4F-04　公開鍵暗号の崩壊アルゴリズム

足立宗三郎
Fuji Artics Co.Ltd.

1. RSA公開鍵暗号の式と記号

RSA公開鍵暗号論の式や記号は、文献によって異なる。一松信著「暗号の数理」では、

$a^r \equiv b(\mathrm{mod}\,n)$
$b^s \equiv a(\mathrm{mod}\,n)$
$r \cdot s \equiv 1\{\mathrm{mod}(p-1)(q-1)\}$

吉田武著「素数夜曲」では、

$x^r \equiv y(\mathrm{mod}\,n)$
$y^s \equiv x(\mathrm{mod}\,n)$
$r \cdot s \equiv 1\{\mathrm{mod}(p-1)(q-1)\}$とある。ほか加藤正隆著「基礎暗号学」では、$T^s \equiv C(\mathrm{mod}\,r)$、$C^t \equiv T(\mathrm{mod}\,r)$、海外文献では、$w^e \equiv c(\mathrm{mod}\,n)$、$c^d \equiv w(\mathrm{mod}\,n)$などの記号もある。

ここでは、メッセージをAとし、暗号メッセージB、暗号鍵r、復号鍵s、法＝modN、式は、$A^r \equiv B(\mathrm{mod}N)$、$B^s \equiv A(\mathrm{mod}N)$と記す。法 Nは、pとqという素数の積であり、rはプライベート(秘密)暗号鍵といい、sはパブリック(公開)復号鍵という。

$A^r \equiv B(\mathrm{mod}N)$、$B^s \equiv A(\mathrm{mod}N)$。

BはA^rだから、$B^s \equiv A^{r \cdot s} \equiv A(\mathrm{mod}N)$でもある。

rとsの関係は、$r \cdot s \equiv 1\{\mathrm{mod}(p-1)(q-1)\}$と、Nを構成する素数p、q(N=p·q)で表わされる。

2. RSAの論理

暗号者は対象メッセージのバイナリコードの数値をAとし、それをr乗し、(法)Nを適用し、残りを暗号メッセージBにして送信。受信者は、その暗号メッセージBをs乗し、(法)Nを適用した残りが最初の数値Aになる。

その暗号用の乗数rは、プライベート暗号鍵であって、暗号者以外の他人は持たない。だから暗号者は固有の暗号が可能であり、暗号鍵rを持たない相手は、暗号文Bは作れない。

発信者である暗号者個有の暗号メッセージBは、復号鍵sを共有する受信者なら復号化ができ、Bをs乗し(modN)＝Aになって、そのAは、発信者の署名であったり、共通鍵暗号方式の鍵であったり、発信者の長文からハッシュ関数で抜き取った短文とし、発信者の改竄されていないメッセージであることがわかる仕組みであったりする。その署名を知ってもらうために、乗数sはパブリック復号鍵として、法Nもパブリックキーとして、渡す相手は不特定多数でもよく、多くの人が共有する。だから公開鍵暗号方式と言う。

3. 公開鍵の弱点

パブリックキーである法Nと、復号鍵sを入手したインターネットの受信者は、Bのs乗≡A(modN)の公式から、みずから任意の数値をBとし、入手したs鍵で、Aの数値にもでき、送信すべきAを自己が解析することも可能であり、インターネットが一般に広がると、そのような受信者の存在は当然考慮する必要がある。

ある挑戦者は、みずからBをs乗して、Aを算出し、そのAをBにするrを算出することができるならば、暗号者つまり署名者だけが持つ署名に必要なrが、他人に知られることであり、他人である挑戦者は、暗号者になりすまして署名ができ、このデジタル署名の公開鍵暗号論理は崩壊する。

The destruct algorithm of public key cryptography
Sosaburo Adachi
Fuji Artics Co.Ltd.
377-13 Dairakuzi Hachiouzi Tokyo
E-Mail:solo.adachi@nifty.ne.jp

---

4. 公開鍵暗号の崩壊

それは任意のメッセージの数値Bを故意に$N-2^{\alpha}$とすることであり、これにパスカルの二項展開の式と法Nを適用する。パスカルの二項展開は$(a+b)^n$であり、展開の三角形は、良く知られているように次のような係数の性質がある。

```
(a+b)¹           1   1.
(a+b)²         1   2   1.
(a+b)³       1   3   3   1.
(a+b)⁴     1   4   6   4   1.
```

ここでは、係数が問題ではなく、n乗の形は、最上位a^nから、最下位b^nを除いて、各項にaのべき乗項を含みbと係数の積の形をとる(係数は?で示す)。

$(a+b)^n = a^n + ?b \cdot a^{n-1} + ?b^2 \cdot a^{n-2} + ?b^3 \cdot a^{n-3}$,,,,,,,, $?b^{n-3}a^3 + ?b^{n-2} \cdot a^2 + ?b^{n-1} \cdot a + b^n$.

