セキュリティ技術

- 暗号・認証技術
- セキュア通信技術
- システムの各要素に関するセキュリティ

暗号・認証技術

- 暗号・認証の説明の前に、身近な認証技術について触れてみましょう
- 最寄の駅、住んでいる県・市町村、出身校、郵便番号などをトリップにしてスレに書き込んでみましょう

暗号・認証技術

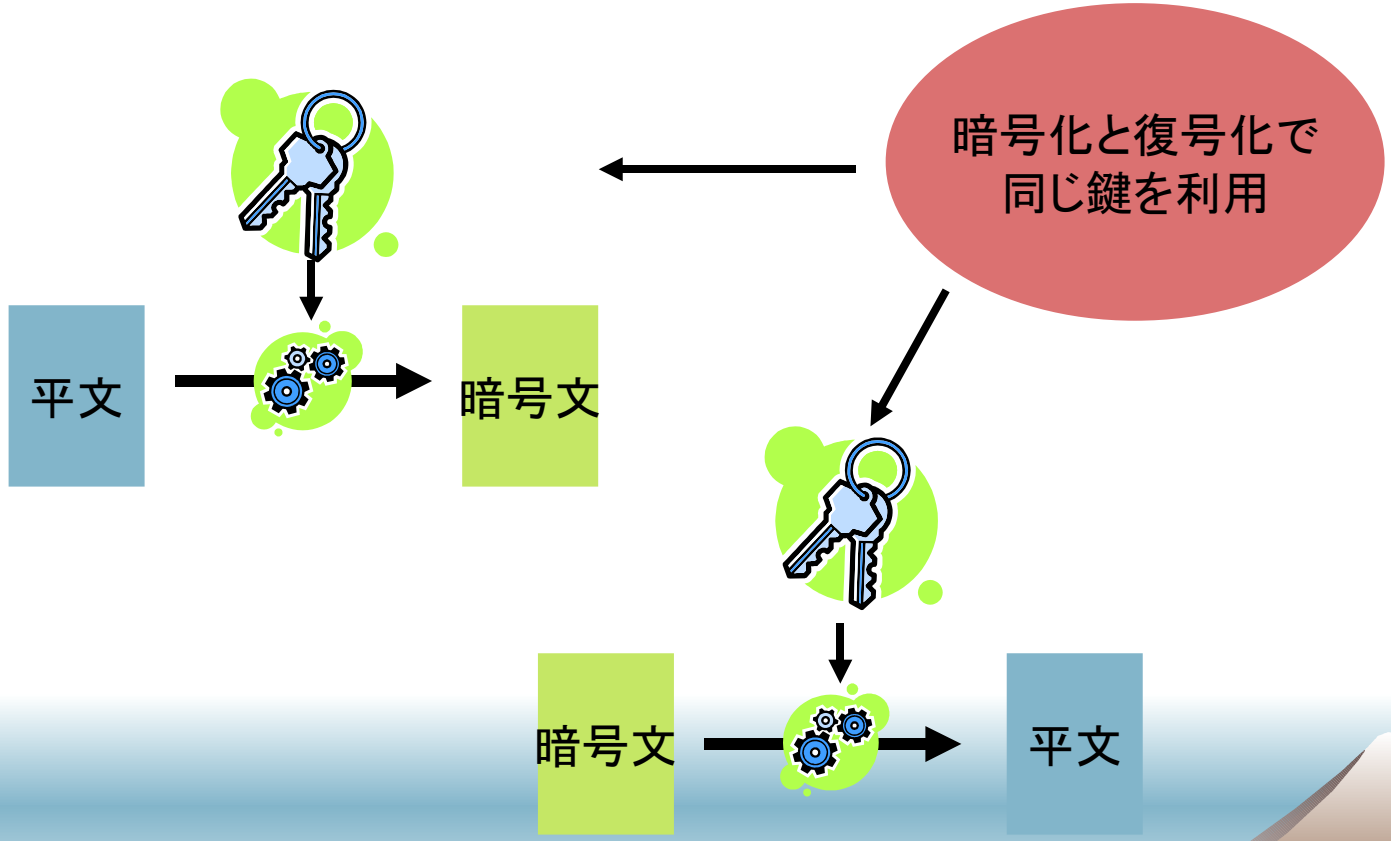
- なぜできるのか？
  - →辞書攻撃：総当りではなく、限られた辞書を選択的に選んで攻撃する
- 強い暗号化（2chの場合はハッシュ）技術を使っても、運用が伴わなければ意味が無い（先ほどの復習）

