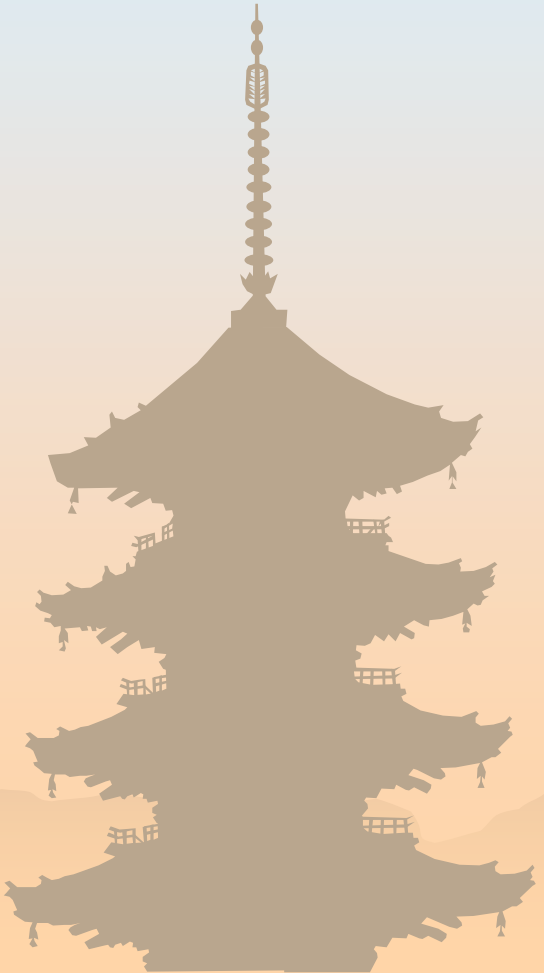
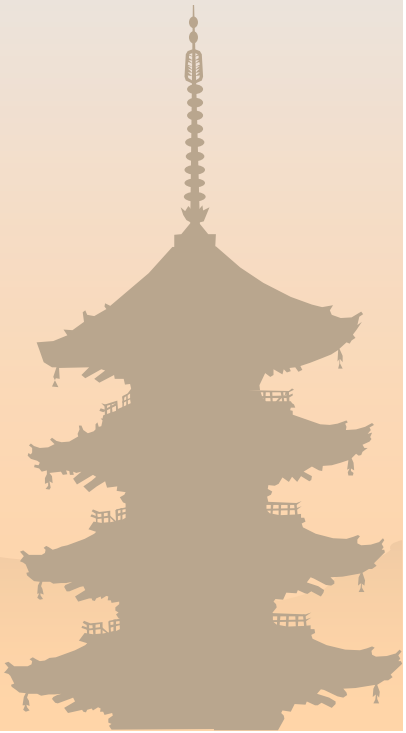
情報処理システム論 (18)



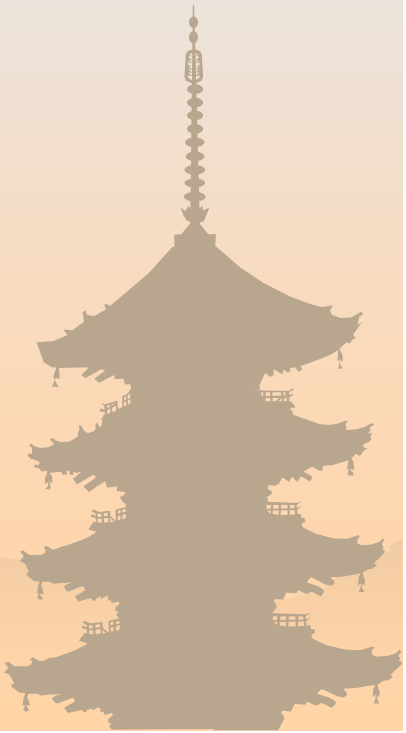
暗号方式

- 共有鍵方式
- 公開鍵方式
  - 公開鍵
  - 秘密鍵



暗号化と署名

- 暗号化
  - 公開鍵でひねって、秘密鍵で戻す
    - 秘密鍵を持っている人しか解読できない
    - だれでも暗号化することができる
- 署名
  - 秘密鍵でひねって、公開鍵で戻す
    - 秘密鍵を持っている人しか署名できない
    - だれでも確認できる

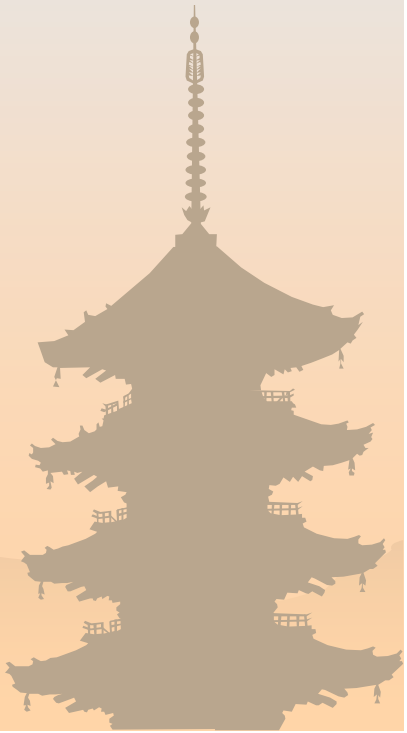


署名の際の考慮点

- 復号化できない人でも読める方がいい
  - 文書はそのまま送る
- そのまま送るとなると
  - 符号化してない文書の確認をする方法が必要
  - 符号化したものとしてないものを一緒に送るのは無駄
- 文書の特徴を抽出する方法を使う

