コンピュータ概論 A/B

-- 暗号化 --

数学科 栗野 俊一 (TA: 宮川 智行 [院生 2 年], 栗原 望 [院生 1 年])

伝言

私語は慎むように !!

- 担任からの連絡
  - 学生証での出席は済ませましたか？
    - 入口の脇の出席装置に学生証を翳す
- 席は自由です
  - できるだけ前に詰めよう
- 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
- VNC Server Address : 10.9.209.27
  - Password : vnc-2017
- 5, 6 限目に「面接」を行います
  - 場所 : 621C / 時間 : 5/6 限 (15 分/名) / 対象 : 7054, 7069, 7093
- 成績表配付：受け取ってない人は直に受取にくる : 7093

Mathematica インストール手順：借り出し

- Mathematica インストール
  - 次回利用予定なので、本日中にインストールを済ませる
- Mathematica インストールメディアの借り出し手順
  - 「学生証」を持って、TA に申し出る
    - 「学生証」とインストール「メディア」を交換 (DVD)
    - DVD ドライブを忘れた人は、USB Memory を受け取る
  - 「メディア」を利用して、インストール
    - ライセンス情報の入力が求められる(この状態で一旦停止)
  - 「メディア」と交換に「ライセンス用紙」を受け取る

    複写禁止、複写禁止、複写禁止、複写禁止
    - 「ライセンス用紙」のラインセンス情報を入力
  - 「ライセンス用紙」と「学生証」を交換

Mathematica インストール手順：インストール

- インストールメディアの利用法
  - DVD ドライブを接続
  - インストールメディア (DVD) を入れる
    - エクスプローラで D: ドライブを開く
  - [Windows] フォルダを開く
  - [setup.exe] を実行する
    - 以下、基本は、[次へ]
  - インストール終了時
    - 「mathematica の起動」を選ぶ
    - 終了した場合は、スタートメニューから mathematica 10.3 を起動
    - 初回だけ、ライセンス情報の入力が要求される (来年 4 月まで有効)

「面接」について

- 面接：こちらから指定した方を対象に面接を行います
  - 面接対象者(以下の番号の人)
    - 講義終了後、栗野のところに来ること

      7054(前回 7052 と間違えて標記), 7069, 7093
    - 基本は、番号順で、終りしだい次の人
- 概要
  - 場所：6 号館 2 階 621C 室
  - 時間：5, 6 限 (一人 15 分程度..)

前回(2017/09/19)の内容

- 講義
  - Excel の基本の復習 (表が作れる、式が使える、相対/絶対参照)
  - Excel の応用
    - 複合参照、行列の計算

本日(2017/09/26)の予定

- 本日(2017/09/26)の予定
  - 暗号化と VeraCrypt
  - Excel 機能の色々(落穂拾い)
- 実習
  - [演習 1] VeraCrypt のインストール
  - [演習 2] VeraCrypt の使い方
  - [演習 3] 課題の作成

今回 (2017/09/26) の課題

- 前回 (2017/09/19) の課題 (前々回の課題)
  - 次のファイルを MS-Excel で作成して CST Portal に提出してください
    - ファイル名 : 20170919-QQQQ.xlsx (QQQQ は学生番号)
    - 内容 : Excel の表 (応用)
- 今回 (2017/09/26) の課題
  - VeraCrypt のボリュームを作成し、CST Portal から提出
    - 表題 : VeraCrypt のボリュームファイルの提出
    - ファイル名 : 20170926-QQQQ.hc (QQQQ は学生番号)
    - 詳しくは、配布した sample-20170926.hc の内容を参照

暗号化

- □ 暗号とは
  - ○ コーディング(符号化)の一種
    - ▹ なんらかの「規則」で、「情報を表現(変換)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)：(逆変換が可能：つまり、全単射)
    - ▹ 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(表現の規則を決め、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 (VeraCrypt)
    - ▹ 公開鍵暗号方式：暗号化と平文化で「異なる鍵」を利用する

対称鍵暗号方式による通信

- □ 対称暗号通信の方式
  - ○ 対称鍵を作り、通信相手に送る
    - ▷ 送信する平文を対称鍵で暗号化して、暗号文にする
    - ▷ 暗号文を通信
    - ▷ 受信した暗号文を対称鍵で平文化して、平文を得る
- □ 対称暗号通信の方式の前提
  - ○ 対称鍵を送受信の双方が持つ必要がある
    - ▷ 「鍵」自身が共有される
    - ▷ その「鍵配送」をどうするかという問題がある

公開鍵暗号方式 (1)

