暗号が暮らしを変える

―― 黒澤研究室～集積システムコース ――

黒澤　馨　教授

LANDFALL31号では、坂庭研究室の取材で通信に関する様々なお話を伺った。取材の最後に、通信に関連する話題として、情報セキュリティの問題があることを教えて頂いた。

コンピュータが普及し、さらに最近ではインターネットも普及しつつある。このような情報化社会において、情報セキュリティの重要性は増す一方である。また、電子マネーの実用化にも情報セキュリティ技術の向上は欠かせない。

そこで今回は、現代暗号の研究をされている黒澤研究室を訪問し、公開鍵暗号を中心とした最近の暗号のお話を伺った。

暗号の必要性とその種類

最近のコンピュータ通信の普及はめざましく、皆さんの中にも、電子メールを日常的にやり取りしている人が多くいるのではなかろうか。また、昨今のインターネットの普及には目を見張るものがある。これからの社会は確実に高度情報化社会への道を歩み、ますますコンピュータを使った通信が身近なものになることだろう。そうなれば、世界中の人々と自由にかつ簡単に情報のやり取りができるようになる。また、世界中のコンピュータにアクセスできるようになる。しかしそれは、言い換えれば世界中の誰とも分からない人と情報交換をし、また、世界中から自分のコンピュータにアクセスされ得るということである。

電子情報というのは、複製や編集がしやすく便利である。だがそれは一方で、悪意を持った書き換えやコピーも簡単にできてしまうことを意味する。それを防ぎ、お互いに信頼できる通信を行なうための方法が暗号技術である。

暗号は、それを解く鍵の種類によって、大きく２種類に分けることができる。それが秘密鍵暗号と公開鍵暗号である。秘密鍵暗号というのは古代ローマ帝国の時代にも使われていた従来型の暗号である。一方、公開鍵暗号というのは、1970年代に生まれた全く新しい方式の暗号である。後でRSA暗号という公開鍵暗号の仕組みを紹介するが、その前に秘密鍵暗号と公開鍵暗号について説明しておこう。

1. 暗号化

ただし、スペースは無視する。

平文 ： IT IS IN THE BOX

⇓ ３つ先の文字に置き換える

暗号文： LWLVLQWKHERA

2. 復号化

暗号文： LWLVLQWKHERA

⇓ ３つ前の文字に置き換える

平文 ： IT IS IN THE BOX

図１　シフト暗号

まず、秘密鍵暗号の例として、シフト暗号を挙げる（図１）。これはシーザー（カエサル）が使ったことからシーザー暗号ともいわれるもので、送りたい文字を何文字分かずらした文字を暗号文として送る。図の例では３文字分ずらしている。

この秘密鍵暗号では、何文字分ずらしたかという数字が重要であり、その数字を鍵という。この鍵は、情報の送り手と受け手が予め知っていて、他の人には秘密にしておかなければならない。これが、秘密鍵暗号と呼ばれる所以である。

これをモデルに示すと、図２(a) のようになる。まず用語を説明しておこう。送りたい文を平文と呼ぶ。その平文に暗号化という操作をほどこして実際に送信する文を暗号文と言う。その暗号文が通る道、つまり、電話回線や電波等のことを通信路という。敵は通信路から暗号文を盗聴し、その暗号文を解読して平文を得ようとするわけである。この秘密鍵暗号で重要なことは、暗号化する時と復号化する時とでは、使う鍵が同じだということである。

一方、公開鍵暗号というのはどのようなものなのだろうか。秘密鍵暗号と同様にモデルに示すと、図２(b)のようになる。ここで、平文を暗号文にするための鍵を暗号鍵と言い、逆に暗号文を平文にするための鍵を復号鍵と言う。公開鍵暗号は秘密鍵暗号と違い、その暗号鍵と復号鍵が別なものとなっている。

暗号鍵と復号鍵が違うなどという不思議な暗号をどのように作るか、ということは後回しにするとして、秘密鍵暗号と公開鍵暗号の違いについて考えてみよう。

まず秘密鍵暗号は、情報の送り手と受け手が予め鍵を知っていなければならない。盗聴者に鍵が知られてしまってはこれから送る全ての暗号文が解読されてしまうので、鍵は絶対安全な通信路を使って送信しなければならない。

しかし、「絶対安全な通信路」などというものは存在しない。どんな通信路であれ、盗聴される可能性が全くないとは言い切れない。そもそも、「絶対安全な通信路」などというものがあるのなら、暗号を使う必要性は全くないのだ。結局、鍵を送るには、実際に会ってどこかで手渡しするなどしかないということになる。

