コンピュータ概論 A/B

-- MS-Excel のまとめ & 暗号化 --

数学科 栗野 俊一

2012/10/23 コンピュータ概論

伝言

私語は慎むように !!

- オリンテーションはお疲れ様でした
- 連絡事項
  - 次回は DVD Drive をもってくる事
    - Mathematica のインストールを行います
- 教室に入ったら
  - 直に Note-PC の電源を入れておく
    - Network に接続し、当日の資料に目を通す
    - skype に Login する
    - Windows Update をしておこう
- やる気のある方へ
  - 今日の資料は、すでに上っています
    - どんどん、先に進んでかまいません
- 作業
  - Web 履修科目登録の確認
    - CST Portal も確認しておきましょう

前回までの復習

- □ 講義
  - ○ Excel での計算
    - ▹ Excel は表計算ソフト(表を作成できる/計算もできる)
    - ▹ 計算式 :「=」で始まり、式を書く / セルの参照(絶対,相対,複合)
    - ▹ 様々な関数(=機能)が利用できる (自分で関数表を *見て置く* 事)
    - ▹ 数列(微積) : 複合参照のコピー / 行列(代幾) : 範囲指定/CSE
  - ○ グラフ :「表現方法」の一つ
    - ▹ 情報のデフォルメ(強調)を行う / 目的意識(何を強調する?)が重要
  - ○ Excel のグラフ化機能
    - ▹ Excel では「表」から「様々なグラフ」を作る事ができる(自分で..)
    - ▹ 関数から表へ (差分化 : 関数を x, y の対応[数値]表で表現)
    - ▹ 数値表(差分化)により、積分(総和になる)も計算可能
  - ○ Excel と TeX の連携
    - ▹ Excel の表(Excel2LaTex)とグラフ(inkscape)は TeX で利用できる
    - ▹「ファイル」を利用する事により、ツール(ExcelとTeX)間で連携できる

本日の予定

- 講義
  - Excel のまとめ
    - Excel による成績処理
  - セキュリティと暗号化
    - 暗号化と TrueCrypt
- 実習
  - [演習 1] Excel による成績処理
  - [演習 2] truecrtpt のインストール
  - [演習 3] truecrtpt の使い方
  - [演習 4] 課題の作成

本日の課題 (2012/10/23)

- 今週 (2012/10/23) 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 : 2012/10/23-QQQQ.tc (QQQQ は学生番号)
    - 詳しくは、配布した sample-2012/10/23.tc の内容を参照
- 先週 (2012/10/16) の課題
  - 次のファイルを提出しなさい
    - ファイル名 : 20121023-QQQQ.pdf (QQQQ は学生番号)
    - 内容 : MS-Excel と TeX の連携
    - 詳しくは、配布した sample-20121023.tex, sample-20121023.pdf の内容を参照

Excel のまとめ

- □ Excel のまとめ
  - ○ Excel は「表形式のデータ」を処理できる
- □ 表データはどこから？
  - ○ 色々な統計データ：複数の「対象」に対する複数の「属性値」を調べる
    - ▹ cf. 対象:都道府県, 属性値:面積/人口/気温/etc..
  - ○ 関数：「関数」は、「集合から集合への対応」: x と y の値の対応表
    - ▹ cf. y=x^2, (x,y) = (1,1), (2,4), (3,9), .. / 数列 / 積分
  - ○ データ：様々な「数値の集まり」が、「整理」によって「表」に変る
    - ▹ cf. コンビニの売上：時間(昼は弁当の売上が..) / 客層(学生は雑誌を..)
- □ Excel の役割
  - ○ データを記録・整理(表)し、加工(式)したあと、見易く表示する(グラフ)
    - ▹ 色々な所で利用できる Tool として利用する
  - ○ Excel の様々な機能の学習
    - ▹ 基本は、「Call by Need (必要に応じて調べる)」
- □ CSV 形式
  - ○ 表形式のデータを Text で保持する形
    - ▹ Excel で読み書きできる / エディタでも読み書きできる

実習 1: Excel による成績処理

- [実習 1] 成績処理のシートを作成する
  - 実習内容
    - ssvb_dat.zip の中にある素点データから偏差値を計算
  - 利用する excel 関数
    - COUNTIF : 条件を満すデータを数える
    - SUM : 総和を計算する
    - SQRT : 平方根を求める
  - 偏差値の計算

    偏差値 T_i は次の式で求める事ができる ([参考] wikipedia:偏差値)。

$$T_i = \frac{10(x_i - \mu_x)}{\sigma_x} + 50$$

ただし、$\sigma_x \neq 0$ であり、

$$\mu_x = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad \sigma_x = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu_x)^2}$$

N:母集団の大きさ、x_i：個々の値、μ_x：算術平均、σ_x：標準偏差

PC セキュリティ (復習)

