情報セキュリティ技術: 暗号の基礎

情報社会とセキュリティ
2024 年度前期
佐賀大学理工学部 只木進一

暗号とは

- 文書の内容を秘密にするために、古代より発生
- 文字を置き換える方法
  - 旧約聖書中で都市名を暗号化: atbash 暗号
  - Caesar 暗号
  - https://ja.wikipedia.org/wiki/%E3%82%B7%E3%83%BC%E3%82%B6%E3%83%BC%E6%9A%97%E5%8F%B7
- 文字を読む位置を変更
  - scytale 暗号
  - https://ja.wikipedia.org/wiki/%E3%82%B9%E3%82%AD%E3%83%A5%E3%82%BF%E3%83%AC%E3%83%BC
- 日本にも: 上杉暗号
  - 正確には暗号化ではなく符号化
  - https://www.hummingheads.co.jp/reports/series/ser01/110519.html

暗号の要素

- 暗号の方式
- 暗号の鍵
    - Caeser 暗号ならば、最初に埋め込む文字列
    - scytale 暗号ならば、何文字毎に読むか

近代以前の暗号の弱点

- 文字の置き換えが固定的
  - 文字の出現頻度等から解読される
- 鍵の共有方法に課題
  - 遠方に鍵を送るには?

質問

メールでパスワード付き ZIP ファイルを送り、次のメールでパスワードを送る方式が批判されています。PPAP とも言われています。何が問題なのでしょう。

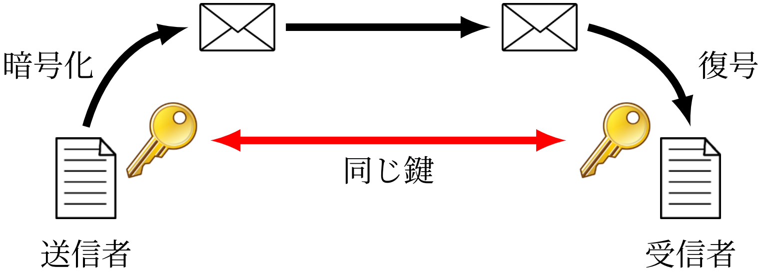
インターネット時代の暗号: 基本的用語

- 符号化: Encode, Encipher, Encrypt
  - 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, Decrypt
  - 暗号テキストを平文テキストに戻す

cipher /'saɪfə(r)/ a secret way of writing, especially one in which a set of letters or symbols is used to represent others.

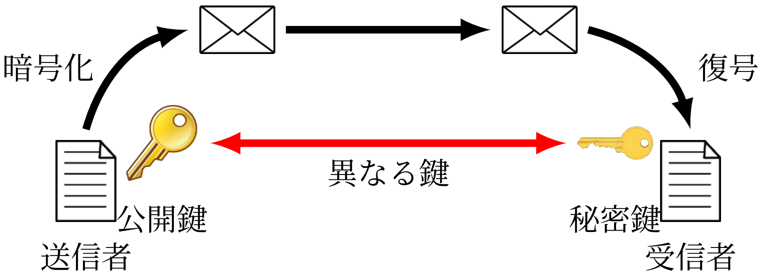
鍵の共有方法: 共通鍵方式/共有鍵方式: Common key cryptosystems

- 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
  - 双方向通信が可能
  - どうやって鍵を送る？



鍵の共有方法: 公開鍵方式: public key cryptosystems

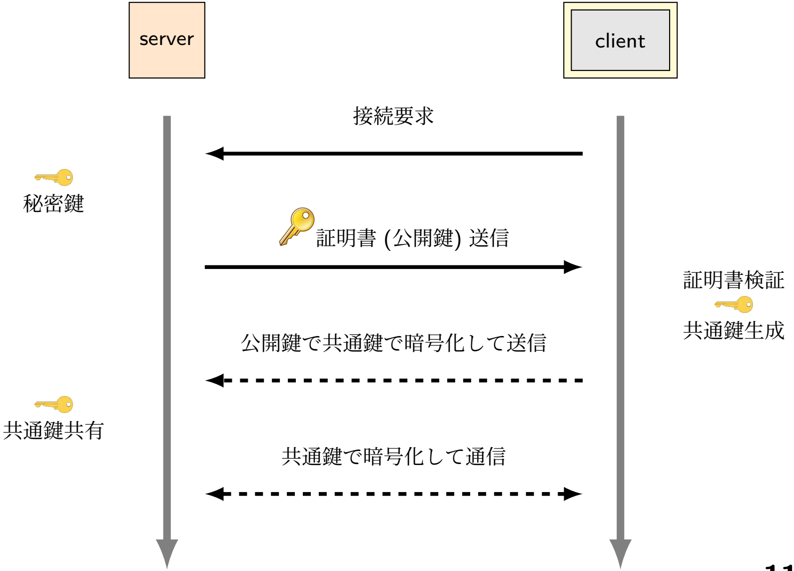
- 送信者と受信者が異なる鍵を使用する方法
  - 符号化と復号化が異なる鍵
  - 暗号文は一方向にしか送れない
  - 公開鍵は公開