暗号技術

- 暗号技術の分類
  - 共有鍵暗号（秘密鍵暗号）
  - 公開鍵暗号
- とりあえず今回は気持ちだけ掴んで・・・

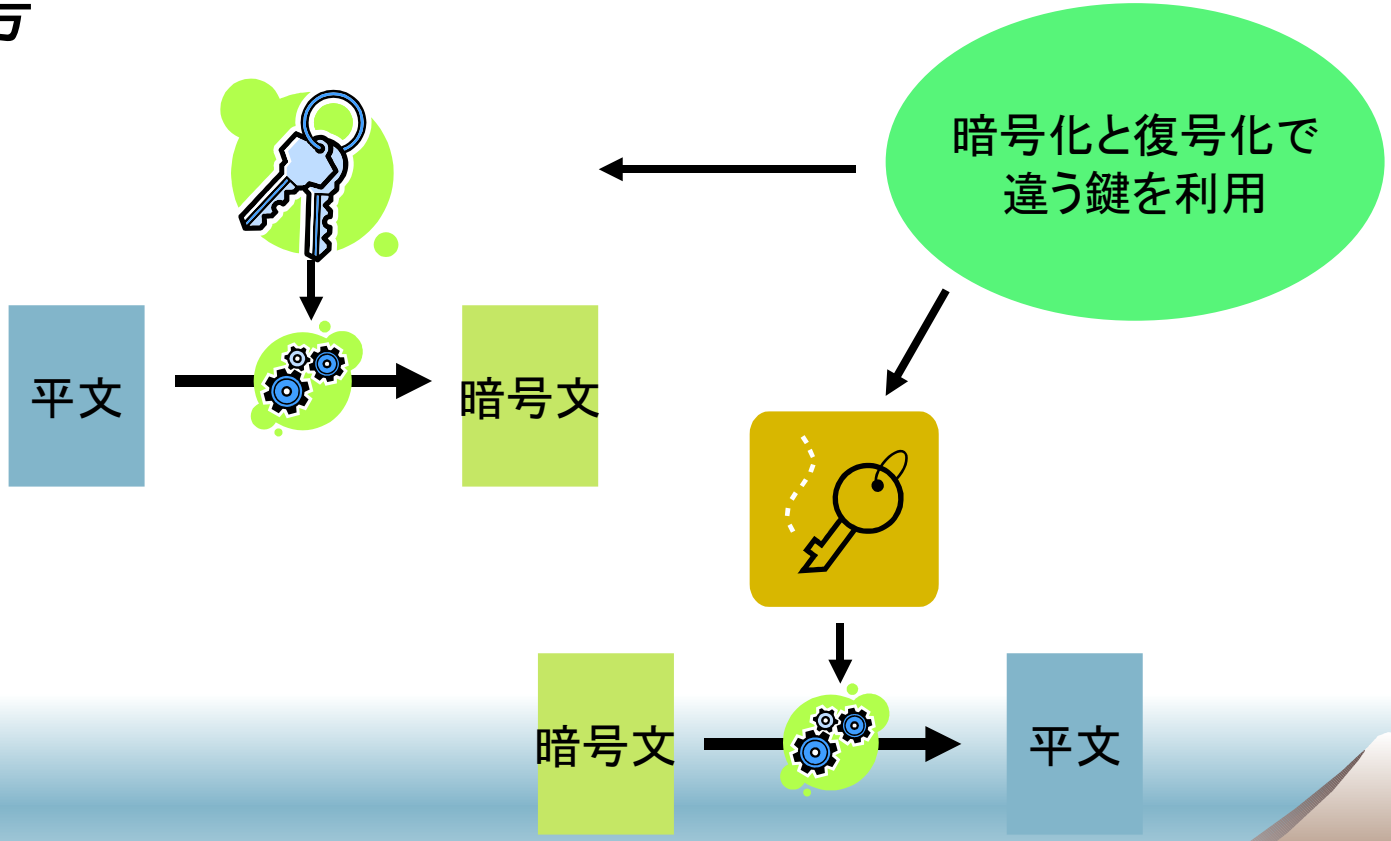
共有鍵暗号

- 一つの鍵で暗号化・復号化する方式



公開鍵暗号

- 公開鍵と秘密鍵でそれぞれ暗号化・復号化する暗号



暗号の種類

- 共有鍵暗号
  - DES, 3DES
    - UNIX の標準暗号、2ch でも使われている
  - AES, IDEA, RC?, etc…
- 公開鍵暗号
  - RSA, DSA
    - PGP/SSLなどに使われている

