情報セキュリティと暗号・認証

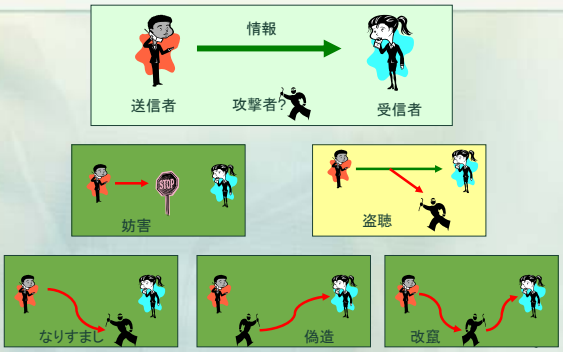
情報の安全性

- 古典的な**情報の安全性**
  - 物理的な保護手段
    （例）機密性の高い文書は鍵のかかる金庫で保管する
  - 管理的な保護手段
    （例）重要な情報の担当者については、採用時の審査を厳しくする
- **コンピュータセキュリティ**
  - ハードウェアの保護
  - ソフトウェアの保護
  - 操作する人間のミスからの保護
- **ネットワークセキュリティ**
  - コンピュータを、ネットワークを介した攻撃から守る
  - ネットワーク上でやりとりされる情報を保護する

情報セキュリティとは

- 情報セキュリティ
  - 情報資産の**機密性、完全性、可用性**の維持
- 情報資産
  - 情報の内容
  - 情報の作成・利用・管理のための仕組み
    - ハード、ソフト、ネットワーク、記録媒体
- **機密性**(confidentiality)
  - 情報の内容が、それにアクセスする権限のある者にしか読めないことを保証すること
- **完全性**(integrity)
  - 情報およびその処理方法が正確かつ完全であることを保証すること
- **可用性**(availability)
  - 情報およびその処理のための仕組みが、必要なときにアクセスできるようになっていることを確実にすること

ネットワークセキュリティの侵害



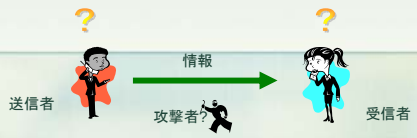
能動的な攻撃と受動的な攻撃

- 能動的な攻撃
  - 妨害(interruption)
    - サービス不能攻撃 (denial of service; DoS)
  - なりすまし(masquerade)
  - 偽造(fabrication)
    - 再生攻撃(replay)
  - 改竄(modification)
- 受動的な攻撃
  - 通信を盗聴または監視する
    - 通信の内容の取得
    - 通信の相手方、通信の事実を観測
  - 発見は困難

正当性(authentication)
•送信者・受信者が、その通信において送信者・受信者となる確かな権限を持つことを保証すること。

秘匿性(concealment)
•通信した事実を、通信の当事者以外には知られないことを保証すること。

否認



- 送信者が送信の事実を否認
  - 送信者のウソ
  - 受信者のウソ
  - 攻撃者による偽造
- 受信者が受信の事実を否認
  - 送信者のウソ
  - 受信者のウソ
  - 攻撃者によるなりすまし

相手がウソをついていることを確信したとしても、そのことを第三者に証明できなければ無意味

- 送信者と受信者で、伝送された情報の内容に食い違い
  - 送信者がウソ
  - 受信者がウソ　} 両方がウソ
  - 攻撃者による改竄

否認不能性(nonrepudiation)
•送信者または受信者が伝送された情報の授受を否定することを防止できること。情報が伝送されたとき、受信者は確かにその送信者から送られたことを証明することができ、逆に送信者はその情報を受信者が受け取ったことを証明できる

個人認証

- 情報にアクセスしようとする者が、アクセス権限を有する**本人**であることを検証する
  - なりすましの防止
  - 否認の防止
- 認証の方法
  - 本人が持つ知識を利用
  - 本人が持つ物を利用
  - 本人の身体的特徴を利用

  これらを組み合わせて利用

7

個人認証の方法(1)「本人の知識」を利用

- 本人なら知っている知識
  - 生年月日、両親の氏名、…
    - 他の人でも知りうる
- 本人**だけ**が知っている知識
  - 暗証番号 (PIN; Personal Identification Number)

  （問題点）サービスごとの暗証番号は覚えきれない
    - 全部同じ暗証番号にする？
    - 手帳に書いておく？

シングルサインオン(single sign on)

•利用者が、1回のログイン手続きで、認証を必要とする複数のサービスを利用できるようにする仕組み

8

個人認証の方法(2)「本人が持つ物」を利用

- 本人だけが持つ物
  - 鍵、印鑑、身分証明書
  - 磁気カード、ICカード、USBキー
    - **電子証明書**（後述）

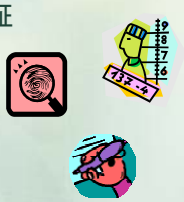
（課題）
  - 紛失、盗難、破損のリスクに対して脆弱
    - PINの併用
  - 複製を困難にするのは高コスト
    - HSM (Hardware Security Module) に電子証明書を格納