それに対して、送り手と受け手で予め鍵を共有しておく必要のない暗号が公開鍵暗号である。受け手は暗号鍵を公開してしまい、復号鍵は自分で誰にもばれないように管理する。つまり、誰でも鍵をかけること（暗号化）はできるが、鍵を開けること（復号化）ができるのは自分のみである。例えるなら、南京錠の錠のみを配布し、それを開けるための鍵は盗まれないように自分で保管しておくようなものだ。自分へ情報を送ってもらう時には公開しておいた暗号鍵を使って暗号化してもらう。もし暗号文が盗聴されたとしても、復号鍵は自分しか持っていないから、復号化されることはない。暗号鍵を電話帳に載せるなどして一般に公開すれば、誰からでも自分へ情報を安全に伝えてもらうことができる。また、全く知らない人へ情報を送りたい時にも、公開されているその人の暗号鍵を調べ、それを使って暗号化することにより、安全に情報を送ることができるわけである。

この公開鍵暗号では暗号鍵を公開するため、暗号鍵から復号鍵が推測できないようにしなければならない。後で説明するように、暗号鍵は復号鍵から計算によって作られる。それならば、逆に復号鍵も暗号鍵から計算によって得られそうなもの

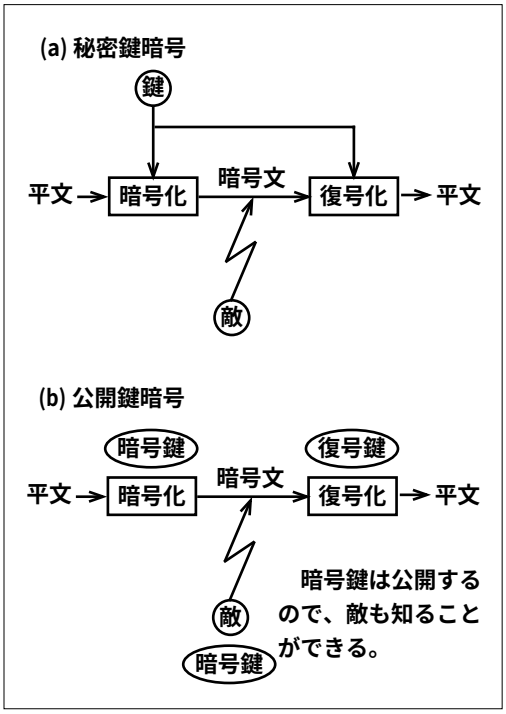

図２　暗号のモデル

だが、その計算には何万、何億年という時間を要するため、現実的には不可能なのである。

このような復号鍵と暗号鍵は、どのようにして作られるのだろうか。具体的な例として、次にRSA暗号の仕組みを紹介しよう。

RSA暗号と黒澤暗号

RSA暗号というのは公開鍵暗号の一種で、３人の開発者Rivest、Shamir、Adlemanの頭文字からそう呼ばれている。現在最も普及している公開鍵暗号である。

この公開鍵暗号では、暗号化は簡単にできるが復号化はできないという不思議なことを、整数の素因数分解を使って実現している。

その仕組みを説明する前に、１つ定理を紹介する。それがフェルマーの定理である（図３）。これはフェルマーの小定理とも呼ばれ、有名なフェルマーの大予想とは違うものである。

そして、RSA暗号の仕組みを図４にまとめる。まず、情報の受け手が２つの大きな素数p、qを適当に決め、それらから公開鍵Rとeを計算によって求める。次に求まったRとeを一般に公開する。また、Rとeから復号鍵dを決め、それを誰にも知られないように保管しておく。Rとeを計算するのは意外と簡単で、パソコンで数分もかからずにできてしまう。復号鍵dもp、qを知っていれば簡単な計算により決められる。

情報の送り手は、公開された暗号鍵Rとeを用いて計算し、暗号文を作成する。なお、ここで平文Mは、文字を整数に変換したものとする。そしてできた暗号文Eを送信する。

それを受信した情報の受け手は、先に保管しておいた復号鍵dを用いて計算し、平文M'を得る。このM'が、情報の送り手が送りたかった平文Mになっているのである。

任意の素数pと、任意の整数a（$1 \leqq a < p$）に対して、

$$a^{p-1} = 1 \bmod p$$

が成り立つ（mod xは、xで割った余りをとるという意味）。

例えば、mod 5 において、

$$2^4 = 16 = 1 \bmod 5$$

$$3^4 = 81 = 1 \bmod 5$$

$$4^4 = (16)^2 = 1 \bmod 5$$

図３　フェルマーの定理

1.準備（情報の受け手）

２つの素数p、qを用意し、R＝p×qと互いに素な数eを適当に選ぶ。

そして、Rとeを公開する。復号鍵dを、

$$ed = x(p-1)(q-1)+1 \quad (x：整数)$$

となるように決め、自分で保管しておく。

2.暗号化（情報の送り手）

平文Mを送りたいとする。公開された暗号鍵Rとeを使って、暗号文

$$E = M^e \bmod R$$

を計算し、送信する。

3.復号化（情報の受け手）

受信した文Eから、保管しておいた復号鍵dを用いて、

$$M' = E^d \bmod R$$

として得たM'が、Mに等しい.

