



暗号入門

情報科学の世界II

只木 進一（工学系研究科）

古代の暗号

旧約聖書：atbash暗号

- ➡ 紀元前5世紀
- ➡ 旧約聖書中の都市名等を秘密に

元の文字	置き換える文字
a	z
b	y
c	x
d	w

- 

Caesarの暗号

- ➡ 紀元前1世紀
- ➡ アルファベットの先頭から鍵の文字列に置き換える
- ➡ 残りは、鍵の終端の後ろに残ったアルファベットを順番に対応させる

鍵 : JULISCAER

abcdefghijklmnopqrstuvwxyz

J u l i s c a e r t v w x y z b d f g h k m n o p q

上杉暗号 16世紀

➡ いろはを数字で表現

	七	六	五	四	三	二	一
一	ゑ	あ	や	ら	よ	ち	い
二	ひ	さ	ま	む	た	り	ろ
三	も	き	け	う	れ	ぬ	は
四	せ	ゆ	ふ	ゐ	そ	る	に
五	す	め	こ	の	つ	を	ほ
六	ん	み	え	お	ね	わ	へ
七		し	て	く	な	か	と

暗号と暗号鍵

➡ 暗号の方式

- ➡ どういう方法で文字を置き換えるのか
- ➡ どういう方法で数字に置き換えるのか

➡ 暗号の鍵

- ➡ 何文字ずらす
- ➡ 何文字置きに読む
- ➡ 数字に置き換える原点

- ➡ 符号化 : Encode, Encipher
 - ➡ 平文テキスト(plain text)を暗号テキスト(cipher text)にする
- ➡ 復号化 : Decode, Decipher
 - ➡ 暗号テキストを平文テキストに戻す

- 鍵を送信者と受信者が共有する方法
 - 共通鍵方式
 - 符号化と復号化で同じ鍵
 - どうやって鍵を送る？
- 送信用鍵と受信用鍵が異なる
 - 公開鍵方式
 - 符号化と復号化が異なる鍵
 - 一方向にしか送れない

公開鍵暗号方式

- ➡ 受信者から送信者へ、符号化用鍵の送信
- ➡ 送信者は送信内容を符号化用鍵で暗号化し、送信
- ➡ 受信者は、自分だけが持つ復号化用鍵で暗号テキストを復号

SSL (Secure Socket Layer)

- ▶ Web 通信で用いる暗号化方式
- ▶ Webの信頼性を示す証明書提示も
- ▶ 重要情報を送る場合には、確認必須

- ▶ クライアントがサーバへ通信要求
- ▶ サーバが証明書と公開鍵を送信
- ▶ クライアントは、共通鍵を生成してサーバから受信した鍵で符号化して送信
- ▶ サーバは共通鍵を受信して復号
- ▶ 双方が共有した鍵で、暗号通信

復号できない暗号

➡ パスワード

- ➡ 符号化できるが、復号できない
- ➡ ユーザが入力したパスワードを符号化し、保存しているものと比較するのみ

➡ 攻撃手法

- ➡ ユーザ名、名前、生年月日などをヒントに
- ➡ 総当たり