SSL: Secure Socket Layer

- HTTPS で利用している暗号化方式
  - 現在は TSL (Transport Layer Security) を使用
- 公開鍵と共通鍵を併用
- Web の証明書提示

HTTPS の接続手順

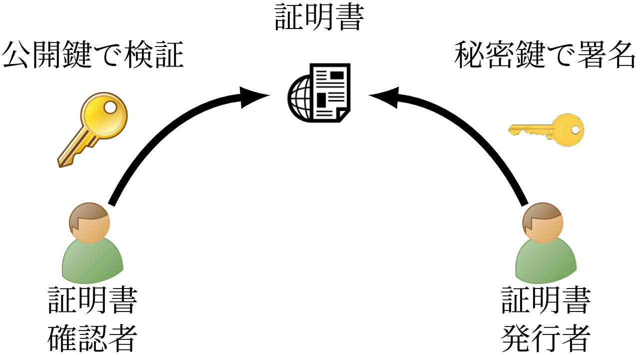

server
client
接続要求
秘密鍵
証明書 (公開鍵) 送信
証明書検証
共通鍵生成
公開鍵で共通鍵で暗号化して送信
共通鍵共有
共通鍵で暗号化して通信

SSL 証明書に記載されていること

- Web ホスト名
  - ブラウザは、URL と証明書内のホスト名を照合
- 証明書の発行元
  - ブラウザは、信用できる発行元かを照合
- 有効期限

公開鍵と電子証明書

- 証明書発行者が秘密鍵で署名
- 証明書受信者が公開鍵で証明書を検証



デジタル証明書の用途

- Web サーバの証明
- クライアント証明書
    - サーバへ接続しているクライアントの証明
    - 特に重要な情報を扱うサーバへの接続
- 電子メールの署名と暗号化

復号できない暗号: パスワード

- ユーザが入力したものを符号化し、保存しているものと比較
- 攻撃手法
  - ユーザ名、名前、生年月日、英単語などをヒントに
  - 総当たり

質問

4 桁の数字しかパスワードとして許さないサービスが沢山ありました。なぜ、4 桁の数字のパスワードは危険なのでしょうか。

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: $a \equiv b \pmod{m}$
- 例: $m = 5$

$$
\begin{aligned}
7 &\equiv 2 \pmod{5} \\
10 &\equiv 0 \pmod{5} \\
9 &\equiv 4 \pmod{5} \\
11 &\equiv 1 \pmod{5} \\
3 &\equiv 3 \pmod{5}
\end{aligned}
$$

整数の合同: Congruence

- $a \equiv a' \pmod{m}$ かつ $b \equiv b' \pmod{m}$ ならば $ab \equiv a'b' \pmod{m}$

$$\begin{aligned} a &= n_a m + a' \\ b &= n_b m + b' \\ ab &= (n_a m + a')(n_b m + b') \\ &= (n_a n_b m + n_a b' + n_b a') m + a'b' \end{aligned}$$

- 例: $m = 7$

$$\begin{aligned} 8 &\equiv 1 \pmod{7} \\ 10 &\equiv 3 \pmod{7} \\ 8 \times 10 = 80 &= 7 \times 11 + 3 \\ &\equiv 3 \pmod{7} \end{aligned}$$

Fermat の小定理

- p を素数、a を p と互いに素とする:$a \not\equiv 0 \pmod{p}$
- このとき:$a^{p-1} \equiv 1 \pmod{p}$
- 例:$p = 11$、$a = 3$

$$
\begin{aligned}
3^2 &\equiv 9 \pmod{p} \\
3^4 &\equiv 81 \pmod{p} \equiv 4 \pmod{p} \\
3^8 &\equiv 16 \pmod{p} \equiv 5 \pmod{p} \\
3^{10} &\equiv \left(3^2 \times 3^8\right) \pmod{p} \equiv 45 \pmod{p} \\
&\equiv 1 \pmod{p}
\end{aligned}
$$

