

### 13.4.0 公開鍵暗号

暗号系の本質： 1つの通信文を、鍵と暗号文との2つの通信路に分けて送る。

鍵は、次の3通りのどの方法で送信してもよい。

- (1) 送信者から受信者に送る。
- (2) 受信者から送信者に送る。
- (3) 第三者が送信者と受信者に送る。

#### 公開鍵暗号系の概念 W. Diffie, M. Hellman (1976)

- 受信者が鍵の対  $e, d$  を作って、暗号化用の鍵  $e$  だけを送信者に送る。
- 復号用の鍵  $d$  は受信者だけの秘密にしておく。
- 暗号化用の鍵  $e$  から秘密の復号用の鍵  $d$  が算出できなければ安全である。

### 13.4.1 剰余演算（割った余りについての演算）

知っていると便利な剰余

例：4日ごとの休日の日付を知る方法

2017年 11月  
日 月 火 水 木 金 土  
                  1 2 3 4  
5 6 7 8 9 10 11  
12 13 14 15 16 17 18   4で割ると余りは1  
19 20 21 22 23 24 25  
26 27 28 29 30

2017年 12月  
日 月 火 水 木 金 土  
                  1 2  
3 4 5 6 7 8 9  
10 11 12 13 14 15 16   4で割ると余りは3  
17 18 19 20 21 22 23  
24 25 26 27 28 29 30  
31

2018年 1月  
日 月 火 水 木 金 土  
  1 2 3 4 5 6  
7 8 9 10 11 12 13   4で割ると余りは0  
14 15 16 17 18 19 20  
21 22 23 24 25 26 27  
28 29 30 31

2018年 2月  
日 月 火 水 木 金 土  
                  1 2 3  
4 5 6 7 8 9 10  
11 12 13 14 15 16 17   4で割ると余りは1  
18 19 20 21 22 23 24  
25 26 27 28

2018年 3月  
日 月 火 水 木 金 土  
                  1 2 3  
4 5 6 7 8 9 10  
11 12 13 14 15 16 17   4で割ると余りは1  
18 19 20 21 22 23 24   (28が4で割り切れるから)  
25 26 27 28

例： 時計の算数（<sup>ほう</sup>法 60 で割る）

$$227 \text{ 分} = \square \text{ 時間 } \square \text{ 分}$$

分の <sup>げん</sup>元（要素）は、0～59 の 60 個である。

### 記法

$$47 \equiv 227 \pmod{60}$$

$$47 \equiv 167 \pmod{60}$$

$$47 \equiv 107 \pmod{60}$$

$$47 \equiv 47 \pmod{60}$$

$$47 \equiv -13 \pmod{60}$$

$$47 \equiv -73 \pmod{60}$$

まとめて書くと、

$$167 \equiv 107 \equiv 47 \equiv -13 \pmod{60}$$

法が 60 のとき、 $47+60k$  ( $k$  は整数) はすべて合同な数である。

### 四則演算

加算  $47+20 \equiv 7 \pmod{60}$

減算  $7-20 \equiv 47 \pmod{60}$

$$7+40 \equiv 47 \pmod{60}$$

20 を引く代わりに 40 を加えても結果は同じだ！

$a$  に対して、法  $-a$  を “ $a$  の補数” という。

法が 60 のとき、 $60-20=40$  が 20 の補数である。

乗算  $56 \times 7 \equiv 32 \pmod{60}$

$$\begin{aligned} 56 \times 7 &\equiv (60-4) \times 7 \equiv 60 \times 7 - 4 \times 7 \\ &\equiv -4 \times 7 \equiv -28 \equiv 32 \pmod{60} \end{aligned}$$

除算  $32 \div 7 \equiv 56 ? \pmod{60}$

法が 60 のときの 7 の逆元 ( $7^{-1}$ ) は 43 だ！

検算：  $7 \times 43 = 301 \equiv 1 \pmod{60}$

$$32 \div 7 \equiv 32 \times 7^{-1} \equiv 32 \times 43 \equiv 56 \pmod{60}$$

法と元とが互いに素 (1 以外に共通の約数をもたない) のとき、乗法の逆元が存在する。(したがって、法が素数なら、0 以外のすべての元に逆元が存在する.)

### 13.4.2 逆関数の表記

関数  $f$   $\longleftrightarrow$  逆関数  $f^{-1}$   
暗号化  $E$   $\longleftrightarrow$  復号  $E^{-1}$  (=D)

(冗長性 redundancy)

これは冗談用です :

#### 4 種類の塩基 (アミノ酸の素)

A アデニン

C シトシン

G グアニン

T チミン