情報ネットワークⅡ（情213）

【第7回】

演習（1）

（中間試験対策）

担当教員：長田智和

E-Mail: nagayan@ie.u-ryukyu.ac.jp

URL: http://n-lab.info/

（講義日：2017年11月16日）

演習（1）

中間試験のポイント

- 重要技術の技術名・用語とその理解
  - 特に講義資料で色文字になっている技術名・用語
- 情報セキュリティで確保・維持する3つの要件
  - 「機密性」「完全性」「可用性」とは？
- 暗号化技術の理解
  - 共通鍵暗号化方式と公開鍵暗号化方式の違いは？
  - RSAにおける、公開鍵ペアの作成、暗号化、復号。
  - DH鍵共有アルゴリズムの理解
    - 原始根とは？
  - ハッシュ関数とデジタル署名の理解

中間試験のポイント

- 認証方式の理解
  - 主体認証の3つのカテゴリーとは？
  - ID連携（IDフェデレーション）とは？
- PKIの理解
  - 認証局モデルにおけるパブリック認証局とプライベート認証局の違いは？
  - EV SSL証明書とは？
  - 証明書チェーンとは？

2.5 ハッシュ関数とデジタル署名

- 2.5.1 ハッシュ関数
  - 任意の長さのデータを固定長（128-512ビット程度）に圧縮する関数のこと。以下の性質を持つ。
    - 一方向性: 出力値から入力値を発見することが困難であること。すなわち、

      h = hash（m）

      を満たすm を求めることが困難であること。
    - 第2原像計算困難性: ある入力値と同じハッシュ値となるような別の入力値を求めるのが困難であること。

      すなわち、

      hash（m） = hash（m’）

      となるような m’（ただし、m ≠ m’） を求めるのが困難であること。

2.5 ハッシュ関数とデジタル署名

- 2.5.1 ハッシュ関数
  - 任意の長さのデータを固定長(128-512ビット程度)に圧縮する関数のこと。以下の性質を持つ。
    - 衝突困難性: 同じ出力値を生成する2つの入力値を発見することが困難セあること。

      すなわち、

      hash（m）= hash（m’）（ただし、$m \neq m'$）

      を満たすm, m’を求めるのが困難であること。
  - ハッシュ関数で生成された値をハッシュ値という。
- （教科書p.55の図2.31を参照）

2.5 ハッシュ関数とデジタル署名

- 2.5.2 デジタル署名
  - メッセージのハッシュ値を秘密鍵で暗号化することで、メッセージの改竄検知、否認防止を実現する仕組み。
  - デジタル署名方式:
    - RSA, DSA, ECDSAを用いるのが一般的
- （教科書p.59の図2.35を参照）

2.5 ハッシュ関数とデジタル署名

2.5.2 デジタル署名

デジタル署名の流れ

- 署名者はあらかじめ公開鍵P 、秘密鍵S を用意し、公開鍵は署名の検証者に安全に渡しておく。
- ハッシュ関数を用いて、送信する平文M のハッシュ値を求める。
- 署名者はあらかじめ用意しておいた秘密鍵S を用いて、ハッシュ値H を暗号化し、署名値H_Sを得る。
- 平文M と署名値H_Sを検証者に送る。
- 検証者は平文M からハッシュ値H’ を求める。
- 署名者が発行した公開鍵P を用いて署名値H_Sを復号し、ハッシュ値H を求める。なお、秘密鍵S で暗号化したデータは秘密鍵S とペアとなる公開鍵P でしか復号できないことに注意。
- 検証者は、署名から得られたハッシュ値H と平文M から求めたH’ が一致するかどうかを確認する。（不一致なら、何らかの攻撃があったとみなす）

2.3 公開鍵暗号化技術

2.3.1 RSAの仕組み

RSAの鍵生成手順

- 大きな素数 p と q をランダムに選ぶ。（p≠q）
- n = pq を求める（ n の長さが鍵長となる）
- （p-1）（q-1）と互いに素な正の整数 e を求める。
- ed ≡ 1（mod （p-1）（q-1））となる正の整数 d を求める。
- 公開鍵（暗号化鍵）として、e と n を公開する。
- d は秘密鍵として安全に管理する。p と q は破棄する。*重要
- 以上より、暗号化、復号は下記の通りとなる。

暗号化: $C = M^e \bmod n$ （C=暗号文、M=平文）

復号: $D = C^d \bmod n$ （D=復号文（＝平文（M））

2.3 公開鍵暗号化技術

2.3.1 RSAの仕組み

RSAの仕組みのまとめ

- ランダムに選んだ2つの素数 p, q（$p \neq q$）とすると、$n = pq$ を法とする世界を考える。
- 平文Mを$(p-1)(q-1)$と互いに素な正の整数e（公開鍵）で冪乗した値を暗号文M^eとする。
- 平文Mは{$(p-1)$と$(q-1)$の最小公倍数+1}回冪乗すると元の値に戻り、さらに{$(p-1)$と$(q-1)$の最小公倍数}回冪乗するたびに元の値に戻る性質がある。

