RSA 暗号の暗号化

C0118005 秋本　遥基

2019/06/10

1　はじめに

本レポートは RSA 暗号による暗号手順について考察をするものである。

2　RSA 暗号による暗号化および復号

RSA 暗号による暗号化及び復号の手順を実例を用いて示す。

2.1　初期値の設定

平文 m を設定する。

$$\text{学籍番号は } C0118005 \tag{1}$$
$$n = pq \tag{2}$$
$$n = 19 \times 31 \tag{3}$$
$$= 589 \tag{4}$$
$$118005 \div (589 - 2) = 201 \ldots 18 \tag{5}$$
$$m = 18 + 2 \tag{6}$$
$$= 20 \tag{7}$$

今回は学籍番号の数字部分を n-2 で割りその余りに 2 を足した数で生成する。RSA 暗号は 2 数の素数を用いるが今回はこれを $p, q = 19, 31$ とする。また、n はこの 2 数の積によって求められる。したがって、$n = 19 \times 31$ より $n = 589$ となる。また $n - 2$ より、割る値は 587 となる。$118005 \bmod 587 = 18$ よって $m = 18 + 2 = 20$

2.2　秘密鍵および公開鍵の設定

以下の式により、秘密鍵 d、公開鍵 e 及び n を設定する。

$$\lambda(n) = LCM(p - 1, q - 1) \tag{8}$$
$$GCD(e, \lambda_{(n)}) = 1(e \in Z_{\lambda(n)}) \tag{9}$$

$$d = \frac{1}{e} \bmod \lambda(n) \tag{10}$$

(8) の LCM() は関数内の最小公倍数を返すものである。したがって、p-1=18,q-1=30 の最小公倍数であり、これは 90 である。

(9) の GCD() は関数内の最大公約数を返すものである。したがって、これは最大公約数が 1 となるため e と $\lambda(n)$ は互いに素な関係である。これを満たす e は、$\lambda(n)$ と素でありかつ 0 以上$\lambda(n)$ 未満な数である。よって e の候補は $7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89$ である。

次に (10) を求める。ここで e を 7 とすると、7d-1 が $\lambda(n)$ で割り切れるものを探せば良いので、$d = 13$ がこれに該当する。したがって、$d = 13, e = 7, n = 589, m = 20$ となる。

2.3 暗号化と復号

$$c = m^e \bmod n \tag{11}$$

$$m = c^d \bmod n \tag{12}$$

ここで、前節で設定した値を用いて暗号化をする。また、暗号文を c と定める。暗号文はで (11) 求められる。したがって、これは m=20 の e=7 乗を n=589 で割ったあまりであり、514 となる。この計算を以下の図に示す。