9

個人認証の方法(3)「本人の身体的特徴」を利用

- バイオメトリクス(biometrics)認証
  - 顔、声
  - 指紋、虹彩、静脈…
  - 手書き署名、筆跡

（課題）
  - 誤認識率が高い
  - 身体や体調の変化で認識されなくなることがある
  - 利用者に心理的抵抗感
    - 情報が漏れても変えられない



10

暗号 — 盗聴の防止

- 情報を隠すには？
  - **暗号化**して、外部の人には解読できないものにする
  - 偽装によりメッセージの存在そのものを隠す

    いろはにほへ**と** ちりぬるをわ**か** よたれそつね**な**
    らむうゐのお**く** やまけふこえ**て** あさきゆめみ**し**
    ゑひもせ**す**

    答なくて死す？

    ⇒透かし(steganography)
- **古典的暗号**
  - 暗号化アルゴリズムを秘密にする
- **近代暗号**
  - 暗号化アルゴリズムそのものは公開し、鍵を秘密にする

11

暗号化アルゴリズムの基礎

- 換字　　鍵：平文と暗号文の文字表の対応関係

  （例）シーザー暗号 … 英アルファベットで3文字ずらす

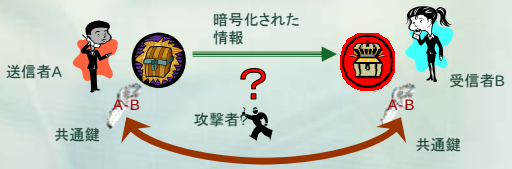
  平文:　we love kyoto university
  暗号文:　ZH ORYH NBRWR XQLYHUVLWB
- 転置　　鍵：平文と暗号文の文字表の対応関係

  （例）暗号文: 13-3-2-21-1-1-8-5
  O DRACONIAN DEVIL!
  OH LAME SAINT!

  平文:
  1-1-2-3-5-8-13-21
  LEONARD DA VINCI!
  THE MONA LISA!

共通鍵暗号系

・共通鍵暗号系(symmetric cryptography)
- データの暗号化と復号に同じ鍵を使う暗号化方式



・送信者と受信者が事前に鍵を安全に共有しておく必要がある
- 送信者と受信者の組み合わせ${}_nC_2=N(N-1)/2$ だけ鍵が必要

13

共通鍵暗号系の例

- DES (Data Encryption Standard)
  - 1977年、米国NBS (National Bureau of Standards)により標準化(2001年まで)。
  - 暗号化アルゴリズムは換字と転置の繰り返し。
    - 56bit の共通鍵
  - 全数検索により時間をかければ解読可能
- 3DES (Triple DES)
  - DESを3回繰り返すことで強化
- AES (Advanced Encryption Standard)
  - 2001年、米政府暗号化標準として採用

14

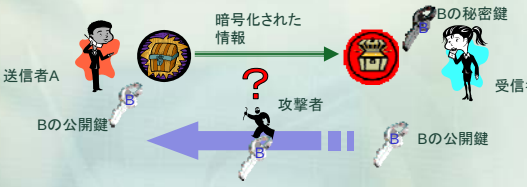
共通鍵事前共有の方法

- 物理的に共有
  - 直接手渡し
- Diffie-Hellman鍵交換法
  - 見知らぬ相手と、動的に生成した共通鍵を安全に共有する方法
    - 後述の公開鍵暗号系のバリエーション
- 公開鍵暗号系を用いた共通鍵配送
  - PKI(公開鍵認証基盤)による相手の認証
  - 共通鍵の配送にのみ公開鍵暗号系を使い、データの伝送は比較的計算負荷の軽い共通鍵暗号系で行う。

15

公開鍵暗号系

- 公開鍵暗号系(public key cryptography)
  - データの暗号化と復号に異なる鍵を使用する暗号化方式
  - 公開鍵で暗号化したデータは、対応する秘密鍵を用いてのみ復号可

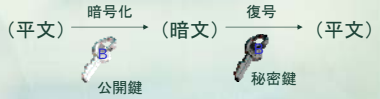


- 受信者Bは、自分の**公開鍵**と**秘密鍵**のペアを生成、
公開鍵のみを**安全な方法**で送信者に配布

16

公開鍵暗号系の暗号強度

- 公開鍵から秘密鍵が推測されることはないか？



公開鍵と秘密鍵は逆関数の関係
順方向の計算は容易だが逆方向の計算が難しい関数を鍵として用いる

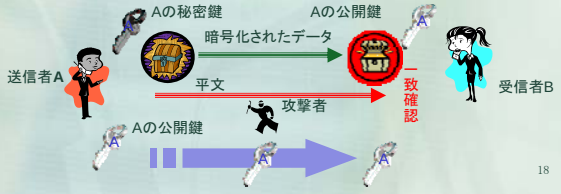
- 公開鍵暗号系の例
  - RSA暗号
    - 大きな2素数の積の素因数分解の困難さ
  - ElGamal暗号
    - 有限体上の離散対数問題の困難さ

