暗号技術

暗号化

- データを別の記号で置き換える
- データ保護における重要な技術
- 「鍵」があればもとに戻せる
- 「謎解き」は「変換の方法」がわからない
- 「暗号」は「変換の方法」はわかるけど，変換に必要な「鍵」（パラメータ）がわからない

シーザー暗号

- 変換の方法：アルファベットをx個ずらす
- 鍵: x 個

```
This is a pen => UijtAjtAbAqfo
```

共通鍵暗号方式

- データにアクセスできる人（データアクセス許可されている人）全員が同じ鍵を共有する
- 暗号方式: DES, AES, etc.
- リスク
  - 鍵が漏洩すると影響範囲が大きい

公開鍵暗号方式

- 二種類の鍵
  - 公開鍵：閉めるだけの鍵
  - 秘密鍵：開けるだけの鍵
- 二つの鍵はペアになっている
- 番号を合わせる南京錠のイメージ
  - データを送る側は誰でも鍵をかけられる
  - データを受け取る側は開けるための番号（秘密鍵）を持っている

RSA暗号

1. 異なる二つの大きな素数 p, q を決める
2. $n = pq$ とする
3. $(p-1)(q-1)$ と互いに素な自然数 e を決める
4. ed を $(p-1)(q-1)$ で割った余りが1となるような自然数 d を決める

- 公開鍵 (e, n) ➡️ 平文 x を e 乗して，n で割った余りが暗号文 y
- 秘密鍵 (d, n) ➡️ 暗号文 y を d 乗して，n で割った余りが平文 x

公開鍵 (e, n) から d がわからないことが大事 ➡️ n が素因数分解できるとばれる

PKI (Public Key Infrastucture)

- そもそも公開鍵が改ざんされていたら？
- 間違いなく本人の鍵であることを誰かが証明
- その誰かが本物か？間違いなく本物であることを誰かが証明
- ・・以下同様
- PKI: 階層構造により鍵の正しさを証明

署名

- データが不正に変更されていないことを証明する
- 署名側
  - データ固有のハッシュ値を計算する
  - ハッシュ値を秘密鍵で暗号化したものを署名として書類につける
- 検証側
  - 受け取ったデータのハッシュ値を計算する（A）
  - 受け取った署名を公開鍵で復号する（B）
  - AとBが一致しているかどうか