- PC のセキュリティを守ろう
  - 知る事：最新の知識を身に付ける
    - cf. セキュリティホール Memo
  - 危険をさける
    - セキュリティホールをなくす (update する)
    - 対策ソフトを入れる
  - 善後策を練る (怪我をしても血がでなければ良い)
    - 暗号化を行う：情報が流出しない
    - バックアップを行う：情報が消失しない
- 結局は、意識の問題
  - 恒常的な努力が必要
    - 最新情報の入手/適切な判断/効果的な対策の実施

暗号化

- □ 暗号とは
  - ○ コーディングの一種
    - ▹ なんらかの「規則」で、「情報を表現する」方法
    - ▹ その「規則」が解らないとそれが「表現している情報」が得られない
- □ 暗号の用語
  - ○ 文(ファイルの形式)
    - ▹ 平文：調べれば、「それが表現する内容」が得られる
    - ▹ 暗号文：その表現(ファイル)だけでは内容を知るのが大変困難な表現(鍵があれば見れる)
  - ○ 変形(操作)
    - ▹ 暗号化(encode)：「平文」を「暗号文」にすること
    - ▹ 平文化(decode)：「暗号文」を「平文」にすること
  - ○ 鍵(情報を秘密にするための「種」)
    - ▹ 暗号化したり平文化するために、必要な情報(cf. パスフレーズ)
    - ▹ 対称鍵暗号方式：暗号化と平文化で「同じ鍵」を利用する
    - ▹ 公開鍵暗号方式：暗号化と平文化で「異なる鍵」を利用する

TrueCrypt

- TrueCrypt とは
  - ファイルの「暗号化を行う」ためのツール
    - ファイルを暗号化して入れる「箱(暗号化ボリューム)」が作れる
    - 暗号化ボリュームを作る時にパスフレーズを設定する
    - 暗号化ボリュームは暗号化されていてパスフレーズを知らないと見れない
  - 暗号化ドライブを作る事ができる
    - 暗号化ボリュームはマウントできる
    - マウントするには、作成した時に利用したパスフレーズが必要
    - マウントすると、ドライブ(USB メモリみたいなもの)になり、普通にファイルが記録できる
    - 利用しない場合はアンマウトしておく
- 暗号化ボリュームとパスフレーズ
  - 暗号化ボリュームは暗号化されているので、普通に交換してよい
    - メールや skype で送ったり web で公開してもよい
  - 暗号化ボリュームの内容を参照するには、パスフレーズが必要
    - パスフレーズは、本当は「安全な方法」で送る必要がある
    - 今回は、skype を使うが、本当は良くない (skype が覗見される可能性がある)
    - 理想は「手渡し」だが...

Truecrypt の仕組(マウント/アンマウント)

マウントする

→

←

実習 2: TrueCrypt のインストール

- [実習 2.1] TrueCrypt のインストール
  - TrueCrypt のインストールファイルのダウンロード
  - TrueCrypt のインストール
    - 右クリックメニューから、「管理者として実行」すること
  - TrueCrypt の言語ファイルのダウンロード
  - TrueCrypt の言語ファイルのインストール
    - Language.ja.xml を c:\Program Files\TrueCrypt にコピーする
- [実習 2.2] TrueCrypt の動作確認
  - sample-20121023.tc をディスクトップにダウンロード
  - TrueCrypt を起動 (sample-20121023.tc をダブルクリックでもよい)
    - sample-20121023.tc を d: にマウントする
    - パスフレーズは skype で伝達
    - ファイルの中身を確認の事 (課題に関する情報がある)

実習 3: 自分用のボリュームを作る

- [実習 3.1] 新規ボリュームファイルの作成
  - TrueCrypt で、新規ボリュームファイルを作成する
    - サイズ : 1 M byte / ファイル名 : 自由 / パスフレーズ : 自分で決める
- [実習 3.2] 内容の作成
  - TrueCrypt で、新規ボリュームを e: マウントする
  - e: にテキストファイルを作成し、メッセージを入れる
  - TrueCrypt で、新規ボリュームをアンマウント
  - skype で、ボリュームファイルとパスフレーズを友人におくる
- [実習 3.3] 手に入れたファイルの確認
  - 手に入れたファイルをパスフレーズを利用して e: にマウントする
  - 内容を確認する
  - e: をアンマウントする

実習 4: 課題の提出

- [実習 4.1] 新規ボリュームの作成
  - TrueCrypt で、新規ボリュームを作成する
    - サイズ / ファイル名 / パスフレーズ : message.txt を参照
- [実習 4.2] 課題の作成
  - TrueCrypt で、実習 4.1 のボリュームを e: にマウント
  - e: に次の二つのファイルを作成する (message.txt を参照)
    - message.txt
    - password.txt
  - e: をアンマウントする
  - 20121023-QQQQ.tc を CST Portal に提出