帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

情報セキュリティ論(4)
暗号(2):公開鍵暗号

中野秀男
情報メディア学科/ICTセンター長

今日の話

- 暗号の復習(3回目の暗号の基礎などをもう一度視聴)
- 公開鍵暗号
- 電子署名の仕組み
- RSA暗号

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

暗号の種類

- 慣用(共通鍵)暗号
  - 暗号化鍵も復号化鍵も秘密(秘密鍵)
  - 1980年前までは、暗号はこれだけ
- 公開鍵暗号
  - 暗号化または復号化鍵を公開する暗号
    - もう1つの鍵は秘密
  - 暗号化鍵を公開:秘匿
  - 復号化鍵を公開:電子署名
  - ちょっと過去を
    - 1970年代に計算量の研究が盛んに
    - 解ける問題と解けない問題
    - P≠NP
    - この研究の流れからRSA暗号ができた

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

公開鍵暗号

- 暗号解読の難易度を数学的に示す
- 1方向性関数（逆計算が難しい）を利用
- RSA暗号(Rivest,Shamir,Adleman)
  - 合成数の素因数分解の難しさが暗号の強度
- 処理速度は一般的に慣用暗号より遅い
- 秘匿化だけでなく署名(認証)にも使える
- 電子署名だけならハッシュ（Hash)も使える
  - ハッシュは暗号と違って元に戻らない
  - 戻らない利点を使って匿名化技術に

公開鍵暗号のインパクト

- 暗号が秘匿化だけでなく認証に使える
- デジタルなものに電子署名
- インターネット上でビジネス
- 慣用暗号と組み合わせると実用的
  - 鍵の交換は公開鍵
  - データ伝送時は慣用暗号
- 数学的な難しさに依存する安心感

公開鍵暗号・デジタル署名の基礎

- 数学的な難しさ
  - 素因数分解：合成数を素数分解する難しさ
    - 素数の判定はランダムアルゴリズムで解ける
- 1方向性関数
  - y=f(x) で、xを与えたときyは簡単に見つかるが、yが与えられたときxを見つけるのは難
  - f(・)が暗号化で、f^{-1}(・)が復号化

公開鍵暗号の原理（1）暗号通信

- 初期化
  - A(Alice)は公開鍵と秘密鍵のペアを生成して、公開鍵は公開鍵簿に登録
- 暗号化
  - B(Bob)は公開鍵簿からAの公開鍵を入手し、その鍵で暗号化してAに送る
- 復号化
  - Aは自分だけの秘密鍵で復号化する
  - これができるのはAだけ

公開鍵暗号の原理（2）電子署名

- 初期化
  - A(Alice)は公開鍵と秘密鍵のペアを生成して、公開鍵は公開鍵簿に登録
- 署名して送る
  - Aは自分の秘密鍵で暗号化してB（Bob)に送る
- 復号化
  - Bは公開鍵簿からAの公開鍵を見つけ、Aから送られてきたものをAの公開鍵で復号化する
  - このような伝送文を送れるのはAだけ

RSA暗号

- 1977年MITのRivest,Shamir,Adleman
- 鍵生成
  - 2つの素数p,q: n=p x q: λ(n)=LCM(p-1,q-1)
  - $Z_{\lambda(n)}$のあるeに対して、d=1/e mod λ(n)
    - ただし、GCD(e,λ(n))=1
  - 秘密鍵（dまたはp、q）：公開鍵（e,n)
- 暗号化：$c=m^e \bmod n$
- 復号化：$m=c^d \bmod n$
- n は200桁程度の数が使われている

RSA暗号（例題）

- 数学的準備
  - Z_3 = {0,1,2} 3進数
- 鍵生成
  - p=7,q=11: n=p x q=77: λ(n)=LCM(6,10)=30
  - $Z_{\lambda(n)}$={0,1,・・,29}のあるe=7に対して、
    - d=1/e mod λ(n)=13, λ(n)=30, 7 x 13 = 91 = 1 mod 30
    - ただし、GCD(e,λ(n))=GCD(7,30)=1
  - 秘密鍵（dまたはp、q）(13または6,10)
  - 公開鍵（e,n) (7,77)
- M={0,1,2,・・,76}
- 暗号化：$c=m^7 \bmod 77$
- 復号化：$m=c^{13} \bmod 77$

その他の公開鍵暗号

- ナップザック暗号
  - 破られた公開鍵暗号：1983年
  - 1+2+4+8+16+32+64+128=255
  - (01010101) = ?
- 楕円暗号：楕円関数を利用

今週のミニレポート

- 公開鍵暗号の慣用暗号との違いと特徴を説明してください。
  - 指定した中野のメールアドレスに2週間以内(5月21日まで)に送る。