# 暗号技術を用いた認証

牧之内研究室M1
久保正明

牧之内研究室「インターネット実習」Webページ

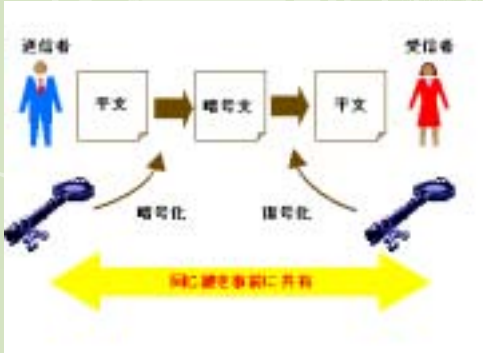
http://www.db.is.kyushu-u.ac.jp/rinkou/internet/

# 暗号

- 暗号化
  - ある情報を他人にわからないように変換する
  - 例：アルファベットをずらす a→b,b→c,…
  - 現在は数学的な理論に基づき暗号化されている
- 暗号化技術はなぜ解読が困難なのか
  - 整数論の環（掛け算はあるが割り算が無い）
    - 一方向の計算しかできない
  - 大きな数を現実的な時間で素因数分解することが困難（という前提）
    - ただし、2002年8月現在、確実に素因数分解ができるアルゴリズムがインドで考案され、暗号解読への応用が期待されている
- 暗号化の種類
  - 共通鍵暗号
  - 公開鍵暗号

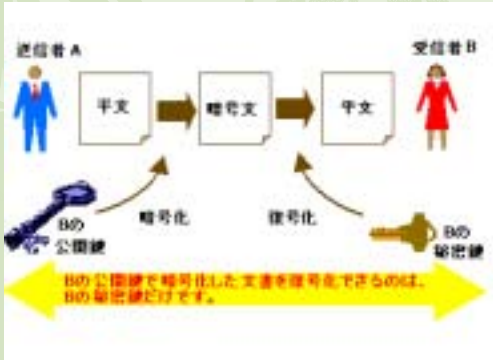
# 共通鍵（秘密鍵）暗号

- 、暗号化と復号化に同じ鍵(秘密鍵)を用いる暗号方式
- 鍵が共通なためデータ送受信の前に鍵を安全な方法で送信する必要がある




# 公開鍵暗号

- 公開鍵と秘密鍵を使ってデータの暗号化･復号化を行う暗号方式
- 公開鍵は他人に広く公開し、秘密鍵は本人だけが管理
- 暗号化と復号化を同じ鍵で行なう共通鍵暗号方式に比べて、鍵を安全な経路で輸送する必要がないため、鍵の管理が簡単で安全性が高い



# 公開鍵、秘密鍵の比較

| | 公開鍵暗号方式 | 共通鍵暗号方式 |
|---|---|---|
| 鍵の管理 | 秘密鍵は1つなので容易 | 複数の秘密鍵が必要なので困難 |
| 鍵の交換 | 公開鍵を交換すれば良い | 秘密鍵の交換が必要 |
| 鍵交換時の危険性 | 改ざんにのみ注意が必要 | 盗聴されれば終わり |
| 処理時間 | 長い（数百～数千倍） | 短い |
| 認証 | 第三者に証明できる | 不十分 |

- 共通鍵方式
  - 暗号化、復号化の鍵が同一→高速
  - 本文、ファイル内容の暗号化に利用
- 公開鍵方式
  - 暗号化と復号化の鍵が異なる→多人数とのやり取り、低速
  - 共通鍵の暗号化･復号化、デジタル署名に使用

# DES

- 1974年 IBMとNSAが開発
- 共通鍵暗号
- パスワードの保存などに使用
- 合衆国商務省標準局（NBS）により長期間標準化
- 64ビット（事実上56ビット）のブロック化
- 鍵を用いた非線形処理

## RSA

- 1977年に開発
- 公開鍵暗号
- 素因数分解を行う効率的なアルゴリズムがないことが大前提
- 合衆国の厳しい輸出規制（ビット数の制限）
  - 1998年に銀行などで128ビットを使用可
- SSHのユーザ認証などに使用

## その他暗号アルゴリズム

- 3DES DESを3回かける
- AES　DESの発展形
- IDEA
- MD5　パスワードなど
- Diffie-Hellman
- Blowfish
- Twofish
- ArcFour

# 暗号化の安全性・脆弱性

- DES
  - 1998年　RSA Lab.のコンテストにより3日で解読される
- RSA
  - 1997年　RSA56ビットが5ヶ月で解読される
  - 1999年　RSA512ビットが5.2ヶ月で解読される
- **現実に暗号解読は可能**
  - ただし、計算機数百台とある程度の時間が必要
  - RSA社が賞金をかけている