これに合同式の法aを適用するとaのべき乗を含むaの積の項はすべて消え$(a+b)^n \equiv b^n(\mathrm{mod}\,a)$となる。

同様に、$N-2^{\alpha}$のメッセージを暗号化すると、$(N-2^{\alpha})^s \equiv (-2^{\alpha})^s(\mathrm{mod}N)$となり、復号する時、$B^s \equiv A^{r \cdot s} \equiv A(\mathrm{mod}N)$から、$(-2\alpha)^{s \cdot r} \equiv N-2^{\alpha}(\mathrm{mod}N)$となる。任意のメッセージ$(N-2^{\alpha})$のαは、偶数であっても、1でも任意にとれる数値であり、中でも(N+2)は一番容易に理解しやすい形である。ここで単純な事例をあげて説明する。

5. 適用事例

15をNとし、パブリック復号鍵sは3が与えられたとしよう。

1). αを偶数の2とした場合、$(-2^2)^{s \cdot r} \equiv (N-2^2)(\mathrm{mod}N)$、偶数のべき乗は+を取るから$2^{2 \cdot s \cdot r} \equiv N+2^2(\mathrm{mod}N) \equiv 4(\mathrm{mod}N)$。$2^{2 \cdot s \cdot r}-4=kN$、数値を入れると$(2)^{2 \cdot 3 \cdot r}-4-k \cdot 15 = 0$となり、$\{(2)^{6 \cdot r}-4\}-15 \cdot 2^{n1} -15 \cdot 2^{n2} -15 \cdot 2^{n3}$,,, ＝0のように、nを順次下位桁にシフトして、kNの減算を効率化する。2進数にすると、次のようになる。

(1000000,,,,,,-100)-(1111·1000,,,,)、、＝0、
11111111111,,,,,00-11110000,,,,-1111＝0

演算は次のようにおこなう。

この2進数の減算は、$2^{6 \cdot r}-4$から15×2^{14}、15×2^{10}、15×2^6、15×2^2を差引いて、0を確認する。

```
－－－－－－－－－－－－－－－－－－－－－－－
 111111 111111 111100.          (2^(6·r)-4)
-1111                           (15×2^14)
-     11 11                     (15×2^10)
-          1111                 (15×2^6)
-                1111           (15×2^2)
                     00.
```

2). αを1とした場合、$(-2)^{3 \cdot r} \equiv (15-2)(\mathrm{mod}15)$、$\{(-2)^{3 \cdot r}-(15-2)\}-k \cdot 15 = 0$、2進数を適用すると、

-1000 000 000-1101=-1000 001 101

この場合は、$-2^{3 \cdot r}-(-15-2)$から15×2^5、15×2^2、15×1を差引いている。

```
－－－－－－－－－－－－－－－－－－－－－－－
  1000 001 101.                 (2^(3·r)+13)
-  111 1                        (15×2^5)
   000 101 101
-        11 11                  (15×2^2)
-         1 111                 (15)
             0.
```

3). メッセージBを、B＝N+2として考えてみよう。

$(2)^{3 \cdot r} \equiv 2(\mathrm{mod}15)$つまり$8^r \equiv 15+2(\mathrm{mod}15) \equiv 2(\mathrm{mod}15)$だから$8^r-2-k \cdot 15 = 0$。2進数では、

1000 000 000-10=111,111,110

8^3-2から15×2^5と15×2^2を差引くと0となる。

```
－－－－－－－－－－－－－－－－－－－－－－－
 111,111,110.                   (2^(3·r)-2)
- 111 1                         (15×2^5)
-       11 11                   (15×2^2)
             0.
```

いずれの場合もrは3として求められている。

N=15は、一番単純な素数3と5の積である。

$r \cdot s \equiv 1\{\mathrm{mod}(p-1)(q-1)\}$から、$r \cdot s-1=(3-1)(5-1)$、9-1=8。s＝3、r＝3 となり合致する。

6. 崩壊アルゴリズム

一番単純な形のメッセージは(N+2)、(N-2)の形であり、($N-2^{\alpha}$)も同じ結果になるから、rを追求するアルゴリズムの基本形として(N+2)が理解しやすい。

rを求める容易な形、メッセージBをN+2の形にすることは、数学の論理では、暗号メッセージはNを越えないと約束するが、それはN+2≡2(modN)であり、2という数値を暗号化しているからである。挑戦者は、数学の論理や慣習、秩序も無視するから、N+2≡2(modN)もありうる。論理的には、N+2とN-2とは合同式での差はNであり、$N-2^{\alpha}$と$N+2^{\alpha}$との差もNである。この差は$\{(-2\alpha)^{s\cdot r}-(N-2^{\alpha})\}-kN=0$の式のkに関係しs、rには無関係である。

アルゴリズムの基本は二進数にあり、

$2^{s\cdot r}$=1000 000 000,,,,,,,,,000 000、

$2^{s\cdot r}-2$=111 111 111 ,,,,,,,,111 110、のように単純な連続した2進数であらわす。

具体的には、2進数の減算を試算するには、1000,000,000,000,000と0が続く2のs乗のべき乗値から、マイナス2を引いた2進数、111,111,111,111,110を用いると試算し易く、法Nの2進数を上位から減算する論理は$N\times 2^n$を順次、nを下位におろして減算し、0が確認された時、その2進数の桁数が、2のs·r乗である。

