暗号の仕組み

情報科学の世界II

2020年度

只木　進一（理工学部）

atbash暗号：旧約聖書

- 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

スパルタの暗号 scytale暗号

- 紀元前5世紀
- 棒に細長い布を巻く
  - 数文字あけて読み解く
  - https://ja.wikipedia.org/wiki/%E3%82%B9%E3%82%AD%E3%83%A5%E3%82%BF%E3%83%AC%E3%83%BC

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

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

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
- 暗号の鍵
  - 何文字ずらす
  - 何文字置きに読む

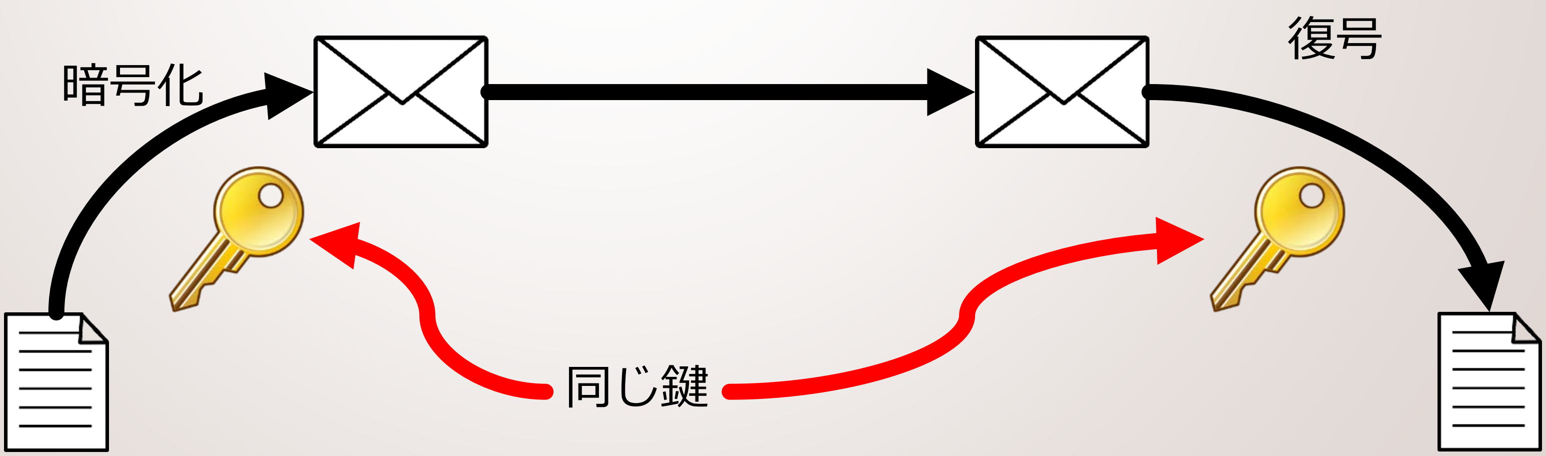
近代以前の暗号の弱点

- 文字の置き換えが固定
- 文字の出現頻度から解読される

- 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

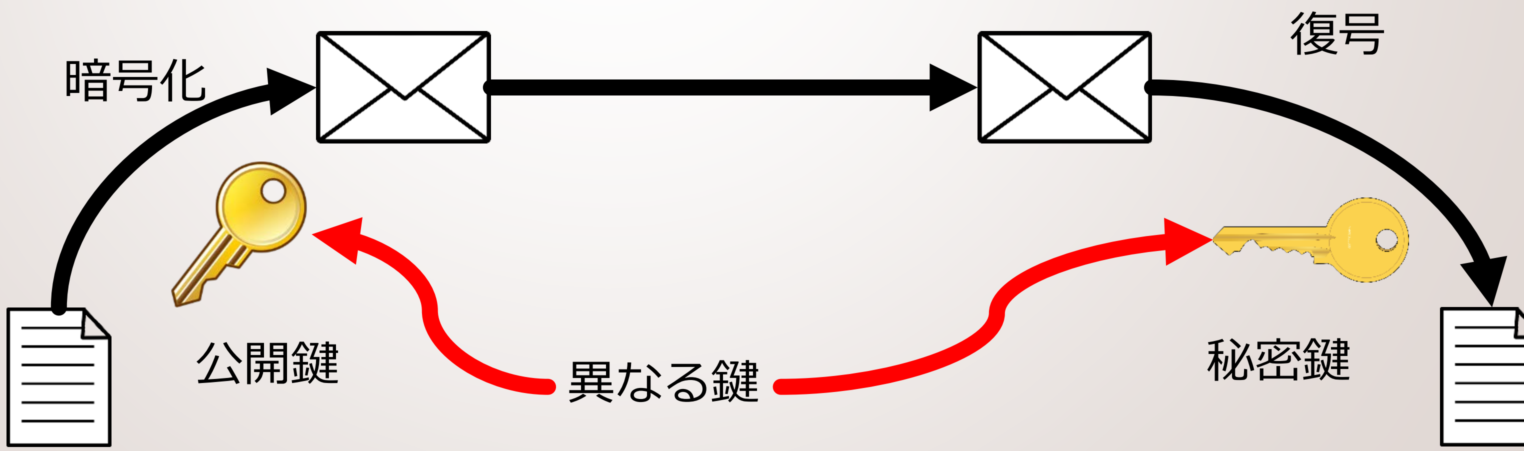
鍵の共有方法：共通鍵方式

- 鍵を送信者と受信者が共有する方法
  - 符号化と復号化で同じ鍵
  - どうやって鍵を送る？



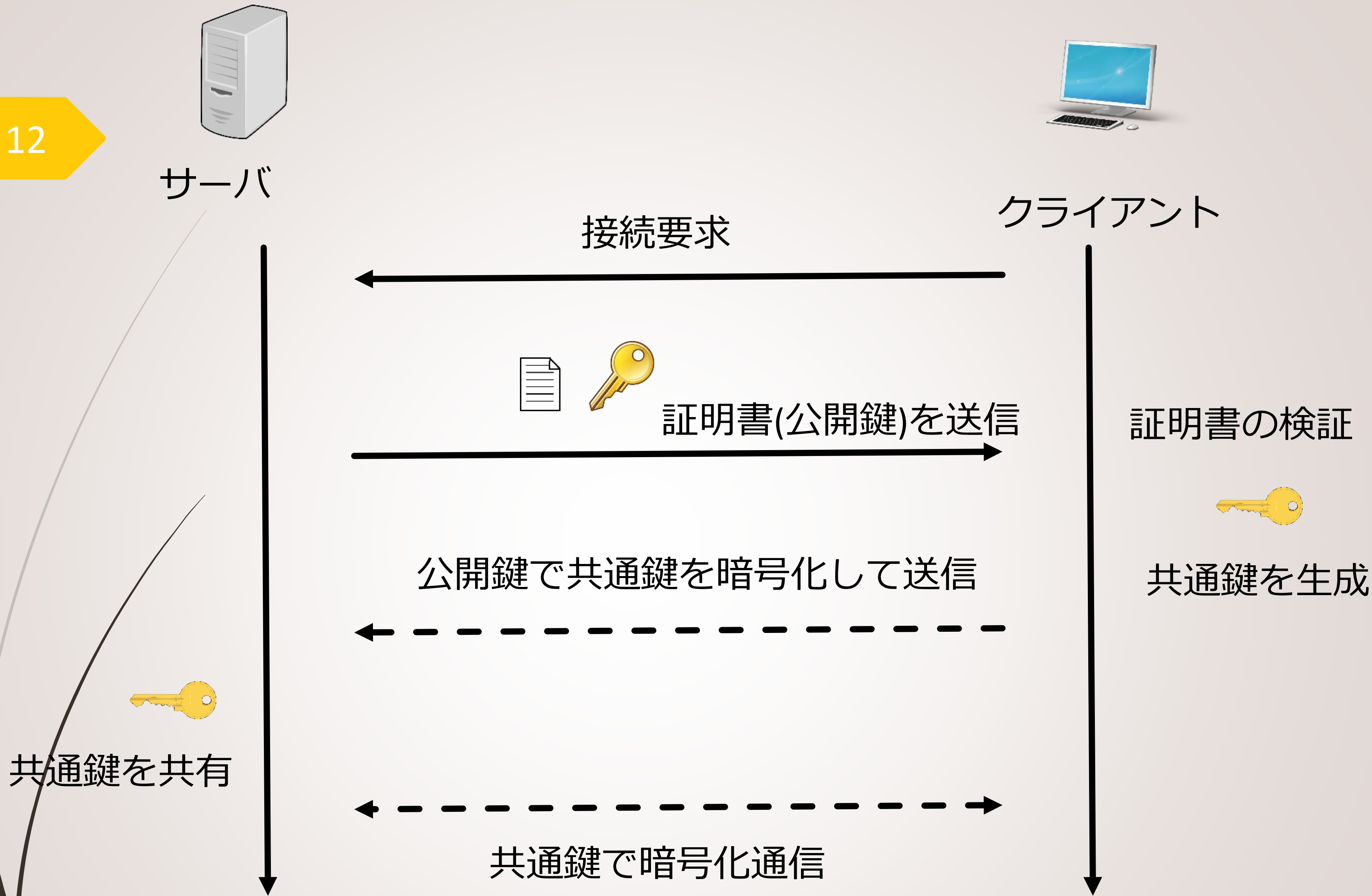
鍵の共有方法：公開鍵方式

- 送信用鍵と受信用鍵が異なる
  - 符号化と復号化が異なる鍵
  - 一方向にしか送れない



SSL (Secure Socket Layer)

