In Laboratory Now

研究室訪問 5

情報セキュリティと現代暗号

——辻井研究室～電気・電子工学科——

辻井重男教授

「情報通信システム講座」というのが辻井研究室の講座名である。しかし，一口に「情報通信」といっても非常に範囲が広く，１つの研究室でそのすべてをカバーするということはできない。辻井研究室ではこれまで，その広い範囲の中から，光伝送，情報理論，デジタル通信などを手がけてこられたが，現在教授が最も力を入れてやっておられるのが，「適応信号処理」とこれから紹介する「情報セキュリティと現代暗号」というテーマである。

公開鍵暗号の誕生

情報のネットワーク化が進んできている現在では，様々な情報が，回線や通信衛星などを通して，日常的にやりとりされている。これらの情報の中には，他人に知られたくないものも多く含まれているだろう。このような情報を他人に分からないようにするための手段として暗号化をするということが考えられる。つまり，情報のセキュリティを保つための一手段として，暗号というものが必要になってくるという事である。

公開鍵暗号というのは，このような状況のもとで生まれたものであるが，この話にはいる前に，セキュリティという観点から見た暗号の歴史について，簡単に触れておこう。

公開鍵暗号が生まれる前の暗号は大きく二種類に分けられる。１つは換字式暗号と呼ばれるものである。図１(a)を見て欲しい。これは換字式暗号の最も簡単な例である。ＤＰＮＦ……という暗号文に，それぞれの文字をアルファベットの順番において１文字ずつ前へずらす，という操作を施すと，Come at once. と読むことができる。このとき１文字ずらすのなら，１というのが，この暗号を解く「鍵」となる。

この方法だと鍵をいくつに設定しても，文字には文章中に現われる頻度というものがあるので，暗号が簡単に解かれてしまう。そこで暗号化の方法をもっと複雑にする必要がある。複雑化した一例を図１(b)に挙げておくので見ておいて欲しい。また実際に使われたものの中には周期が何億という乱数を足し込んだものもあるが，これも結局は解かれてしまった。

もう一種類の暗号は置換式暗号と呼ばれるものである。この暗号を作るために，まず適当な太さの円筒と細長い紙を用意する。そして，細長い紙を円筒に巻きつけ，筒と平行に平文（暗号にする文）を書くと，元に戻された細長い紙には文字の順序の入れ替わった暗号文ができ上がる。

暗号を受けとった側は，同じ太さの円筒に暗号文を巻きつければ元の文を読むことができる。しかし，ある一定の間隔をおいて文字を読んでいけばよいのだから，この種の暗号が容易に解かれてしまうということは，想像に難くないであろう。

これまで説明してきたのは慣用鍵暗号と呼ばれるものである。慣用鍵暗号は暗号の送信者と受信者が鍵を

図 1

(a)

D P N F B U P O D F

⇊

C O M E A T O N C E

（1文字ずらす）

(b)

E P P G B W Q O F G

| | | | | | | | | |

ⓐ ⓑ ⓒ ⓐ ⓑ ⓒ ⓐ ⓑ ⓒ ⓐ

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

C O M E A T O N C E

ⓐ：2文字ずらす
ⓑ：1文字ずらす
ⓒ：3文字ずらす

共有する方式であり，暗号化の単純な逆操作によって復号化することができる。この種の暗号では，どのような鍵を使って暗号化したかが，何らかの手段でわかれば，簡単に暗号を解くことができてしまう。

これに対し，これから説明する公開鍵暗号というのは，慣用鍵暗号の考え方を根本的にくつがえしたもので，鍵も，暗号化や復号化のアルゴリズムも公開した上で暗号を作ろうというものである。公開するといっても，すべてを公開するのでは暗号にならないので，暗号化の鍵と復号化の鍵を別々に用意をして，暗号化の鍵だけを公開するのである。

このようなことが本当に可能であるのかと疑問に思う人をいるかもしれない。しかし，後で詳しく説明するが，数学的な一方向性関数を用いることにより，暗号化した本人さえも復号化できないような暗号を作ることができる。これはホテルの部屋で内側から外側へは誰でもでられるが，外側から内側へは鍵を持っていないと入れないということに似ている。

