情報セキュリティー RSA 暗号

c0115114 菅野 路哉

2016 年 06 月 18 日

1　平文

自分の学籍番号を用いて平文を求める。

初めに、十分に大きい素数である任意の p と q を決定する。今回の暗号化では、p と q は 19, 31 を用いる。

次に、p と q を掛けた値を n とし、学籍番号 (115114) を n - 2 で割った余りに 2 を足したものを平文 m とする。また、n は公開鍵の 1 つである。

$$
\begin{aligned}
p &= 19 \\
q &= 31 \\
n &= p \times q = 19 \times 31 = 589 \\
m &= (115114 \bmod (n-2)) + 2 = (115114 \bmod 589) + 2 = 64
\end{aligned}
$$

n: 589
m: 64

2　秘密鍵生成

p - 1 と q - 1 の最小公倍数を求める。求めた最小公倍数を λ(n) とする。導いた λ(n) を用いて公開鍵の 1 つである e を求める。e が 0 以上 λ(n) 未満かつ、λ(n) と e の最小公約数が 1 となるように e を定める。

$$
\begin{aligned}
\lambda(n) &= LCM(p-1, q-1) \\
p-1 &= 18 = 2 \times 3 \times 3 \\
q-1 &= 30 = 2 \times 3 \times 5 \\
\lambda(n) &= 2 \times 3 \times 5 \times 3 = 90
\end{aligned}
$$

$$
\begin{aligned}
GCD(e, \lambda(n)) &= 1 \\
GCD(0, \lambda(n)) &= 90 \\
GCD(1, \lambda(n)) &= 1 \\
GCD(2, \lambda(n)) &= 2 \\
GCD(3, \lambda(n)) &= 3 \\
GCD(4, \lambda(n)) &= 2 \\
GCD(5, \lambda(n)) &= 5
\end{aligned}
$$

$$GCD(6, \lambda(n)) = 6$$
$$GCD(7, \lambda(n)) = 1$$
$$GCD(8, \lambda(n)) = 2$$
$$GCD(9, \lambda(n)) = 9$$
$$GCD(10, \lambda(n)) = 10$$
$$GCD(11, \lambda(n)) = 1$$
$$GCD(12, \lambda(n)) = 6$$
$$GCD(13, \lambda(n)) = 1$$
$$GCD(14, \lambda(n)) = 2$$
$$GCD(15, \lambda(n)) = 15$$
$$GCD(16, \lambda(n)) = 2$$
$$GCD(17, \lambda(n)) = 1$$
$$GCD(18, \lambda(n)) = 18$$
$$GCD(19, \lambda(n)) = 1$$
$$GCD(20, \lambda(n)) = 10$$
$$GCD(21, \lambda(n)) = 3$$
$$GCD(22, \lambda(n)) = 2$$
$$GCD(23, \lambda(n)) = 1$$
$$GCD(24, \lambda(n)) = 6$$
$$GCD(25, \lambda(n)) = 5$$
$$GCD(26, \lambda(n)) = 2$$
$$GCD(27, \lambda(n)) = 9$$
$$GCD(28, \lambda(n)) = 2$$
$$GCD(29, \lambda(n)) = 1$$
$$GCD(30, \lambda(n)) = 30$$
$$GCD(31, \lambda(n)) = 1$$
$$GCD(32, \lambda(n)) = 2$$
$$GCD(33, \lambda(n)) = 3$$
$$GCD(34, \lambda(n)) = 2$$
$$GCD(35, \lambda(n)) = 5$$
$$GCD(36, \lambda(n)) = 18$$
$$GCD(37, \lambda(n)) = 1$$
$$GCD(38, \lambda(n)) = 2$$
$$GCD(39, \lambda(n)) = 3$$
$$GCD(40, \lambda(n)) = 10$$
$$GCD(41, \lambda(n)) = 1$$
$$GCD(42, \lambda(n)) = 6$$
$$GCD(43, \lambda(n)) = 1$$
$$GCD(44, \lambda(n)) = 2$$
$$GCD(45, \lambda(n)) = 45$$
$$GCD(46, \lambda(n)) = 2$$