- Web 通信で用いる暗号化方式
  - HTTPSプロトコルと呼ぶ
- 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


サーバ
クライアント
接続要求
証明書(公開鍵)を送信
証明書の検証
共通鍵を生成
公開鍵で共通鍵を暗号化して送信
共通鍵を共有
共通鍵で暗号化通信

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

RSA(Riverst-Shamir-Adleman)暗号

- 整数論という数学の応用
- 因数分解が困難であることに基づく
- 公開鍵暗号に利用される
- James H. Ellis (1969)及びClifford Cocks(1973)が理論的基礎を発見したが、長く秘密にされていた
- 1977年にRSAが公表。

整数の合同
Congruence

- 二つの整数aとb。ある整数mで除した余りが等しい
  - aとbは法mについて合同：$a \equiv b \pmod{m}$
- $a \equiv a' \pmod{m}$かつ$b \equiv b' \pmod{m}$ならば
  - $ab \equiv a'b' \pmod{m}$

$$a = n_a m + a'$$

$$b = n_b m + b'$$

$$ab = \left(n_a m + a'\right)\left(n_b m + b'\right) = \left(n_a n_b m + n_a + n_b\right) m + a'b'$$

Fermatの小定理

- pを素数、$a \not\equiv 0 \pmod{p}$
- このとき、$a^{p-1} \equiv 1 \pmod{p}$
- 例示：$p = 11, a = 3$

$$3^2 \equiv 9 \pmod{p}$$

$$3^4 \equiv 81 \pmod{p} \equiv 4 \pmod{p}$$

$$3^8 \equiv 16 \pmod{p} \equiv 5 \pmod{p}$$

$$3^{10} \equiv \left(3^2 \times 3^8\right) \pmod{p} \equiv 45 \pmod{p} \equiv 1 \pmod{p}$$

Fermatの小定理
応用

- pとqを素数、$\gcd(a, pq) = 1$
- このとき、$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$
- 例示：$p = 5, q = 7, a = 11$

$$11^2 \equiv 121 \pmod{35} \equiv 16 \pmod{35}$$

$$11^4 \equiv 256 \pmod{35} \equiv 11 \pmod{35}$$

$$11^8 \equiv 16 \pmod{35}$$

$$11^{16} \equiv 11 \pmod{35}$$

$$11^{4\times 6} \equiv 11^{(16+8)} \pmod{35} \equiv (11\times 16) \pmod{35} \equiv 1 \pmod{35}$$

秘密鍵と公開鍵

- メッセージを受信する者
  - 二つの大きな素数pとqを生成し、秘密鍵とする。
  - $m = pq$
  - $\phi(m)$：mと互いに素である1以上m以下の自然数の数。今は$(p-1)(q-1)$
  - k：$\phi(m)$と互いに素である適当な自然数
- mとkを公開鍵とする

メッセージ暗号化
送信側

- mはLビットであるとする
- メッセージMを$L-1$ビット毎の語に区切る
  - $M = a_0 a_1 \cdots a_n$
- 各語を変換
  - $b_i = a_i^k \pmod{m}$
  - $M' = b_0 b_1 \cdots b_n$
- M'を送信

復号

- $kv - \phi(m)u = 1$の適当な解(u, v)を得る

$$
\begin{aligned}
b_i^{\,v} &\equiv a_i^{\,kv} \pmod{m} \equiv a_i^{\,1+\phi(m)u} \pmod{m} \\
&\equiv \left(a_i \pmod{m}\right)\left(a_i^{\phi(m)} \pmod{m}\right)^u \\
&\equiv \left(a_i \pmod{m}\right)\left(1 \pmod{m}\right)^u \\
&\equiv a_i \pmod{m}
\end{aligned}
$$

数学的裏付けのある暗号

- 確実に符号化・復号化ができる
  - 数学的に保証されている
- 方式は公開／鍵は非公開
- 素数への因数分解が困難
  - 今のところ有効なアルゴリズムなし
- コンピュータの高速化によって、長い鍵が必要になっている