高校生のための現代数学講座　　東京大学
「素数と暗号」　　玉原国際セミナーハウス
講義 (2) 高木 俊輔　　2017 年 7 月 22 日

「RSA 暗号の実際」

この講義では 2 人 1 組になり，RSA 暗号を計算してみよう．現在インターネット上で実際に使われている RSA 暗号には $n = pq$ として 10 進数で 300〜1000 桁という非常に大きい数が用いられるが，計算の都合上この講義では n は高々 4 桁の数とする．まず鍵の作成担当者が，§1 の手順に従い，鍵を作成する．暗号化の担当者は，§2 の手順に従い，公開鍵を用いて暗号文を作成せよ．そして鍵の作成担当者は，§3 の手順に従い，秘密鍵を用いてその暗号文を復号せよ．

1　鍵の作成手順

ステップ 1-1

$$29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

の中から好きな数を 2 つ選び，p, q とする．ただし，同じ数を 2 つ選んではいけない．さらに $n = pq$ とする．

$p =$ ☐　$q =$ ☐　$n =$ ☐

ステップ 1-2　$(p-1)(q-1)$ を計算し，$(p-1)(q-1)$ を割り切らない素数 e を

$$3, 5, 7, 11, 13$$

の中から 1 つ選ぶ．小さい e を選んだ方が暗号化の計算が楽になる．

$(p-1)(q-1) =$ ☐　$e =$ ☐

ステップ 1-3　$m(p-1)(q-1) \equiv -1 \pmod{e}$ となる自然数 $1 \leq m \leq e-1$ を求める．そして，$m(p-1)(q-1)+1$ を e で割った商を d とする．

$m =$ ☐　$d =$ ☐

ステップ 1-4　n, e が**公開鍵**である．n, e の値を相手に教えよう．p, q, d は**秘密鍵**なので，決して相手に教えてはいけない!

2　暗号化の手順

ステップ 2-0　相手から受け取った公開鍵を書き込もう．

$n =$ ＿＿＿＿＿＿　$e =$ ＿＿＿

ステップ 2-1　相手に伝える平文を決めて，ローマ字で記入する．

平文（ローマ字）＝ ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

ステップ 2-2　次の表を使ってアルファベットを数字に変換し，各数字の間をハイフンでつなぐ．

アルファベット	数字
A	2
B	3
C	4
D	5
E	6
F	7
G	8
H	9
I	10

アルファベット	数字
J	11
K	12
L	13
M	14
N	15
O	16
P	17
Q	18
R	19

アルファベット	数字
S	20
T	21
U	22
V	23
W	24
X	25
Y	26
Z	27
スペース	28

例えば，平文が BARUSU（バルス）ならば，3-2-19-22-20-22 となる．

平文（数字）＝ ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

ステップ 2-3　得られた数字の列を M_1-M_2-$\cdots$-M_r（各 M_i は 28 以下の自然数）としたとき，各 $i = 1, \ldots, r$ について $M_i^e \equiv N_i \pmod{n}$ となる自然数 $1 \leq N_i \leq n-1$ を計算する．N_1-N_2-$\cdots$-N_r が暗号文である．

暗号文 ＝ ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

暗号文のみ相手に教える．平文は教えてはいけない!

3　復号の手順

ステップ 3-0　相手から受け取った暗号文を書き込もう．

暗号文 =

ステップ 3-1　暗号文を N_1-N_2-$\cdots$-N_r（各 N_i は $n-1$ 以下の自然数）としたとき，各 $i = 1, \ldots, r$ についてフェルマーの小定理を用いて $N_i^d \equiv M_i \pmod{n}$ となる自然数 $2 \leq M_i \leq 28$ を計算する（§4 のステップ 3-1 を参考にせよ）．M_1-M_2-$\cdots$-M_r が復元された平文（数字）である．

平文（数字）=

ステップ 3-2　次の表を使って各 M_i をアルファベットに変換する．

数字	アルファベット
2	A
3	B
4	C
5	D
6	E
7	F
8	G
9	H
10	I

数字	アルファベット
11	J
12	K
13	L
14	M
15	N
16	O
17	P
18	Q
19	R

数字	アルファベット
20	S
21	T
22	U
23	V
24	W
25	X
26	Y
27	Z
28	スペース

平文（ローマ字）=

ステップ 3-3　正しく復元されたか，相手に確かめてみよう．

4 例

例として，$p = 29, q = 41$ として鍵を作成し，平文 BARUSU を暗号化・復号する手順を確認する．

ステップ 1-1 $p = 29$、$q = 41$ とする．このとき，$n = pq = 1189$ である．

ステップ 1-2 $(p-1)(q-1) = 1120$ は 3 で割り切れない．そこで $e = 3$ とする．

ステップ 1-3 $1120 \equiv 1 \pmod 3$ なので，$m = 2$ とすると，

$$1120m \equiv 2 \equiv -1 \pmod 3$$

となる．$1120m + 1$ を 3 で割った商は 747 なので，$d = 747$ とする．

ステップ 2-1 平文 (ローマ字)=BARUSU

ステップ 2-2 平文 (数字)=3-2-19-22-20-22

ステップ 2-3 $3^3 \equiv 27 \pmod{1189}$，$2^3 \equiv 8 \pmod{1189}$，$19^3 \equiv 914 \pmod{1189}$，$22^3 \equiv 1136 \pmod{1189}$，$20^3 \equiv 866 \pmod{1189}$ より，暗号文は 27-8-914-1136-866-1136 となる．

ステップ 3-1 $d = 747, n = 1189$ なので，暗号文の数字の 747 乗を 1189 で割った余りが知りたい．以下で，914 の 747 乗を 1189 で割った余りの計算の仕方を説明する．

914 を $p = 29$ で割った余りを計算すると，$914 \equiv 15 \pmod{29}$ である．フェルマーの小定理より $15^{28} \equiv 1 \pmod{29}$ であるので，$747 \equiv 19 \pmod{28}$ から

$$914^{747} \equiv 15^{747} \equiv 15^{19} \equiv 19 \pmod{29}$$

が従う．各アルファベットは 28 以下の自然数に変換されているので，復号して得られる数字も 28 以下の自然数である．よって 914 の 747 乗を 1189 で割った余りも 28 以下の自然数でなければならない．このことから $914^{747} \equiv 19 \pmod{1189}$ を得る．

914 を $q = 41$ で割った余りを計算すると，$914 \equiv 12 \pmod{41}$ である．フェルマーの小定理より $12^{40} \equiv 1 \pmod{41}$ であるので，$747 \equiv 27 \pmod{40}$ から

$$914^{747} \equiv 12^{747} \equiv 12^{27} \equiv 19 \pmod{41}$$

が従う．このことから $914^{747} \equiv 19 \pmod{1189}$ であると結論付けてもよい（どちらか一方を計算すれば十分である）．

同様にして，$27^{747} \equiv 3 \pmod{1189}$，$8^{747} \equiv 2 \pmod{1189}$，$1136^{747} \equiv 22 \pmod{1189}$，$866^{747} \equiv 20 \pmod{1189}$ と計算できるので，平文（数字）は 3-2-19-22-20-22 である．

ステップ 3-2 平文 (ローマ字)=BARUSU