$GCD(47, \lambda(n)) = 1$
$GCD(48, \lambda(n)) = 6$
$GCD(49, \lambda(n)) = 1$
$GCD(50, \lambda(n)) = 10$
$GCD(51, \lambda(n)) = 3$
$GCD(52, \lambda(n)) = 2$
$GCD(53, \lambda(n)) = 1$
$GCD(54, \lambda(n)) = 18$
$GCD(55, \lambda(n)) = 5$
$GCD(56, \lambda(n)) = 2$
$GCD(57, \lambda(n)) = 3$
$GCD(58, \lambda(n)) = 2$
$GCD(59, \lambda(n)) = 1$
$GCD(60, \lambda(n)) = 30$
$GCD(61, \lambda(n)) = 1$
$GCD(62, \lambda(n)) = 2$
$GCD(63, \lambda(n)) = 9$
$GCD(64, \lambda(n)) = 2$
$GCD(65, \lambda(n)) = 5$
$GCD(66, \lambda(n)) = 6$
$GCD(67, \lambda(n)) = 1$
$GCD(68, \lambda(n)) = 2$
$GCD(69, \lambda(n)) = 3$
$GCD(70, \lambda(n)) = 10$
$GCD(71, \lambda(n)) = 1$
$GCD(72, \lambda(n)) = 18$
$GCD(73, \lambda(n)) = 1$
$GCD(74, \lambda(n)) = 2$
$GCD(75, \lambda(n)) = 15$
$GCD(76, \lambda(n)) = 2$
$GCD(77, \lambda(n)) = 1$
$GCD(78, \lambda(n)) = 6$
$GCD(79, \lambda(n)) = 1$
$GCD(80, \lambda(n)) = 10$
$GCD(81, \lambda(n)) = 9$
$GCD(82, \lambda(n)) = 2$
$GCD(83, \lambda(n)) = 1$
$GCD(84, \lambda(n)) = 6$
$GCD(85, \lambda(n)) = 5$
$GCD(86, \lambda(n)) = 2$
$GCD(87, \lambda(n)) = 3$

$$GCD(88, \lambda(n)) = 2$$
$$GCD(89, \lambda(n)) = 1$$
$$GCD(90, \lambda(n)) = 90$$

$\lambda(n)$: 90

e の候補: 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77, 79, 83, 89

e: 17

導いた λ(n) を用いて秘密鍵 d を求める。d を求める式を以下に示す。

$$d = \frac{1}{e} \bmod \{\lambda(n)\}$$

式を変形して、$(d \times e - 1) \bmod \lambda(n) = 0$ となるように d を決定する。

$$(d \times e - 1) \bmod \lambda(n) = 0$$
$$(53 \times 17 - 1) \bmod 90 = 0$$
$$900 \bmod 90 = 0$$

