R. L. Rivest, A. Shamir and L. Adleman: A Method for Obtaining Digital Signature and Public-key Cryptosystems

Comm. ACM, Vol.21, No.2, pp,120-126（1978）

今回紹介する Rivest, Shamir, Adleman の論文の序章は，"The era of "electronic mail" may soon be upon us; we must ensure that two important properties of the current "paper mail" system are preserved:（a）messages are private, and（b）messages can be signed." で始まる．2003 年の現在，彼らの予想通り，電子メールによる通信は生活の中に定着し，さらにインターネットによる商品売買，情報収集も日常茶飯事のことになりつつある．ネットワークは我々の生活から取り外すことができなくなった．情報セキュリティは，ネットワーク上を流れるデータの保護を目的とした研究である．その代表的な技術が，今回紹介する論文で提案された RSA 暗号である．情報セキュリティという言葉も，すっかり私たちの生活に定着しつつあるので，RSA 暗号を知っている読者も多いかもしれない．

彼らが論文を書いた 1978 年，この時代の通信手段の主流は手紙であった．1970 年代後半，情報セキュリティに関して現在の幅広い研究につながる画期的な論文が発表された．まず 1976 年の Diffie と Hellman による公開鍵暗号の概念の提案である．公開鍵暗号とは，

1. 暗号化に用いる暗号鍵と復号化に用いる復号鍵が異なる，
2. 暗号鍵から復号鍵を求めるのは困難である，
3. 暗号化と復号化は容易にできる，

という性質を満たす暗号である．2 の性質から，復号鍵のみを秘密に保持し暗号鍵を公開することから，公開鍵暗号と呼ばれる．また公開鍵暗号において，暗号鍵は公開鍵，復号鍵は秘密鍵と呼ばれる．公開鍵暗号の概念は，これまでの暗号の常識を完全に覆すものだった．つまり暗号といえば，同じ鍵を用いて暗号と復号を行うため，秘密通信を行う相手同士があらかじめ何らかの方法で，秘密の鍵を共有する必要があった．さらに異なる通信相手ごとに，異なる秘密の鍵を共有する必要があるのも明らかだろう．一方，公開鍵暗号の概念は，各ユーザが自分用の暗号鍵（公開鍵）と復号鍵（秘密鍵）を生成し，公開鍵を電話帳などで公開することでどんな相手とも秘密通信を可能にする．まさに今日の普及したインターネットでの秘密通信に不可欠な技術といえよう．ところが残念なことに，彼らは公開鍵暗号が，"trap-door one-way function"（トラップドア付一方向性関数）により可能になる（トラップドア付一方向性関数を暗号化に利用し，トラップドアを復号鍵として与えるとよい）ということを明らかにしたが，具体的なトラップドア付一方向性関数を与えることはできなかった．

具体的なトラップドア付一方向性関数は，Rivest, Shamir, Adleman によって初めて与えられた．このトラップドア付一方向性関数は，2 つの素数 p, q の積である合成数 n と $(p-1)(q-1)$ と互いに素である正整数 e を用いて，

$$f(m) = m^e \pmod{n}$$

と定義される．つまり e と合成数 n が公開鍵で，メッセージ m の暗号文が $f(m)$ になる．ここで $m^e \pmod{n}$ は m^e を n で割った剰余を意味する．このシンプルな関数の効率的な逆関数の求め方は 25 年たった現在でも明らかになっていない．ところが，$ed = 1 \pmod{(p-1)(q-1)}$ となる整数 d をトラップドアに持つユーザは，

$$f^{-1}(f(m)) = f(m)^d = m^{ed} \pmod{n}$$

と簡単に復号ができる．トラップドアの d だが，n が素因数分解できると，$(p-1)(q-1) = l$ を求め，e と l から求められる．素因数分解は，古くから数論で知られる問題であるが，その問題がこのようなシンプルなテクニックで公開鍵暗号の実現を可能にした．

現在利用される RSA 暗号は，暗号化の前にメッセージに冗長部を付加するなどの変更がされているが，25 年を経ても安全性が素因数分解の困難性に基づくことは変わらない．彼らの論文の素晴らしさは，公開鍵暗号を実現する具体的な方法を与えただけでなく，これまで科学とはある意味無縁と思われていた数論の分野と情報セキュリティの分野の架け橋を与えたことにもあるといえる．

（平成 15 年 3 月 19 日受付）

宮地充子／北陸先端科学技術大学院大学情報科学研究科
miyaji@cs.ucdavis.edu