文書の特徴抽出

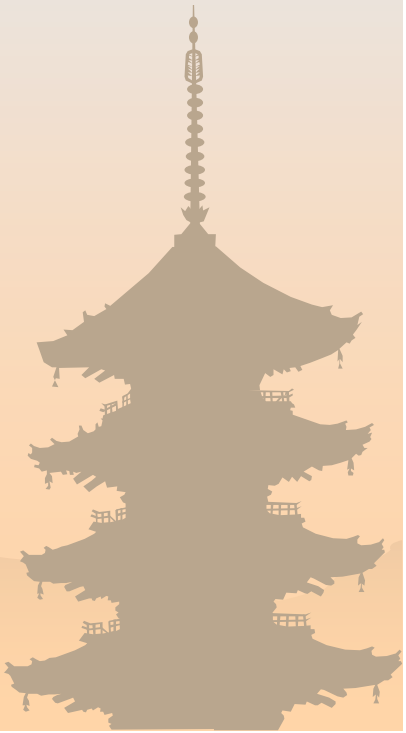
- 簡単に考えると、
  - 文書のチェックサムを計算し、
  - 署名符号化して送り、
  - 符号化して、
  - 一致検査
- チェックサムだと偽造が簡単
- 偽造の難しい計算方法
  - 一方向関数、落とし戸関数
    - MD2, MD4, MD5 (Message Digest) など



そのまま読める署名された文書

- 文書の特徴抽出
- 特徴データを署名符号化
- 相手に送る

- 文書の特徴抽出
- 送られてきた特徴データを復号化
- 特徴データを比較

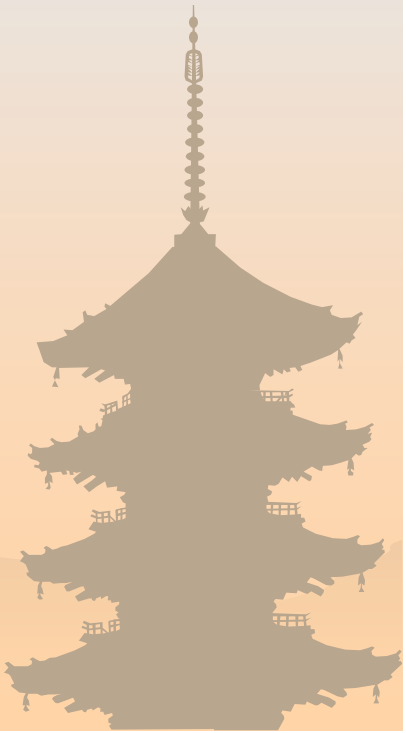


暗号化の際の考慮点

- 複数の人に暗号化された文書を送るには

- 暗号化は相手の公開鍵でひねる
- 文書を複数の公開鍵でひねったら、
  - だれも読めない

- どうしよう…



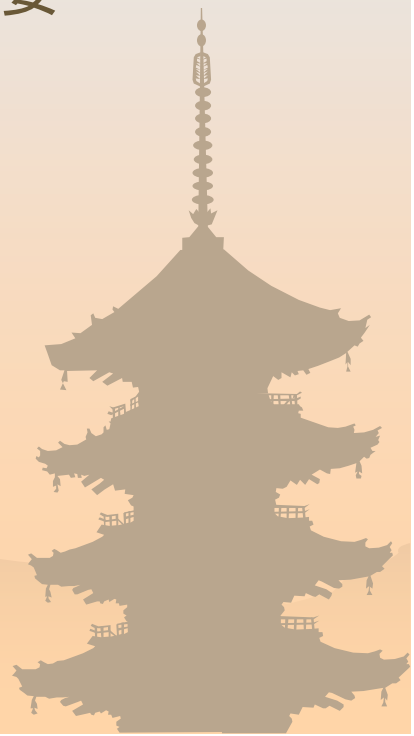
共有鍵を併用した暗号化

- 適当な共有鍵を生成
- 文書を共有鍵で暗号化
- 用いた共有鍵を送り先の公開鍵で暗号化
- 送り先の数だけ列挙する

- 受信者は自分の公開鍵で暗号化された共有鍵を取り出す
- 文書を共有鍵で復号化

グループへの暗号化の問題点

- グループのメンバ管理
  - メンバが個々にする？
    - すべてのメンバが全員の公開鍵を持つ必要
    - 個人ごとに暗号化情報をつける
  - まとめて一個所で管理？
    - グループに対する公開鍵1つをもつ
    - 暗号化情報は一つだけ