d: 53

3 暗号化

暗号文 c を求める。暗号文は $c = m^e \bmod n$ で求める。

公開鍵 e: 17, n: 589

平文 m: 64

$m^e = 64^{17}$

```
    64
*   64
------
   256
  384
------
  4096

    4096
*     64
--------
   16384
  24576
--------
  262144

    262144
```

```
*       64
----------
   1048576
  1572864
----------
  16777216

    16777216
*         64
------------
    67108864
  100663296
------------
  1073741824

   1073741824
*          64
-------------
   4294967296
  6442450944
-------------
  68719476736

    68719476736
*            64
---------------
   274877906944
  412316860416
---------------
  4398046511104

    4398046511104
*              64
-----------------
   17592186044416
  26388279066624
-----------------
  281474976710656

    281474976710656
```

```
*                 64
-------------------
   1125899906842624
  1688849860263936
-------------------
  18014398509481984

    18014398509481984
*                  64
---------------------
    72057594037927936
  108086391056891904
---------------------
  1152921504606846976

   1152921504606846976
*                   64
----------------------
   4611686018427387904
  6917529027641081856
----------------------
  73786976294838206464

    73786976294838206464
*                     64
------------------------
   295147905179352825856
  442721857769029238784
------------------------
  4722366482869645213696

    4722366482869645213696
*                       64
--------------------------
   18889465931478580854784
  28334198897217871282176
--------------------------
  302231454903657293676544

    302231454903657293676544
```

```
*                          64
---------------------------
   1208925819614629174706176
  1813388729421943762059264
---------------------------
  19342813113834066795298816

    19342813113834066795298816
*                           64
-----------------------------
    77371252455336267181195264
  116056878683004400771792896
-----------------------------
  1237940039285380274899124224

   1237940039285380274899124224
*                            64
------------------------------
   4951760157141521099596496896
  7427640235712281649394745344
------------------------------
  79228162514264337593543950336

    79228162514264337593543950336
*                              64
--------------------------------
   316912650057057350374175801344
  475368975085586025561263702016
--------------------------------
  5070602400912917605986812821504
```

$$
\begin{aligned}
&5070602400912917605986812821504 \bmod n \\
&= 5070602400912917605986812821504 \bmod 589
\end{aligned}
$$

```
        8608832599173034984697475078
   --------------------------------
589)5070602400912917605986812821504
    4712
    ----
```

```
358
3586
3534
----
  52
  520
    0
  ---
  520
  5202
  4712
  ----
   490
   4904
   4712
   ----
    192
    1920
    1767
    ----
     153
     1530
     1178
     ----
      352
      3529
      2945
      ----
       584
       5841
       5301
       ----
        540
        5402
        5301
        ----
         101
         1019
          589
         ----
```

```
430
4301
4123
----
 178
 1787
 1767
 ----
   20
   206
     0
   ---
   206
   2060
   1767
   ----
    293
    2935
    2356
    ----
     579
     5799
     5301
     ----
      498
      4988
      4712
      ----
       276
       2766
       2356
       ----
        410
        4108
        3534
        ----
         574
         5741
         5301
         ----
```

```
440
4402
4123
----
 279
 2798
 2356
 ----
  442
  4422
  4123
  ----
   299
   2991
   2945
   ----
     46
     465
       0
     ---
     465
     4650
     4123
     ----
      527
      5274
      4712
      ----
       562
```

暗号: 562

よって、暗号文 562 が導かれた。また、復号の確認も行う。復号は、$m = c^d \bmod n$ によって確認できる。

$562^1 = 562$

$562^2 = 315844$

$562^3 = 177504328$

$562^4 = 99757432336$

$562^5 = 56063676972832$

$562^6 = 31507786458731584$

$562^7 = 17707375989807150208$

$562^{8} = 99515453062716184168 96$

$562^{9} = 55927684621246495502955 52$

$562^{10} = 3143135875714053047266100224$

$562^{11} = 1766442362151297812563548325888$

$562^{12} = 992740607529029370660714159149056$

$562^{13} = 557920221431314506311321357441769472$

$562^{14} = 313551164444398752546962602882274443264$

$562^{15} = 176215754417752098931392982819838237114368$

$562^{16} = 99033253982776679599442856344749089258274816$

$562^{17} = 55656688738320493934886885265748988163150446592$

$562^{18} = 31279059070936117591406429519350931347690550984704$

$562^{19} = 17578831197866098086370413389875223417402089653403648$

$562^{20} = 9879303133200747124540172325109875560579974385212850176$

$562^{21} = 5552168360858819883991576846711750065045945604489621798912$

$562^{22} = 3120318618802656774803266187852003536555821429723167450988544$

$562^{23} = 1753619063767093107439435597572825987544371643504420107455561728$

$562^{24} = 985533913837106326380962805835928204999936863649484100390025691136$

$562^{25} = 553870059576453755426101096879791651209964517371010064419194438418432$