# 具体的なパスワードの解読法

hoge2000

これかな？

適当に想定

hoge2000

暗号化手順

逆は不可能

eD7Cif9sDS

・パスワードファイル内の暗号化された文字列

・単語辞書
・Pwdファイルの一般的情報

・個人情報からの想定
・一般単語からの想定

パスワード解読ソフト

John the ripper

# SSH

リモートでログインするプログラム

通信路の暗号化

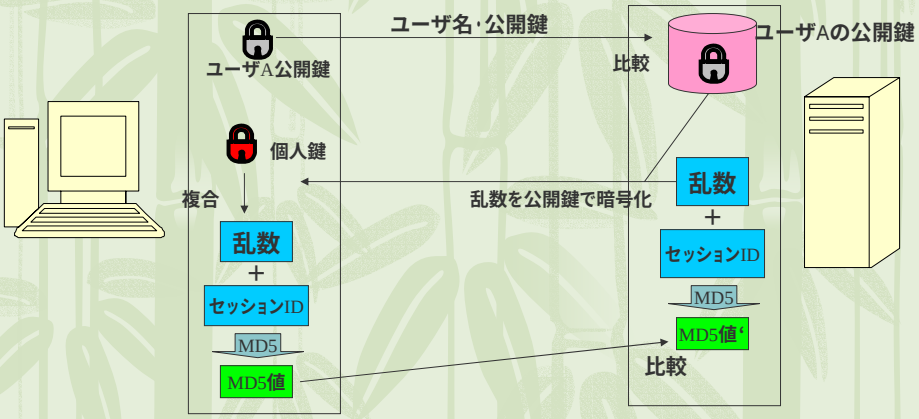
認証

- 公開鍵暗号 (RSAなど：バージョンにより異なる)

セッション

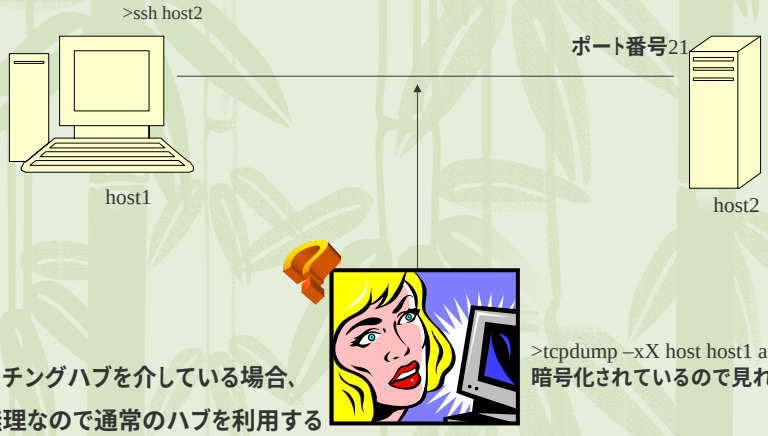
- 共有鍵暗号 (3DESなど：バージョンにより異なる)

# SSHでの認証のしくみ



# 実験

- SSHの盗聴

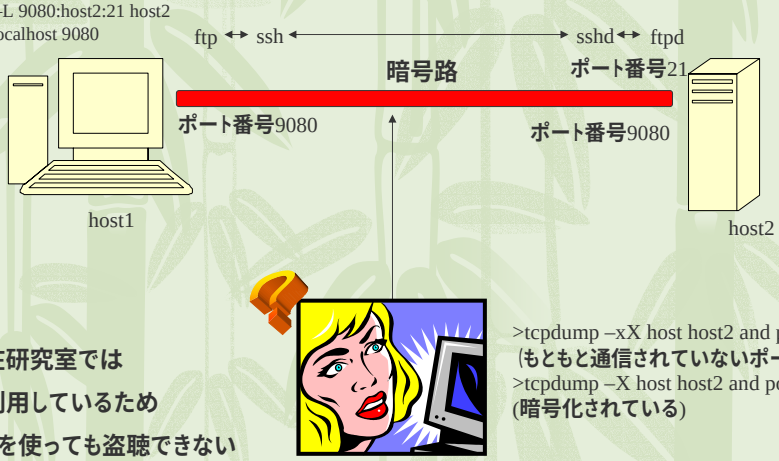



>tcpdump –xX host host1 and port 22
暗号化されているので見れない

注：スイッチングハブを介している場合、
盗聴は無理なので通常のハブを利用する

# SSHでのポート転送

FTPの暗号化
>ssh –L 9080:host2:21 host2
>ftp localhost 9080




>tcpdump –xX host host2 and port 21
(もともと通信されていないポート)
>tcpdump –X host host2 and port 22
(暗号化されている)

注：現在研究室では
sftpを利用しているため
単にftpを使っても盗聴できない