「僕の研究室でこういう暗号をやり出したのは，公開鍵暗号の方が数学的に面白いからで，もし慣用鍵だったら……。」

と教授は語っておられたが，公開鍵暗号というのは，発想的にも，理論的にも，いろいろと興味深い点を含んでいる暗号である。

公開鍵暗号の具体例～ＲＳＡ暗号～

では，ここで公開鍵暗号の代表的な例であるＲＳＡ暗号を用いて，具体的な公開鍵暗号の例を見ていくことにしよう。

A，B，C……からなるグループでBからAにa_{BA}という文を暗号化して送る場合を考える。ここでa_{BA}はある定められた規則によって数字列に変換され，何文字かごとに区切られてブロック化されているものとする。

Bは公開されているAの暗号化鍵e_A，n_Aを用いて次のように暗号化をする。

$$b_{BA} = a_{BA}^{\ e_A} \pmod{n_A}$$

(mod n_Aというのは$a_{BA}^{\ e_A}$をn_Aで割った余りをとるという意味)

このとき，Aの暗号化の鍵であるe_Aとn_Aは，十分大きな素数p_A，q_Aから次のように作られている。

$$\begin{cases} e_A : (p_A-1)(q_A-1) \text{と互いに素な整数} \\ n_A : p_A \cdot q_A \end{cases}$$

p_A，q_Aは復号化のとき重要な働きをするのでAが秘密に保管しておく。

n_Aが公開されているのでp_A，q_Aは他人に分かってしまうのではないかという心配があるが，そのような心配はいらない。実は先程のホテルのドアの例と同じでp_Aとq_Aがある程度大きいとp_Aとq_Aからn_Aは簡単に計算できるが，n_Aを素因数分解してp_A，q_Aを求めることは，ほとんど不可能に近い。前に「十分大きな素数」と書いたのはそのためである。

暗号文b_{BA}を受けとったAは次のように復号化する。

まずp_A，q_Aから次の式を満たすd_Aを求める。

$$e_A d_A = 1 \pmod{(p_A-1)(q_A-1)}$$

紙面の都合上d_Aの求め方は省略するが，次にこのd_Aを用いて，b_{BA}をd_A乗することにより，

$$\begin{aligned} & b_{BA}^{\ d_A} \pmod{n_A} \\ &= (a_{BA}^{\ e_A})^{d_A} \pmod{n_A} \\ &= a_{BA}^{\ e_A d_A} \pmod{n_A} \\ &= a_{BA} \pmod{n_A} \end{aligned}$$

となる。このようにして，AはBからの暗号文を読むことができる。

今まで説明したところの具体的な例を図2に示してあるので見ておいてほしい。

図 2

公開鍵：n＝55　e＝7

秘密鍵：p＝5　q＝11　(p－1)(q－1)＝40

　　d＝23　(7×23(mod 40)＝1)

平　文：a＝3

暗号化：$b = a^e \pmod{n} = 3^7 \pmod{55} = 42$（暗号文）

復号化：$a = b^d \pmod{n} = 42^{23} \pmod{55} = 3$

（実際に使われるp，qは10^{100}程度）

送信者の認証をいかにして行なうか～ディジタル署名～

暗号を作るとき，他人に解読されないように作るというのは大変重要であるが，他に，誰が送ったかを，きちんと識別できるように作るというのもまた非常に重要である。もしこのことができないと，CがBになりすましてAに偽の暗号文を送るということが簡単にできてしまう。暗号化鍵が公開されている公開鍵暗号ではなおさらである。

先程出てきたＲＳＡ暗号では，次に示すように，送信者の識別がきち

んとできるようになっている。(以下の手法をディジタル署名という。)