2のs乗の桁をグループ(sの数0を持つ)にして、s·r乗とはs乗グループの幾つか(r倍)に限られるから、グループの終わりで、0が確認されると、グループの数がrなのである。

7. 他の適用事例

1).ある暗号者から次の鍵を提供されたとする。

N=35、s=5

$2^s=2^5$=32:100000、N=35:100011

```
  100000 00000 00000 00000 00000.  (2^(5·r))
   11111 11111 11111 11111 11110.  (2^(5·r)-2)
-----------------------------------------------
35:10001 1                              (35×2^19)
     1110 01
-    1000 11
      101 101
-      10 0011
        1 01011
-       1 00011
           1000 11
-          1000 11
                  111 111
-                 100 011
                   11 1001
-                  10 0011
                    1 01101
-                   1 00011
                       1010 11
-                      1000 11
                         10 0011
-                        10 0011
                                0.
   11111 11111 11111 11111 11110.(33554430)
-----------------------------------------------
```

2^5:100000.

32^5 :100000 00000 00000 00000 00000.

32^5-2:11111 11111 11111 11111 11110.

32^5=33554432

33,554,432-2=33554430=35×958698

$2^{5\cdot5}-2-k\cdot35=0$　k=958698　r=5

r·s≡1{mod(5-1)(7-1)} 素数は5と7。

5·5-1=4·6　25-1=24　r=5で合致する。

2).ある暗号者から次の鍵を提供されたとする。

N=33、S=3。

2^3=8：1,000、N=33:100001.

```
  1000 000 000 000 000 000 000.  (2^(3·r))
   111 111 111 111 111 111 110.  (2^(3·r)-2)
-----------------------------------------------
33: 100 001                          (33×2^15)
     11 110 1
-    10 000 1
      1 110 01
-     1 000 01
        110 001
-       100 001
         10 000 1
-        10 000 1
                11 111 1
-               10 000 1
                 1 111 01
-                1 000 01
                   111 001
-                  100 001
                    11 000 1
-                   10 000 1
                     1 000 01
-                    1 000 01
                             0.
   111,111,111,111,111,111,110.  (=2097150)
```

(2097152-2)-(k×33)=0　k=63550

$(2^3)^7$：2097152

r·s≡1{mod(3-1)(11-1)}

r·s≡1{mod(2×10)}　r·s-20=1

(3×7)-20=1　素数は3と11、rは7。

2^3=8：1,000.

8^7：1000,000,000,000,000,000,000.(=2097152)

2097152-2

：　111,111,111,111,111,111,110.(=2097150)

---

8. 試算の推奨

これまでの事例では素数3,5、3,7、3,11を用いた。ほかN=39(素数3,13)s=5、N=51(素数3,17)s=11、N=55(素数5,11)s=9、N=65(素数5,13)s=7などから順次2桁程度の素数を組み合わせて試算されるとRSA公開鍵暗号が単純な論理として理解されるだろう。

rとsの関係は、r·s≡1{mod(p-1)(q-1)}というオイラーの定理と呼ばれる著名な公式で、法Nをpとqに素数分解することが必要で、その素数分解は、過去から計算機でも困難な(幾万年もの処理時間が必要とも)性質をもつアルゴリズムと知られており、他人がNやsからrを知ろうとしても、その素数分解は困難という、明確で巧妙な論理によって相当な納得性が得られていた。しかし、この崩壊アルゴリズムでは、その素数分解は不要である。

公開鍵の弱点は、パスカルの二項展開にあり、そこに2進数を適用すると、べき乗値がいくら巨大でも論理的な理解範囲に捉えられる。実際の公開鍵のNやs、rは、ここで論じているよりも遥かに超巨大な数値であり、その解析はコンピュータでのプログラム処理になるが、今回の論理で短時間の処理で済むことは明らかと考える。その成果はプログラム領域のご専門家に任せたい。

9. 参考文献

一松信「暗号の数理」講談社(1980)
加藤正隆「基礎暗号学Ⅰ,Ⅱ」ｻｲｴﾝｽ社(1986)
吉田武「素数夜曲」海鳴社(1994)
足立宗三郎「電子ﾏﾈｰの全貌」海鳴社(1997)
足立:<ICｶｰﾄﾞを媒体とした電子ﾃﾞｰﾀｻｰｸﾙ>2S-5
「情報処理学会第50回全国大会講演集」(1995)
足立:<公開鍵に替える共通鍵配送方式>1S-8
「情報処理学会第52回全国大会講演集」(1996)
足立:<RSA暗号の強度>「ｶｰﾄﾞｳｪｰﾌﾞ誌'96-4月号」
ｼｰﾒﾃﾞｨｱ社(1996)