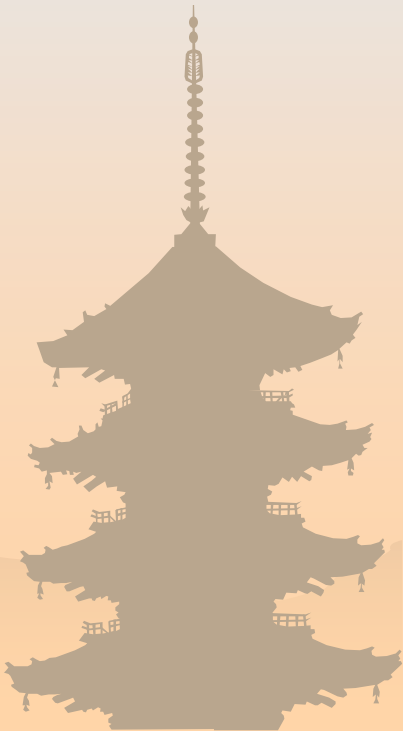


メンバの変更との親和性

- メンバの出入りの管理を個々にするのは面倒
- メンバでなくなったら読めなくしたい
- メンバになったら古い文書も読みたい？
- メンバがぬけたら鍵を変更するのも面倒
  - 理想的な解決法はない？

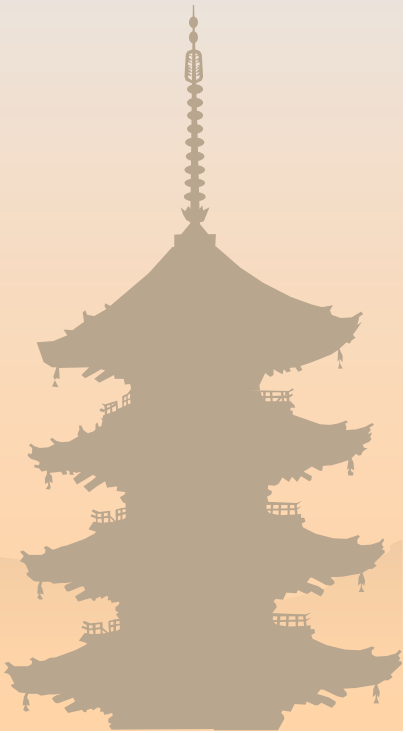
公開鍵方式のインターネットでの利用

- PGP (Pretty Good Privacy)
- SSL (Secure Socket Layer) 技術
  - Netscape Navigator / Internet Explorer
  - たとえば Netscape だと
    - SSL を用いたページで鍵の絵がつながる



SSL 技術の利用

- サーバ側の鍵は必ず存在
  - サーバからの情報の正当性
  - ユーザからの情報の暗号化
- ユーザ側の鍵は任意
  - ユーザの認証
  - サーバからの情報の暗号化



鍵をどうやって用意するのか

- 鍵を提供する組織から入手する
- 自分で勝手に作る
  - PGP 方式

- 鍵の信頼性の問題
  - 第3者が勝手に公開鍵を配布していないか
    - なりすまし
  - どうやって公開鍵の信頼性を高めるか
    - 公開鍵に署名をする

公開鍵の認証

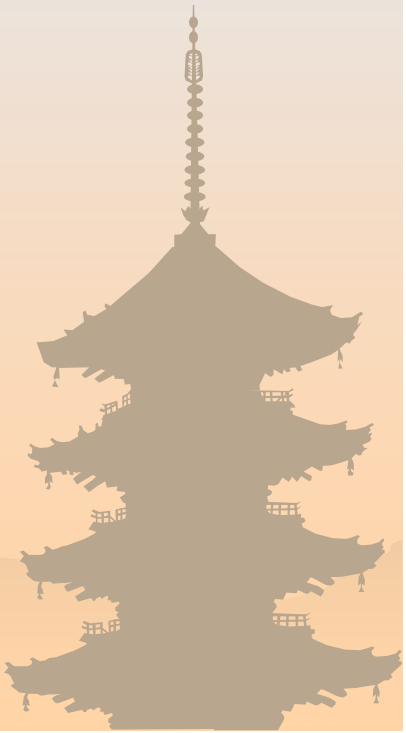
- 公開鍵にどのような署名をするか
  - 自分の秘密鍵で署名
    - 改竄の防止
  - 多くの友人に署名してもらう
    - PGP 方式
    - 友人が信頼できれば、友人の友人も信頼する
  - 証明機関(公証局)に署名してもらう
    - 権限を持った証明機関(鍵の発行機間)を利用
      - Navigator で
        - » オプション→ セキュリティ → サイト証明書

鍵の発行機関

基本的に有料

- VeriSign
- Cyber Trust
- BBN Certificate Service
- US Postal Service

など…



まとめ

- 公開鍵方式といってもいろいろ
  - 一組の鍵でなんでもできるわけではない
- 発行機関から鍵を入手するにはお金がいる
- 発行機関はどれくらい信用できるのか
- 秘密鍵の管理問題
  - PC が憶えている
  - 席を立っている間のいたずら