4.M'がMに等しいことの証明

フェルマーの定理より

$$M^{p-1} \bmod p = 1$$

であることを使うと、

$$M' = E^d \bmod R$$
$$= M^{ed} \bmod R$$
$$= M^{1+x(p-1)(q-1)} \bmod p$$
$$= M \cdot M^{x(p-1)(q-1)} \bmod p$$
$$= M \cdot (M^{p-1} \bmod p)^{x(q-1)} \bmod p$$
$$= M \cdot (1)^{x(q-1)} \bmod p$$
$$= M \bmod p$$

同様に$M' = M \bmod q$**も言えるから、**

$$M' = M \bmod R$$

図４　RSA暗号の仕組み

このRSA暗号によって暗号化された暗号文を盗聴し、それを解読しようとすると、Rがp×qに素因数分解できれば解読できてしまうことは分かるだろう。しかし、素因数分解というのは計算機科学が発達した今でも難しく、非常に時間がかかる。例えばpとqにそれぞれ200桁の素数を選んだとしよう。そのp、qからR（＝p×q）を計算するには、パソコンでほんの0.01秒もかからない。しかし求まったRを素因数分解して元のpとqを求めるには、500億年以上かかってしまう。世界中のコンピュータを使って計算しても非現実的な時間がかかり、事実上不可能だ。

これで、暗号化はできるけれど復号化はできない、という公開鍵暗号が実現されたわけである。

しかし、このRSA暗号には大きな問題がある。それは、素因数分解ができれば解けるということは分かっているが、素因数分解ができなければ解けないということは証明されていないことである。

つまり、素因数分解以外にもRSA暗号を解読する方法があるかもしれないのだ。今のところ、そのような素因数分解以外の解読法は見つかっていないが、明日にでも素因数分解以外の解読法が発見されないとも限らないので、重要な情報を伝える場合には心配である。

それを解決したのはラビン暗号である。少々複雑になるので、ここではその仕組みを説明することができないが、この暗号は素因数分解以外の方法では解読できないことが証明されている。

しかし、ラビン暗号ではその仕組み上、復号化の時に４通りの平文候補が出てきてしまう。ただ１通りの平文ができることを、一意に復号化できると言うが、一意に復号化できないということは、暗号としては失格である。４通りの平文候補を求めるのだから、復号化にも余計な時間がかかることになる。

これをも解決したのが、黒澤先生が考案された黒澤暗号である。計算途中で逆数を使うことから、逆数暗号とも呼ばれる。この暗号では、暗号文の他に２ビット（１ビットは２進数の１桁）付け加えたものを送信する。その２ビットにより、きちんと１通りの平文が得られる。もちろん素因数分解以外に解読の方法がないことも、きちんと証明されている。

すなわち、黒澤暗号は、解読の不可能性が証明され、かつ復号の一意性も保証された、貴重な国産の公開鍵暗号なのである。

暗号の利用と今後

これまで、公開鍵暗号で文書を暗号化する仕組みを見て頂いたが、この公開鍵暗号には他にも用途がある。それが電子署名、すなわち電子的な印鑑である。

例えば、パソコン通信でビジネスのデータをやり取りする場合、取引先から発注書が届いても、その情報が本当にその取引先からのものかどうかを確認しなければならない。そのために必要なのがこの電子署名なのである。

