帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

情報セキュリティ論(3)
暗号(1):歴史と慣用暗号

中野秀男
情報メディア学科

今日の話

- 暗号の歴史
- 暗号理論
- 暗号の基礎
- 慣用(共通鍵)暗号、公開鍵暗号
- 慣用暗号
  - DES
  - AES

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

暗号の歴史

- 古くはシーザ暗号:文字を数文字シフト
  「NAKANO」→「OBLBOP」 1文字シフト
  英語の大文字26文字だけ使用
  - 暗証番号程度なら便利
- 換字と転置の組み合わせ
  - 換字:文字を変える
    - 頻度分布解析で簡単に解読:E,TH,HE,THE
  - 転置:文字順の入れ替え
    - もとの字が残る:「なかの」→「のなか」

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

暗号の歴史(続)

- 1970年後半まで(公開鍵暗号の出現まで)
  - 鍵を秘密にする:秘密鍵暗号→慣用暗号
  - 第1次、第2次世界大戦までの暗号
    - Enigma
  - 戦争の歴史:暗い暗号研究
- 1980年以降(公開鍵暗号出現以来)
  - 暗号の利用範囲が多岐に(署名にも)
    - 電子署名→電子商取引
  - 慣用暗号と公開鍵暗号の長短所を使って併用
    - 鍵の交換を公開鍵で、データ伝送は慣用暗号

暗号理論の動き

- 目的: データの秘匿化だけから認証も
- 専門家: 研究と実践(閉じた系とオープン系)
  - 研究者、組織の管理者、政府系
- 種類: 慣用暗号, 公開鍵暗号
- 暗号の強さ(強度評価)
  - 秘密度から解読に要するリソース量
- 公開鍵暗号
  - 1970年代後半から現れた暗号系
  - 新しい概念も:ゼロ知識証明

暗号の基礎

- 平文(plain text)
- 暗号文(cryptography)
- 暗号化:平文を暗号文にする
- 復号化:暗号文を平文に戻す
- 暗号解読:正当でない人(?)が復号する
- 暗号化鍵 と 復号化鍵
  - 両方を秘密にすると慣用(共通鍵)暗号系
  - 片方を公開すると公開鍵暗号系
- ブロック暗号:64ビットの毎に暗号
- ストリーム暗号:1ビット毎に暗号,最強の暗号

暗号の言葉

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

慣用(共通鍵)暗号

- DES(Data Encryption Standard)
  - 1970年代後半からの標準
  - UNIXのパスワードにも
  - 今では危ないが、強度は方式でカバー
- AES(Advanced Encryption Standard)
  - 世界中から公募して選んだ
- 一般に暗号/復号化は速い

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
  - y=f(x), x?
- 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

暗号（含ハッシュ）の応用

- いろいろな応用や考え方に
  - SSL(Secure Socket Layer)
  - PGP(Pretty Good Privacy)
  - Challenge and Response
- 暗号等の性質を使って
  - 慣用暗号（処理速度）
  - 公開鍵暗号（署名）
  - ハッシュ（ハッシュ値は固定長）

共通鍵暗号、慣用暗号

- 暗号化鍵と復号化鍵を同じにして秘密に
  - 新しい公開鍵暗号に対して従来からあるという意味で慣用暗号とも
- 1970年代まではアルゴリズムも秘密
- 1970年代にDES
- 1998年にTriple-DES
- 2001年にAESとしてRijndael

DESの歴史

- Data Encryption System
- 1970年代に米国で政府標準暗号の公募
- IBMのみが応募
- IBMの応募をもとに政府がDES案を策定
- 1977年に最終決定
- 1998年まで有効な暗号として承認
- 1998年Triple-DES

DES暗号

- ブロック暗号：適当なブロック毎に暗号化する
  - ブロック暗号以外にストリーム暗号
- DES暗号
  - 1ブロックは64ビット
  - 鍵は56ビット＋8ビットパリティ＝64ビット
  - 基本は換字式と転置式の組み合わせ
  - 16段の反復処理
  - 各段で異なるSBOX（変換表）をもったF関数処理

DESの問題点

- 設計として
  - SBOXの設計基準が公表されていない
  - 鍵（56ビット）が短すぎる
  - 段数（16段）が少なすぎる
- 多くのアタック法が出現
  - 差分攻撃
  - 線形攻撃：1994年、WS12台、50日
  - 全数探索：1997年

DESの改善

- Triple-DES
  - DESを3段重ね：暗号(K1)＋復号(K2)＋暗号(K1)
  - 鍵は56＋56＝112ビット
  - K1=K2ならDESと同じ
- AES(Advanced Encryption Standard)
  - 新しい共通鍵暗号を公募（米国）
  - 2000年：Rijndael暗号を承認
  - あと10年程度は安全

AES:Rijndael暗号

- AESでRijndaelが選ばれるまで
  - 21の応募、15が候補として認定
  - 最後は残った5つから投票で
- 128ビットブロック、128ビット鍵、10段
  - 192ビット鍵、256ビット鍵
  - 段数は最大14段
  - 数学的にはガロア体理論で安全度を保証
  - C言語でのコード記述にも配慮

今週のミニレポート

- 復号、暗号鍵、復号鍵、暗号解読のそれぞれについて説明してください。
  - 指定した中野のメールアドレスに5月21日までに送る。