れ 第 12 回

名古屋大学多元数理科学研究科 谷本　祥

2023 年 1 月 27 日

暗号

RSA 暗号

公開鍵暗号

インターネット上でクレジットカードで買い物をする時、当然カード情報を暗号化する必要がある。そこでは公開鍵暗号というものが使われている。

公開鍵暗号以前の暗号は暗号化するための鍵と復元するための鍵は同一であった。

そのため暗号化するための鍵を秘密裏に配送する必要があり、インターネット上ではそれは不可能。

公開鍵暗号

公開鍵暗号とは暗号化のための鍵と復元のための鍵を別にし、暗号化のための鍵を公開できるようにした暗号化方式。

元々 1960 年代にイギリスの諜報組織 GCHQ の James Elis が考案したが、その研究内容は国家機密扱いとなり 90 年代まで公開されることはなかった。

先に論文として公表し、世間に広めたのは Whitfield Diffie と Martin Hellman。彼らはこの業績で Turing 賞などを受賞している。

RSA 暗号

RSA 暗号: Ron Rivest, Adi Shamir と Leonard Adleman が MIT にいた時開発した世界最初の公開鍵暗号。

3 人もこの業績により、Turing 賞を受賞。

GCHQ で公開鍵暗号を発案した Elis は同じく GCHQ で働いていた数学者 Clifford Cocks と同じ暗号方式を開発したが、それもまた機密扱いとなり 90 年代まで公表されることがなかった。

剰余環

n を正の整数とする。集合 $\mathbb{Z}_n$ を以下で定める。

$$\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$$

$a, b \in \mathbb{Z}_n$ を任意の元とすると a と b の和を n で割った余りを r とし、$\mathbb{Z}_n$ における和を

$$a + b = r \mod n$$

と定める。

積も同様に定める。例えば $n = 12$ とすると

$$7 + 8 = 3 \mod 12, \quad 4 \cdot 7 = 4 \mod 12$$

などがいえる。

RSA 暗号: 鍵生成

p, q を非常に大きな相異なる素数とする。$n = pq$ と定める。

暗号を受け取りたい人間 Bob は $\phi(n) = (p-1)(q-1)$ とし、$\phi(n)$ と互いに素な正の整数 e を選ぶ。

Bob は Euclid の互除法を用いて

$$de + x\phi(n) = 1$$

となる整数 d, x を計算する。

最後に Bob は e と n を公開する。

RSA 暗号: 暗号文生成

平文 $m \in \mathbb{Z}_n (m$ と n は互いに素とする$)$ を Bob に送りたい Alice は暗号文を以下の要領で生成する。

$$c = m^e \mod n$$

Alice は c を暗号文として Bob に送る。

RSA 暗号: 暗号文復元

復元には以下の Fermat の小定理を使う。n と互いに素な a について以下が言える。

$$a^{\phi(n)} = 1 \mod n$$

これにより Bob は以下を計算できる

$$c^d = m^{de} = m^{de+x\phi(n)} = m \mod n$$

従って平文 m を復元できた。

なぜ安全か？

復元鍵 d を構成するには $\phi(n)$ を知る必要がある。

そのためには n を素因数分解しなければならない。

一般に大きな数の素因数分解は時間がこの上なくかかる。よって、それは現実的には不可能と考えられる。

しかし、本当に素因数分解が困難かという問題は今も未解決な問題として残っている。

演習問題

$p = 7, q = 11$ とし $n = 77$ とする。公開鍵を $e = 7$ としたときの復元鍵 d を求めよ。さらに平文 $m = 25$ を暗号化せよ。さらにその暗号文を復元鍵を用いて復元せよ。