計算量理論的安全性

17

公開鍵暗号系を用いた電子署名
— 偽造と否認の防止

- 公開鍵と秘密鍵の対称性
  - RSA暗号系などでは「秘密鍵で暗号化したデータは公開鍵で復号できる」という性質が成り立つ。
- 電子署名の原理
  - 送信者Aは、伝送したいデータに加え、それを自分の秘密鍵で暗号化したものを添付して送る。
  - 受信者Aは、添付の暗文をAの公開鍵で復号、それがデータに一致すれば、確かにAが送信したことが確認できる。
  - 実際にはデータそのものではなく**要約(digest)**したものを暗号化して添付



18

暗号鍵を用いた認証

- **共通鍵**を用いた認証
  - 鍵そのものを相手に送る
    - 盗聴のリスク
    - なりすましのリスク
  - One Time Password
    - 毎回違う鍵を使う

CRAM (Challenge-Response Authentication Mechanism)

0. AとBが鍵Kを共有
1. AはBにchallenge Cを提示
2. Bは d(C,K) を計算してAに返送
   - d は一方向関数
3. Aはd(C,K)の値を確認

逆を行えば相互認証も可能

- **公開鍵**を用いた認証

0. AはBの公開鍵を持っている
1. Bは、認証要求を自分の秘密鍵で署名してAに提示
2. Aは、Bの公開鍵で署名を確認

19

公開鍵配布の問題

偽の公開鍵を配布されてしまうと**なりすまし**が可能

- 受信者Bの公開鍵が攻撃者B'の公開鍵にすり替えられると？
  - 送信者AはB'で暗号化して送ってしまう。それはBでは復号できず攻撃者だけが読めてしまう
- 送信者Aの公開鍵が攻撃者A'の公開鍵に摩り替えられると？
  - 攻撃者は秘密鍵A'を使った署名つき文書を作成、受信者Bは公開鍵A'を使って検証、Aからの署名つき文書だと誤認させられてしまう

⇒公開鍵は、秘密ではないが、**安全**に配送する必要がある。

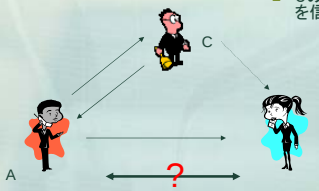
（公開鍵を安全に配布するための方法）
Public Key Infrastructure (PKI)；公開鍵認証基盤

20

PKIの原理

（ケーススタディ）
AとBは初対面、しかしAとBには共通の信頼できる知人Cがいたとする
- A, BはCの公開鍵を持っている

- Aは、「安全な方法で」自分の公開鍵をCに渡し、Cに署名してもらう(Aの**電子証明書**)
- Aは、自分の電子証明書をBに見せる
- Cの署名により、BはAの公開鍵を信用することができる

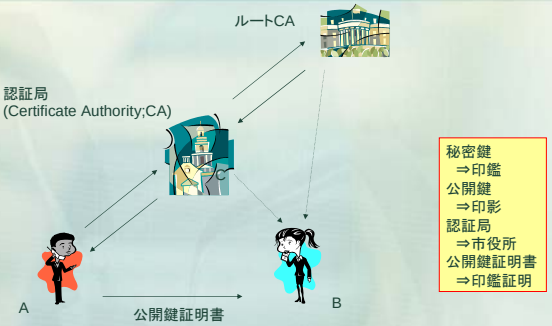


直接の知人がいなくても知人の知人の知人,,,のような連鎖により同様のことができる

一見さんお断り
○○先生のご紹介やったら～

21

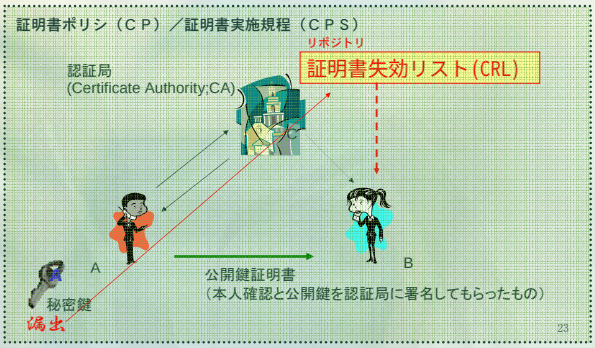
PKIの仕組み



秘密鍵
⇒印鑑
公開鍵
⇒印影
認証局
⇒市役所
公開鍵証明書
⇒印鑑証明

22

PKIの仕組み：証明書の失効



23