図 1　$m^e \bmod n$ の筆算

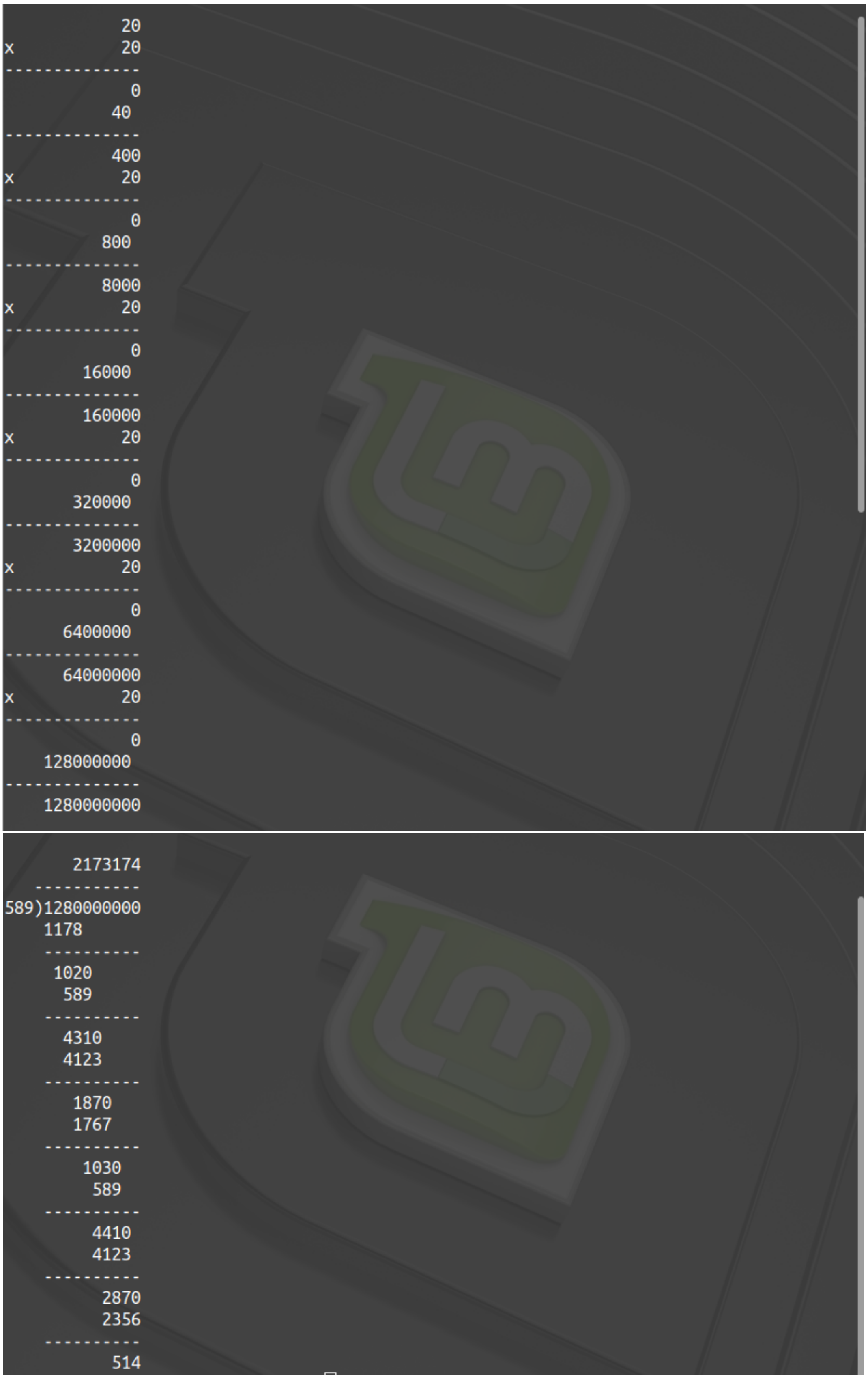
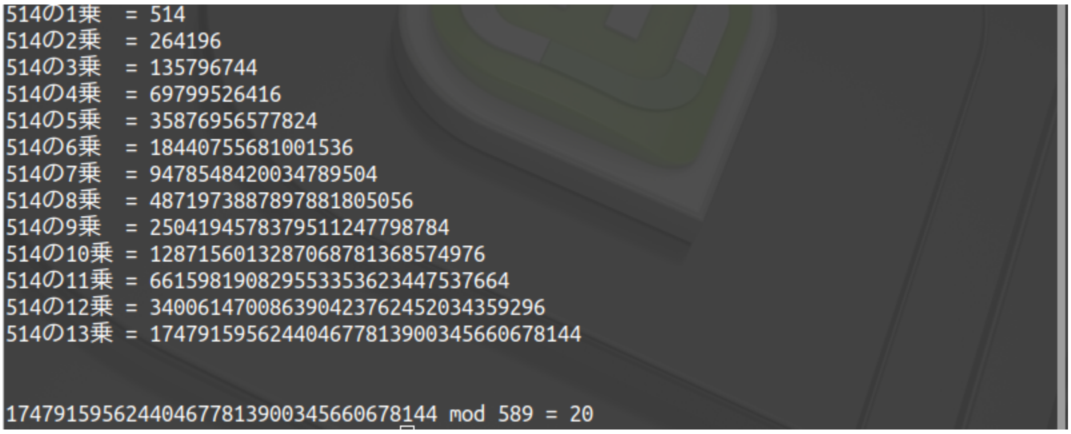


図 1　$m^e \bmod n$ の筆算

また、この復号は (12) で求められる。これは 20 となり、正しく復号されたことがわかる。この計算を以下の図に示す。



```
514の1乗  = 514
514の2乗  = 264196
514の3乗  = 135796744
514の4乗  = 69799526416
514の5乗  = 35876956577824
514の6乗  = 18440755681001536
514の7乗  = 9478548420034789504
514の8乗  = 4871973887897881805056
514の9乗  = 2504194578379511247798784
514の10乗 = 1287156013287068781368574976
514の11乗 = 661598190829553353623447537664
514の12乗 = 340061470086390423762452034359296
514の13乗 = 174791595624404677813900345660678144


174791595624404677813900345660678144 mod 589 = 20
```

図 2　$c^d \bmod n$ の筆算

3　考察

RSA 暗号による暗号の n を決めるための 2 値の推定の難しさと、公開鍵と秘密鍵による暗号化・復号の容易さが確かめられた。