BからAにBの署名文を送る場合を考えてみる。

Bの署名文をb_Bとすると，Bはまず自分の秘密鍵 $\{d_B\}$ で，

$$a_B = b_B^{\ d_B} \pmod{n_B}$$

を計算し，次にAの公開鍵 $\{e_A, n_A\}$ を用いて，

$$m_B = a_B^{\ e_A} \pmod{n_A}$$

を求める。

Bがm_Bを送ると，これを受けとったAは，まず自分の秘密鍵で，

$$m_B^{\ d_A} \pmod{n_A}$$
$$= (a_B^{\ e_A})^{d_A} \pmod{n_A} = a_B$$

を知り，さらにBの公開鍵を用い，

$$a_B^{\ e_B} \pmod{n_B}$$
$$= (b_B^{\ d_B})^{e_B} \pmod{n_B}$$
$$(b_B^{\ e_B})^{d_B} \pmod{n_B} = b_B$$

というようにすればAはBの署名文b_Bを読むことができる。そして，a_BはBにしか計算することができないので，AはBが送信者であることを確認できるのである。

相手のIDを使って暗号を作る～TID暗号～

RSA暗号は数学的に巧妙な手法を用いたすぐれた暗号であるが，この暗号にも欠点がある。それはRSA暗号を初めとする普通の公開鍵暗号は，多数の相手端末の暗号化鍵を記憶していなければならないという点である。

そこで，辻井教授は，次のようなID暗号を世界で初めて提案し，TID暗号と名付けている。(Tは辻井教授，Iは協力者の伊東助手のイニシャル，そしてTITとIDを連想させるよう命名したそうである。)これは公開鍵の代わりに，グループ内のメンバーそれぞれのIDを使って暗号を作ろうというものである。

以下の説明は図3を参照しながら読んでほしい。まずIDをn桁の二進数で表す。次にセンターを用意して，ここにa_1，a_2……a_n を極秘に保管しておく。

もし，AがBに暗号を送りたいときは，計算機の端末かなにかにBのIDを打ち込むと，センターはBの公開鍵y_Bを計算して返してくる。(cf 図3の①)

次にAは送りたいメッセージ m_A と勝手に決めたランダムな数k_Aを用いてg^{k_A}と$m_A y_B^{\ k_A}$を計算する。

Aのこのような暗号文を受けとったBは，自分の秘密鍵s_Bを用いて，g^{k_A}をs_B乗する。すると

$$(g^{k_A})^{s_B} = (g^{s_B})^{k_A} = y_B^{\ k_A}$$

となり，k_Aの値にかかわらず$m_A y_B^{\ k_A}$を$y_B^{\ k_A}$で割ることによってm_Aを求めることができる。

この暗号にも欠点がないわけではない。センターの信用が問題となるし，何割かのメンバーが結託するならば，線形連立方程式を解くことによりa1，a2……anが分かってしまう可能性が生じる。暗号を作成する側としては，常に最悪の場合を考慮しなければならないので，このことは今後の重要な課題となっている。

図 3　TID暗号における公開鍵の作りかた

Bの IDが　0 I 0 I I　とすると，

Bの秘密鍵s_Bは　↓ ↓ ↓ ↓ ↓

s_B = a_2 + a_4+a_5　となる。

$y_i = g^{a_i} \pmod{p}$ とすると ⇐ (一方向性関数)

Bの公開鍵y_Bは

$y_B = y_2 \cdot y_4 \cdot y_5$

という様に作られる。—①

このとき

$$y_B = g^{a_2} \cdot g^{a_4} \cdot g^{a_5}$$
$$= g^{(a_2+a_4+a_5)}$$
$$= g^{s_B}$$

「最近，学生さんに研究室で，日常生活からの発想，遊びからの発想が，非常に大事だということをよく言っているんですけどね。」と取材中に教授はおっしゃった。公開鍵暗号の様な新しい発想はやはり普段とは違った視点からみることによって生まれてきたのであろう。我々は一つの発想にこだわるあまりに思考が行き詰まってしまいがちであるが，そのようなときこそ，日常生活や遊びからの発想が要求されるのではないだろうか。

この取材をするにあたって，辻井教授のほか，留学生の趙さんなどいろいろな方に御世話になった。そのような方々に御礼をいって，この文章を終わりにしたい。

(中野)