コンピュータ概論 A/B

-- 公開鍵暗号 --

数学科 栗野 俊一 (TA: 佐藤 淳 [院生 1 年])

伝言

私語は慎むように !!

- 席は自由です (出席パスワード : 20151124)
  - できるだけ前に詰めよう
  - 教室にきたら直ぐにやる事
    - PC の電源 On / ネットワーク接続 / Web を参照する / skype を起動する
- 色々なお知らせについて
  - 栗野の Web Page に注意する事

    http://edu-gw2.math.cst.nihon-u.ac.jp/~kurino
- ネットワークの認証が変りました
  - これまでは、ダイアログ表示だったのですが、先日から認証ページに代りました

前回(2015/11/17)の内容 (1)

- □ 講義
  - ○ 暗号について
    - ▹「暗号化」とは「対応の予測」ができない「全単射」の関数の適用
    - ▹「関数」が解らないと、元に戻せない(逆関も解らない)
    - ▹「暗号鍵」:暗号化の関数と復号(平文)化の関数(逆関数になる)を指定する情報
  - ○ 暗号形式
    - ▹ 対称鍵暗号方式 (暗号鍵を共有する) : 暗号化鍵と復号(平文)化鍵が同じ
    - ▹ 公開鍵暗号方式 (暗号鍵を公開する) : 暗号化(公開)鍵と復号(平文)化(秘密)鍵が異る
    - ▹ 公開鍵暗号方式では、公開鍵を公にしてよい(対称鍵では、それができない)
  - ○ システムとメタシステム
    - ▹ システム : 操作の対象(例:数)と、操作(例:計算)からなる
    - ▹ メタシステム : 対象となる「システムの操作」を操作するシステム
    - ▹ メタシステムは「強力」だが、利用が難しい(間違った使い方が横行している)

前回(2015/11/17)の内容 (2)

- 演習 (TrueCrypt の操作)
  - tc ファイルの作成 : 名前とサイズとパスワードを指定 (金庫の作成)
    - パスワードは、tc ファイル固有のもの (ファイル毎に別のものを指定)
  - tc ファイルのマウント : tc のファイルの内容を参照 (金庫を開ける)
    - そのファイル用のパスワードを指定する (新しいドライブができる)
  - tc ファイルのアン(ディス)マウント : ファイルを閉じる (金庫を閉める)
    - 「閉まったまま」の tc ファイルは、内容が参照できない (安全)
  - tc ファイルを利用した、秘密メッセージの通信
    - (対称鍵方式なので) パスワード(暗号鍵)を相手(自分)に報せる
    - そのパスワードで tc ファイルを作成
    - ファイルをマウントしてファイル(通信文)を入れる
    - ファイルをアンマウントして、安全にする
    - そのファイルを相手に渡す (USB Memory, Skype, メール等)

本日(2015/11/24)の予定

- 本日(2015/11/24)の予定
  - 公開鍵暗号
  - UI (2015/11/10 の資料)
- 実習
  - Kleopatra の利用 (2015/11/17 の資料)

今回 (2015/11/24) の課題

- 今回 (2015/11/17) の課題 (前々回の課題)
  - 次の TrueCrypt のボリュームを作成し、CST Portal から提出
    - 表題 : TrueCrypt のボリュームファイルの提出
    - ファイル名 : 20151117-QQQQ.tc (QQQQ は学生番号)
    - 詳しくは、配布した sample-20151117.tc の内容を参照
- 今回 (2015/11/24) の課題
  - 自分専用の鍵ペアを作成し、「公開鍵ファイル」を提供する
    - 表題 :「公開鍵ファイル」の提出
    - ファイル名 : 20151124-QQQQ.asc (QQQQ は学生番号)
    - 詳しくは、配布した kurino-pubkey.asc の内容を参照

実習

- [実習 1] Kleopatra の利用
  - 前回(2015/11/17) の資料を参照
- [実習 2] 課題の提出
  - 自分の鍵の「公開鍵(public key)」ファイルを CST Portal に提出
    - 「秘密鍵(private key)」ファイルを提出したら「無効」
    - 「秘密鍵(private key)」は大事なものなので、他人にしらせてはいけない
- [実習 3] 公開鍵の交換
  - skype やメール等で、公開鍵を互に交換する
- [実習 4] 暗号メッセージの作成
  - 暗号メッセージの作成し、相手に skype やメール等で、送る
  - 暗号メッセージを受け取ったらその内容を確認する