共有鍵暗号

- 最古の暗号とされる「シーザー暗号」
  - アルファベットを何文字かずらしたもの
  - 復号するときは同じ数だけ戻す
  - 6個ずらしたとして A → G とした場合、この暗号の「鍵」は6という数字になる

共有鍵暗号

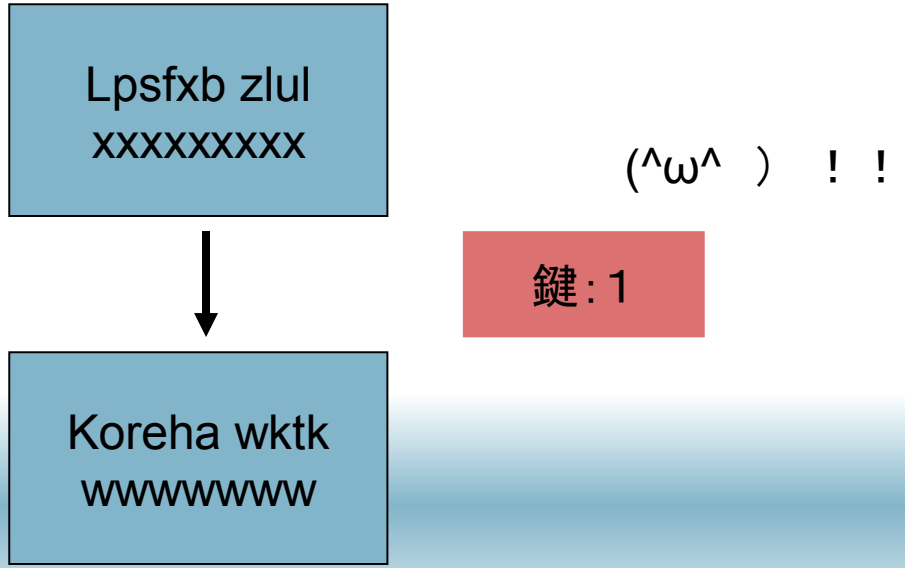
- 暗号をやりとりする双方で前もって鍵を「共有」する必要があるから「共有鍵暗号」
- 暗号文だけ渡されてもわからない
  - シーザー暗号での例