では、どのようして公開鍵暗号を電子署名に応用できるのだろうか。その手順を簡単に説明しよう（図５）。

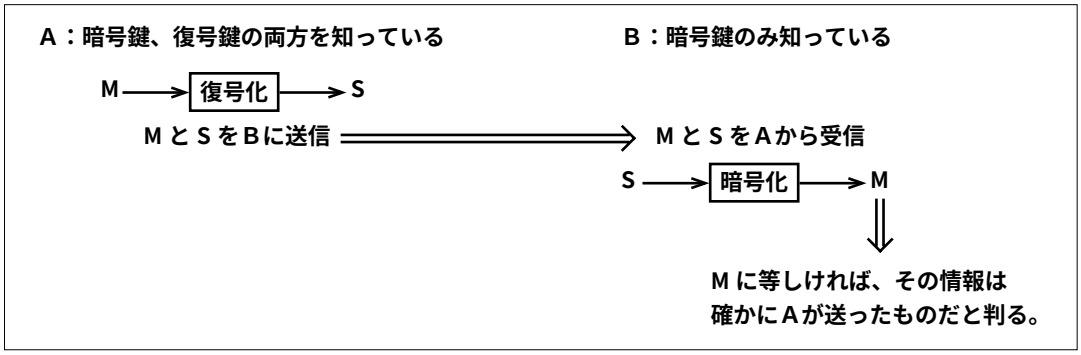

図５　電子署名

公開鍵暗号を電子署名に利用する場合は、これまでと逆に、先に復号化をしてしまう。送信者をA、受信者をBとしよう。送信者Aは、暗号鍵、復号鍵の両方を知っている。Aは暗号鍵のみ公開するから、受信者Bは暗号鍵を知っているが、復号鍵は知らない。

Aは送信したい平文Mを復号鍵で復号化する。そうしてできた文をSとする。そして、MとSを送信する。それを受信したBは暗号鍵を知っているので、Sを暗号化してみてMと比べる。そしてSを暗号化したものとMが等しいことが判れば、その文書は確かにAから送られたということになる。なぜなら、MからSを作ることができるのは、復号鍵を知っているAのみだからである。ここで、暗号文でなく、平文Mを復号化する、ということを疑問に思った方もいるだろう。これは、暗号化と復号化が逆の操作であると考えれば解って頂けるのではなかろうか。すなわち、暗号化したものを復号化すると元に戻るということは、復号化したものを暗号化すれば元に戻るということでもある。また、暗号鍵を公開するので暗号化は誰にでもできるが、一方の復号鍵は送信者しか知らないので、復号化はその送信者にしかできない。これによって、匿名性が高いインターネット上でも署名ができるのである。

このように、非常に便利な公開鍵暗号だが、欠点もある。それは、秘密鍵暗号に比較すると計算が大変だということだ。そのため、時と場合により秘密鍵、公開鍵暗号を使い分けなければならない。例えば秘密鍵暗号は、会社内のネットワーク等の、ローカルな通信には向いているだろう。一方、インターネット等、不特定多数の人とのグローバルな情報通信においては、予め鍵を共有しておく必要のない公開鍵暗号の方が有利である。特に公開鍵暗号は、我々の生活にも大きく影響してくる。

例えば先の電子署名が可能になれば、パソコン通信を使った買い物が安全にできるようになる。また、最近言われている電子マネーにも、電子署名が必要だ。現在考えられている方式の主流はICカードを使ったもので、例えば銀行からお金を引き出す場合は銀行からICカードにお金のデータを移動させる。この時に、確かに受け取ったという署名が必要である。またクレジットカードと同様に、買い物をした時にも署名が必要である。電子署名によってこれらが可能になると、紙幣を持つ必要がなくなり、おつりも不要になる。家に持ち帰り、ICカードとパソコンを組み合わせれば、家計簿など入出金の管理の手間が大幅に省かれる。

また、契約者のみ見られる有料テレビをペイテレビと言うが、これにも暗号技術が関わっている。ペイテレビは、テレビ番組を暗号化して放送しする。契約者には、復号鍵の組み込まれた復号機を配布し、それにより暗号化されたテレビ番組を復号するという仕組みになっている。しかし、もしその復号機が勝手に複製されてしまうと、テレビ局は経営が成り立たなくなる。最近黒澤先生は、このペイテレビの復号機の海賊版を防ぐ最適な方式を考案され、Eurocrypt'98という、この分野で最もレベルの高い国際会議の１つに採択されたそうである。これが実用化されれば、ペイテレビという新しい放送形態が普及する大きなきっかけになるだろう。

さらに、暗号によりパソコン通信を使った選挙が可能になれば、低迷している投票率も上がるかもしれない。

暗号は、我々の日々の暮らしを大きく変える可能性を持っているのである。

RSA暗号よりも黒澤暗号の方が、素因数分解ができなければ解読できないことが証明されているし、しかもラビン暗号と違って一意に復号化できるという点で優れていると言える。一方、エルガマール暗号と呼ばれる暗号など、素因数分解以外の、離散対数問題などに基づく公開鍵暗号も存在する。

これからの暗号がどうなっていくのかは分からない。しかし、その重要性がどんどん増していくことは確かだろう。見ず知らずの人とも安心して情報交換ができる、そんな時代が来るのもそう遠くはないのかもしれない。

最後になったが、大変面白く、かつ分かりやすい話をして下さった黒澤先生に感謝すると共に、黒澤研究室のますますの発展をお祈りしたい。

(奥田　敦)