- 対称鍵暗号方式の問題点
  - 暗号の利用目的は？
    - 通信経路が安全でない -> 通信の内容を暗号化して秘密に情報交換したい
  - 対称鍵暗号方式の特徴：送信元と送信先が同じ鍵を持つ必要がある
    - 鍵をどうやって通信相手に渡せばよいのか？(通信経路が安全でないのに)
- 公開鍵暗号方式の利点
  - 暗号化と平文化の鍵が異る
    - 送信元に必要な物：暗号化鍵(Public Key) / 誰が知っていても良い(公開鍵)
    - 送信先に必要な物：平文化鍵(Privacy Key) / 自分だけの秘密(秘密鍵)
  - 公開鍵から秘密鍵を知る事ができなければ安全

公開鍵暗号方式 (2)

- 公開鍵暗号方式を用いた暗号通信
  - 準備 (1 度だけやればよい) : 自分用の鍵ペア (秘密鍵+公開鍵) を作る
    - 通信相手に自分の「公開鍵」を送る
    - 公開鍵はバレてもよいが、「自分の物」である事は「別に保証する」必要がある
  - 暗号通信
    - 通信相手に、「公開鍵」を利用して、メッセージを暗号化して送ってもらう
    - 自分の「秘密鍵」でメッセージを平文化すれば、メッセージを見る事ができる

対称鍵暗号方式と公開鍵暗号方式

- □ 対称鍵暗号方式と公開鍵暗号方式の本質的な違い
  - ○ 対称鍵暗号方式：暗号化と平文化に同じ鍵を使う
    - ▹ 例：自宅の鍵 (錠をかけるにも、錠を開けるにも同じ鍵を使う)
    - ▹ 鍵としての情報を比較的自由に選べる(鍵が小さくすむ) [効率的]
  - ○ 公開鍵暗号方式：暗号化と平文化に異る鍵を使う
    - ▹ 例：ホテルのオートロック (錠は誰でもかけられる、開けるにはカードキー)
    - ▹ 公開鍵と秘密鍵は特殊な関係がある(鍵として利用できるものが少ない) [非効率]
- □ 対称鍵暗号方式と公開鍵暗号方式の使い分け
  - ○ 公開鍵暗号方式の方が鍵配送において安全だが、非効率的
  - ○ 対称鍵暗号方式の方が効率的だが、鍵の配送において危険
    - ▹ 良いとこ取りをする
  - ○ ハイブリッド方式 (効率と安全の両方を得る)
    - ▹ メッセージ本体は、対称鍵方式で暗号化
    - ▹ 「対称鍵」自身を公開鍵暗号方式で暗号化(効率の悪さは最小限度)

VeraCrypt

- VeraCrypt 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
    - 理想は「手渡し」だが...

VeraCrypt の仕組(マウント/アンマウント)

マウントする

->

←

実習 1: VeraCrypt のインストール

- [実習 1.1] VeraCrypt のインストール
  - VeraCrypt のインストールファイルのダウンロード
  - VeraCrypt のインストール
  - 日本語化
    - [Settings] -> [Language] -> [日本語]
- [実習 1.2] VeraCrypt の動作確認
  - sample-20170926.hc をディスクトップにダウンロード
  - VeraCrypt を起動 (sample-20170926.hc をダブルクリックでもよい)
    - sample-20170926.hc を p: にマウントする
    - パスフレーズは、「当日のみ画面」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 2: 自分用のボリュームを作る

- [実習 2.1] 新規ボリュームファイルの作成
  - VeraCrypt 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 (拡張子は .hc) / パスフレーズ : 自分で決める
- [実習 2.2] 内容の作成
  - VeraCrypt で、新規ボリュームを p: マウントする
  - p: にテキストファイルを作成し、メッセージを入れる
  - VeraCrypt 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送る
- [実習 2.3] 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 p: にマウントする
  - 内容を確認する
  - p: をアンマウントする

実習 3: 課題の提出

- [実習 3.1] 新規ボリュームの作成
  - VeraCrypt 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 3.2] 課題の作成
  - VeraCrypt で、実習 3.1 のボリュームを p: にマウント
  - p: に次の二つのファイルを作成する (message.txt を参照)
    - message.txt
    - password.txt
  - p: をアンマウントする
  - 20170926-QQQQ.hc を CST Portal に提出

実習 4: Excel 落穂拾い

- [実習 4.1] 統計グラフ
  - 統計情報を利用して、様々なグラフを作る事ができる
- [実習 4.2] 関数グラフ
  - 関数の値表を作り、それを利用して、関数のグラフを作る
- [実習 4.3] 数表の作成
  - パスカルの三角形を利用して、組み合わせの表を作る
- [実習 4.4] 自然対数の底(オイラー数)の値の計算
  - 数列の極限の計算を利用して、自然対数の底の値を数値計算する