Lpsfxb zlul
xxxxxxxxx

(^ω^;)　！？

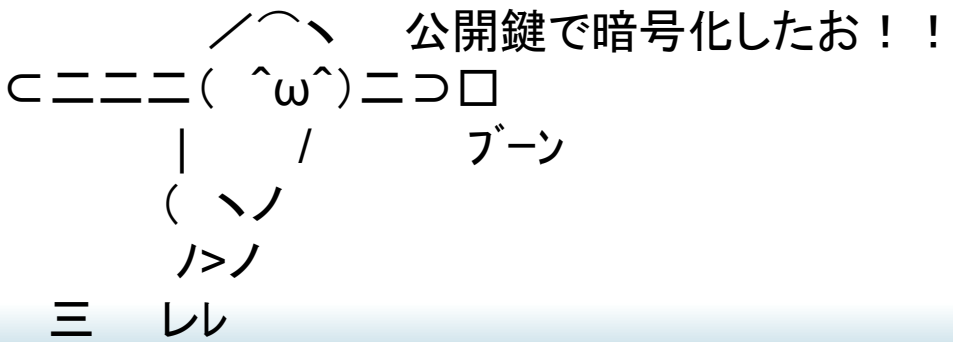
共有鍵暗号

- 暗号をやりとりする双方で前もって鍵を「共有」する必要があるから「共有鍵暗号」
- 暗号文だけ渡されてもわからない
  - シーザー暗号での例



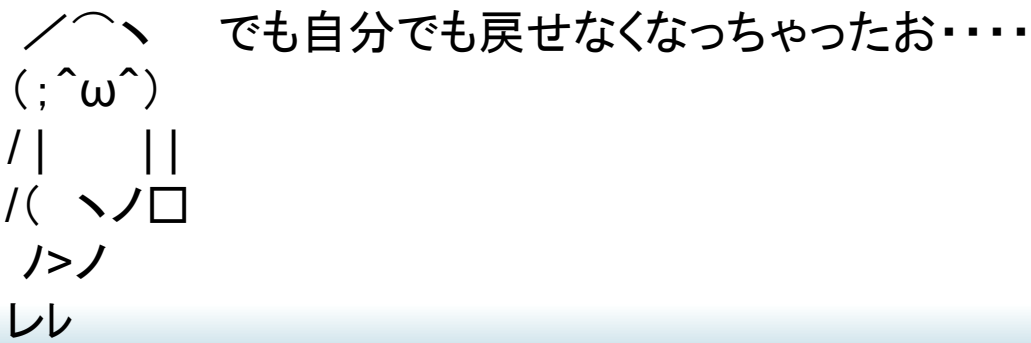
公開鍵暗号

- 公開鍵と秘密鍵で暗号化･復号化する方式
- それぞれの鍵を使って暗号化した文章は、
  その鍵を使っても復号化できない



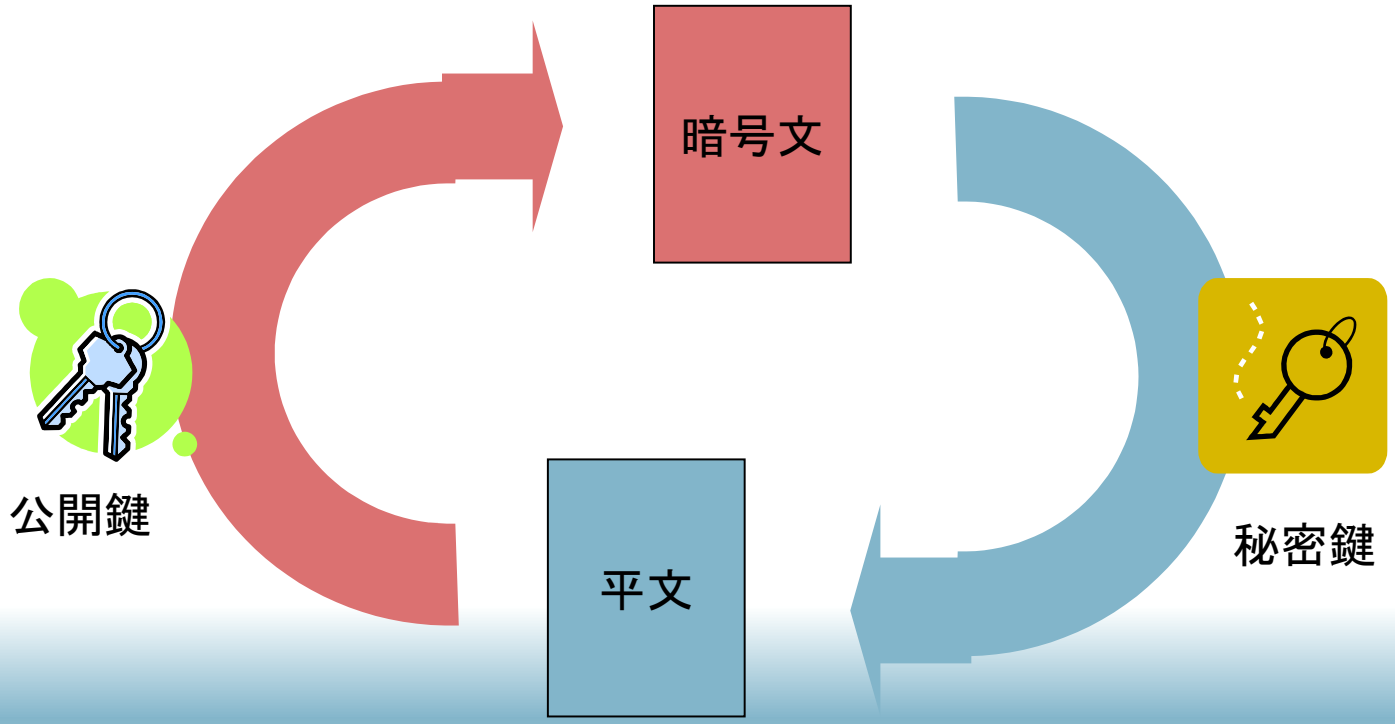
公開鍵暗号

- 公開鍵と秘密鍵で暗号化･復号化する方式
- それぞれの鍵を使って暗号化した文章は、
  その鍵を使っても復号化できない



秘密鍵と公開鍵の関係

- それぞれ一方通行でしか処理できない



暗号技術のまとめ

- 共有鍵暗号方式と公開鍵暗号方式

ハッシュ

- あるデータの塊を固定長のデータにする
- 簡単なハッシュの例
  - それぞれの文字コードを足して行って、結果の下2桁を取る
- 実用のためには、データの中身が少し違うだけで結果が大きく異なることが必要