  すなわち、整数 d を秘密鍵とすると、

  $(M^e)^d = M^{\{(p-1)(q-1)+1\}} \rightarrow ed = (p-1)(q-1)+1$

  $\therefore ed \equiv 1 \pmod{(p-1)(q-1)}$

  が成り立つ。

2.3 公開鍵暗号化技術

- 2.3.1 RSAの仕組み
  - RSAの演算の例
    - 鍵の生成
      - 2つの素数を p=3 及び q=5 とする。
      - n = pq = 15　→ 15 を法とする世界を考える。
      - (p-1)(q-1)と互いに素な正の整数を e=3 とする。

        ＊互いに素＝最大公約数が 1 となる数
      - ed ≡ 1(mod (p-1)(q-1))となる正の整数をd=3 とする。
      - 以上より、e=3, n=15 を公開鍵、d=3 を秘密鍵とする。

2.3 公開鍵暗号化技術

- 2.3.1 RSAの仕組み
  - RSAの演算の例
    - 暗号化
      - 平文を 2 とする。
      - $C = 2^3 \bmod 15 = 8$
    - 復号
      - $D = 8^3 \bmod 15 = 2$

2.4 鍵共有アルゴリズム

- 2.4.1 Diffie-Hellman（DH）鍵共有アルゴリズム
  - アルゴリズムの説明
    - 鍵を交換する主体をA, B とする。
    - A, B はあらかじめ素数 p とその原始根 g を交換しておく。（p, g は秘密にする必要はない）
    - 鍵の共有時は、A は乱数 x、B は乱数 y を生成し、秘密に管理する。
    - A は $n = g^x \bmod p$、Bは $m = g^y \bmod p$ を計算する。A, B は n, m を互いに交換する。（n, m は秘密にする必要はない）
    - A, B は、$K = \{m|n\}^{\{x|y\}} \bmod p = (g^{xy} \bmod p)$ を共有する暗号化鍵として使用する。
- （教科書p.53の図2.29を参照）

2.4 鍵共有アルゴリズム

- 2.4.1 Diffie-Hellman（DH）鍵共有アルゴリズム
  - DH鍵共有アルゴリズムに対するMITM攻撃
    - 主体A, B の間に攻撃者I が入り込み、I は自身が生成した n', m' をA, B に成りすましてそれぞれに転送する。
    - 問題点: 素朴なDH鍵共有アルゴリズムでは、A, B が受け取ったメッセージの真正性を確認できない。このため交換するメッセージにデジタル署名を施すなどの防御策が必要。
- （教科書p.54の図2.30を参照）

2.4 鍵共有アルゴリズム

- 原始根とは？
  - 原始根とは、素数 p を法とした場合、冪乗した値によって、素数 p より小さい正の整数（pで割ったときの余り）がすべて得られる値のこと。
  - （例）5 を法として 3 の冪乗を計算してみる。

$3^0 \equiv 1 \pmod 5$
$3^1 \equiv 3 \pmod 5$
$3^2 \equiv 4 \pmod 5$
$3^3 \equiv 2 \pmod 5$
$3^4 \equiv 1 \pmod 5$
$3^5 \equiv 3 \pmod 5$　∴ 3 は法 5 において原始根である。

[フェルマーの小定理]
pが素数、かつ、$1 \leqq a < p$ (aは正の整数) のとき、
$a^{p-1} \equiv 1 \pmod p$
が成り立つ。

例題（XOR）

- 排他的論理和(XOR)では、同じ値を適用すると元の値に戻る性質ある。ここで、$P = B4_{(16)}$、$K = AA_{(16)}$としたとき、
  - C = P XOR K
  - P = C XOR K

  となることを示せ。ただし、16進数は2進数に変換してXOR演算すること。

例題（RSA）

- RSA公開鍵暗号化方式において、2つの素数をp,q(p≠q)とし、n=pqとする。また、暗号化する前の平文をMとし、暗号化した暗号文をCとする。ここで、2つの素数をp=3及びq=7とする。このとき、公開鍵(e,n)と秘密鍵(d)を定め、平文(M)=2を公開鍵(e,n)を用いて暗号化し、暗号文(C)を求めよ。また、秘密鍵(d)を用いて復号し、元の平文(M)が得られるか検算せよ。

例題（原始根）

- DH鍵共有アルゴリズムで重要となる、鍵を共有する主体者同士で交換する素数pとその原始根gについて、p=7とした場合の原始根gの候補を全て求めよ。

【次回予告】
第8回
中間試験

また来週！