$562^{26} = 311274973481967010549468816446442907980000058762507656203587274391158784$

$562^{27} = 174936535096865459928801474842900914284760033024529302786416048207831236608$

$562^{28} = 98314332724438388479986428861710313828035138559785468165965819092801154973696$

$562^{29} = 55252654991134374325752373020281196371355747870599433109272790330154249095217152$

$562^{30} = 31051992105017518371072833637398032360701930303276881407411308165546687991512039424$

$562^{31} = 17451219563019845324542932504217694186714484830441607350965155189037238651229766156288$

$562^{32} = 9807585394417153072393128067370344132933540474708183331242417216238928121991128579833856$

$562^{33} = 5511862991662440026684937973862133402708649746785999032158238475526277604559014261866627072$

$562^{34} = 3097667001314291294996935141310518972322261157693731456072930023245768013762166015169044414464$

$562^{35} = 1740888854738631707788277549416511662445110770623877078312986673064121623734337300525002960928768$

$562^{36} = 978379536363111019777011982772079554294152253090618918011898510262036352538697562895051664041967616$

$562^{37} = 549849299436068393114680734317908709513313566236927831922686962767264430126748030347019035191585800192$

$562^{38} = 309015306283070436930450572686664694746482224225153441540550073075202609731232393055024697777671219707904$

$562^{39} = 173666602131085585554913221849905558447523010014536234145789141068263866668952604 8969$

2388015105122547584 2048

$562^{40} = 9760063039767009908186123067964692384750793162816936358993349728036429306795136395207$
$1220644890788717423230976$

$562^{41} = 5485155428349059568400601164196157120229945757503118233754262547156473270418866654106$
$4026002428623259191855808512$

$562^{42} = 3082657350732171477441137854278240301569229515716752447369895551501937977975403059607$
$7982613364886271665822964383744$

$562^{43} = 1732453431111480370321919474104371049481906987832814875421881299944089143622176519499$
$5826228711066084676192505983664128$

$562^{44} = 9736388282846519681209187444466565298088317271620419599870972905685780987156632039587$
$6543405356191395880201883628192399 36$

$562^{45} = 5471850214959744060839563343790209697525634306650675815127486772995408914782027206248$
$2617393810179564484673458599044128 44032$

$562^{46} = 3075179820807376162191834599210097850009406480337679808101647566423419810107499289911$
$5230975321320915240386483732662800 18345984$

$562^{47} = 1728251059293745403151811044756074991705286441949776052153125932329961933280414600930$
$2759808130582354365097203857756493703 10443008$

$562^{48} = 9712770953230849165713178071529141453383709803757741413100567739694386065035930057228$
$1510121693872831531846285680591494611 4468970496$

$562^{49} = 5458577275715737231130806076199377496801644909711850674162519069708244968550192692162$
$2208688391956531320897612555249241997163315 61418752$

$562^{50} = 3067720428952244323895513014824050153202524439258060078879335717176033672325208292995$
$1681282876279570602344458254500740024057833751 7338624$

$562^{51} = 1724058881071161310029278314331116186099818734863029764330186673052930923846767060663$
$2844880976469118678517585539029415893520502568474 4306688$

$562^{52} = 9689210911619926562364544126540872965880981289930227275535649102557471792018830880927$
$6588231087756446973268830729345317321585224434826300 358656$

$562^{53} = 5445336532330398728048873799115970606825111484940787728851034795637299147114582955081$
$3442585871319123198977082869892068334730896132372380801 564672$

$5445336532330398728048873799115970606825111484940787728851034795637299147114582955081344258587131 9$
$1231989770828698920683347308961323723808015 64672 \bmod 589 = 64$

復号: 64

初めに求めた平文と同じ結果が得られたため、復号が正しく行われた。