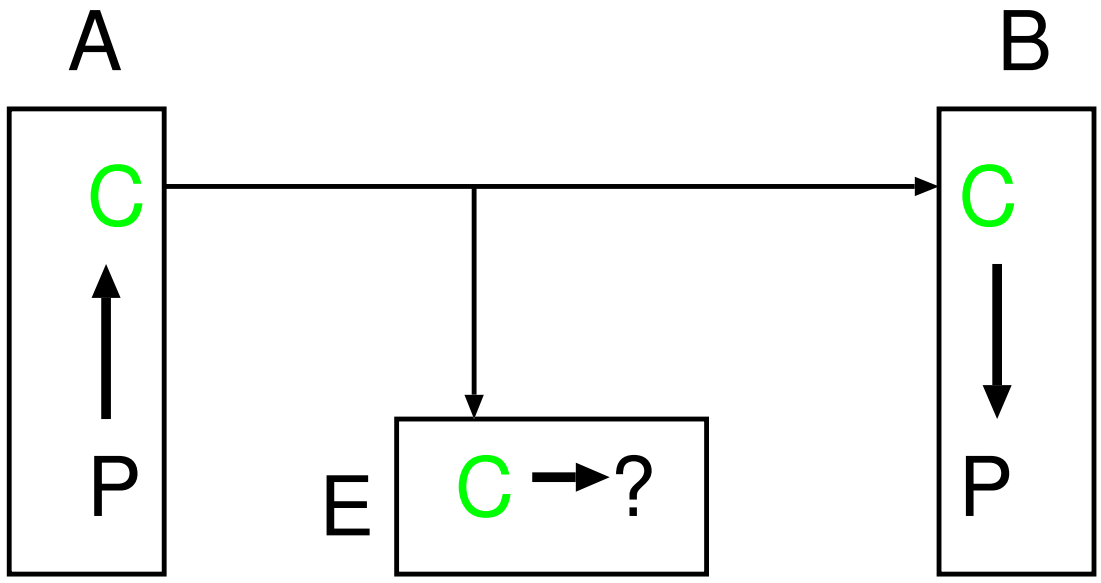
暗号 (cryptography)



- 送信者 A が平文 P を暗号化、暗号文 C を送信
- 受信者 B が暗号文 C を受信、平文 P に復号
- 盗聴者 E は暗号文 C を知っても
  平文 P を復元できない

$\longrightarrow$ B だけが**復号鍵**を持っていることが必要

暗号 (cryptography)

公開された情報伝達路 (盗聴可能 と仮定) で、

暗号方式を公開 して通信

- 対称鍵暗号 (symmetric-key cryptography)
  (秘密鍵暗号・共通鍵暗号とも)
- 公開鍵暗号 (public-key cryptography)

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： $1 \leq \mathrm{n} \leq 25$ **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: $\mathrm{n} =$ **?** **:** **?????** $\longrightarrow$ **KHOOR**

例：Caesar 暗号

鍵： $1 \leq \mathrm{n} \leq 25$ **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: $\mathrm{n} = 3$ **：** 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)

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

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

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

(余談) “法 (modulus)” という用語について

7 を 3 で割ると、2 が立って余り 1

$$\begin{array}{ccccccc} 7 & = & 3 & \times & 2 & + & 1 \\ \textbf{実} & & \textbf{法} & & \textbf{商} & & \textbf{余} \end{array}$$

割る数・基準・単位になるもの・沿うべきもの

“のり”
(典・徳・法・紀・憲・則・範・規・儀・教)

合同式

m：1 以上の整数を一つ取って固定

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

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

$\overleftrightarrow{\iff}$ 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)

以下、暫く板書で解説