授業期間短縮について

今夏に予想される電力供給の逼迫の対策として、
授業期間が 2 週間短縮されます

本科目は今の所は補講を計画していません

必要に応じて課題などで対応する予定です

暗号 (cryptography)

- **共通鍵暗号** (秘密鍵暗号)
  - ⋆ 送信者・受信者で同じ鍵を秘密裡に共有
  - ⋆ 共通の鍵で暗号化・復号を行なう

- **公開鍵暗号**
  - ⋆ 暗号化鍵 (公開鍵)・復号鍵 (秘密鍵) が別
  - ⋆ 公開された暗号化鍵を用いて暗号化
  - ⋆ 復号鍵は受信者だけの秘密

秘密鍵 (共通鍵) 暗号

暗号化鍵・復号鍵が同じ

- 換字暗号・Caesar 暗号
- 線型ブロック暗号
- Vernam 暗号
- DES (Data Encryption Standard)
- AES (Advances Encryption Standard)

例：Caesar 暗号

鍵： $1 \leq n \leq 25$ **なる整数** n

暗号化：alphabet を後ろに n **だけずらす**

復号：alphabet を前に n **だけ戻す**

$\cdots$ XYZABCDEFGHIJKLMN
OPQRSTUVWXYZABC $\cdots$

例: $n = 3$ **：** HELLO $\longrightarrow$ KHOOR

Caesar 暗号の脆弱性

鍵を知らなくても容易に解読されてしまった

- **鍵の可能性が少なく、総当たりで倒せる**
- **暗号文に平文の特徴が残っている**

このような脆弱性を克服した暗号方式が
現在では用いられている

- **DES (Deta Encryption Standard)**
- **AES (Advanced Encryption Standard)**

脆弱性の克服手段の例

- 鍵の可能性が少なく、総当たりで倒せる
  $\longrightarrow$ 鍵の可能性 (鍵空間) を大きくする
  $\star$ 何文字かの組で暗号化 (ブロック暗号)
  $\star$ ずらす以外の変換も考える (換字暗号)

- 暗号文に平文の特徴が残っている
  $\longrightarrow$ 同じ平文を毎回異なる暗号文に変換する
  $\star$ 直前のブロックを変換に影響させる
  $\star$ 乱数を利用する　　など

脆弱性の克服手段の例

“ずらす以外の変換” をうまく作るには ？

$\longrightarrow$ 文字集合の数理的な構造を利用

文字が m 種類

$\longrightarrow$ 各文字を $0, 1, \ldots, \mathrm{m}-1$ と番号付け (符号化)

$\longrightarrow$ “m で割った余り” と考える (剰余系)

合同式

m : 1 以上の整数を一つ取って固定

m で割った余りのみに注目して計算する

a と b とが m を法として合同
(congruent modulo m)

$$a \equiv b \pmod{m}$$

$\overleftarrow{\iff}$ a と b とを m で割った余りが等しい

$\iff$ $m \mid (a-b)$ ($a-b$ が m で割切れる)

$\iff$ $\exists k \in \mathbb{Z} : a - b = mk$

合同式の基本性質 (同値律)

以下暫く、
法 m を固定して考えて $(\mathrm{mod}\ m)$ を省略

- $a \equiv a$ **(反射律)**
- $a \equiv b \Longrightarrow b \equiv a$ **(対称律)**
- $a \equiv b, b \equiv c \Longrightarrow a \equiv c$ **(推移律)**

合同関係 $\equiv$ は同値関係である (同値律を満たす)

合同式の基本性質 (演算との関係)

- $x \equiv y \Longrightarrow x \pm c \equiv y \pm c, cx \equiv cy$

- $a \equiv a', b \equiv b'$
  $\Longrightarrow a \pm b \equiv a' \pm b', ab \equiv a'b'$

加減乗は余りだけを見て計算が出来る

では除法は？

拡張版 Euclid の互除法

2 **整数** $a, b \in \mathbb{Z}$ **の最大公約数を**
$d := \gcd(a, b)$ **とするとき、**

$$\exists x, y \in \mathbb{Z} : ax + by = d$$

特に、 a, b **が互いに素なとき、**

$$\exists x, y \in \mathbb{Z} : ax + by = 1$$