- mod p のみに注目し、演算を簡素化

Fermat の小定理: 証明準備: 参考

- p を素数、$a \in N$ とすると $a^p \equiv a \pmod{p}$ が成り立つ
- $(a+1)^p \equiv a^p + 1 \pmod{p}$

$$(a+1)^p \equiv a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k + 1 \pmod{p} \equiv a^p + 1 (\mathrm{mod}\ p)$$

- $a = 1$

$$(1+1)^p \equiv 1^p + 1 \pmod{p} \equiv 2 \pmod{p}$$

- $(a+1)^p \equiv a + 1 \pmod{p}$ を仮定

$$(a+1+1)^p \equiv (a+1)^p + 1 \pmod{p} \equiv a + 2 \pmod{p}$$

Fermat の小定理: 証明: 参考

- $a^p \equiv a \pmod{p}$ を使う
- a は p と互いに素な自然数とする

$$a^p - a \equiv 0 \pmod{p} \equiv a(a^{p-1} - 1) \pmod{p}$$

- a は p と互いに素であることから

$$a^{p-1} - 1 \equiv 0 \pmod{p}$$

Fermat の小定理: 応用

- p と q を素数、a を pq と互いに素とする
- このとき:$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$ (Euler の定理)
- 例: $p = 5$、$q = 7$、$a = 11$

$$
\begin{aligned}
11^2 &\equiv 121 \pmod{35} \equiv 16 \pmod{35} \\
11^4 &\equiv 256 \pmod{35} \equiv 11 \pmod{35} \\
11^8 &\equiv 16 \pmod{35} \\
11^{16} &\equiv 256 \pmod{35} \equiv 11 \pmod{35} \\
11^{4\times 6} &= 11^{16+8} \equiv \ (11 \times 16) \ \pmod{15} \\
&\equiv 1 \pmod{35}
\end{aligned}
$$

秘密鍵と公開鍵

- 受信者
  - 二つの大きな素数 p と q を生成し、秘密鍵とする。
  - $m = pq$
  - $\varphi(m)$: m と互いに素である 1 以上 m 以下の自然数。ここでは、$\varphi(m) = (p-1)(q-1)$
  - k: $\varphi(m)$ と互いに素である適当な自然数
- m と k を公開鍵とする

送信者によるメッセージ暗号化

- m は L ビットであるとする
- メッセージ M は、$L-1$ ビットよりも短い語に区切る

$$M = a_0 a_1 \cdots a_n$$

- 各語を変換

$$b_i \equiv a_i^k \pmod{m}$$
$$M' = b_0 b_1 \cdots b_n$$

- M' を送信

受信者による復号

- $kv - \phi(m)u = 1$ の適当な解 (u, v) を得る

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

- 復号完了

例

- 秘密鍵: $p = 13,\ q = 11,\ \varphi(m) = 120$
- 公開鍵: $m = 143,\ k = 7$
- m は 8 ビット
  - 7 ビット毎の語に分離
- $kv - \varphi(m)u = 1$ の解 $(u, v) = (6, 103)$

逆方向の符号化

- 秘密鍵を使って符号化

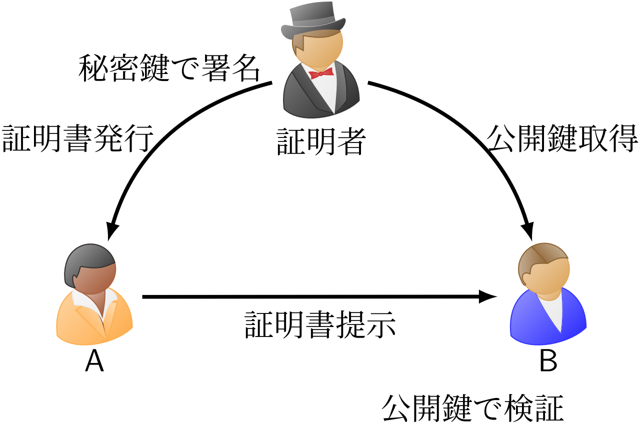
$$b_i \equiv a_i^v \pmod{m}$$

- 公開鍵を使って復号

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

- 公開鍵で復号できるため、暗号にはならない!

デジタル証明書



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
  - 今のところ有効な高速アルゴリズムなし
- 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

課題

佐賀大学総合情報基盤センターのホームページは、HTTPS で暗号化している。つまり、サーバ証明書を持っている。サーバ証明書を確認しなさい。