コンピュータ概論 A/B

-- 暗号化 --

数学科 栗野 俊一 (TA: 北野拓也 [院生 2 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 : 10.9.209.18:0
  - Password : vnc-comp-2016
- 本日利用するファイルを、今の内にダウンロードしておこう

前回(2016/11/22)の内容

- □ 講義
  - ○ TeX と Mathematica の連携
    - ▹ Mathematica で作成した式や図を TeX で利用する事ができる
- □ 演習
  - ○ Mathematica で作成したデータのファイルへの保存
    - ▹ 式の TeX 形式での保存 : Put[TeXForm[「式」],"expr.tex"]
    - ▹ 図の eps 形式での保存 : Export["graph.eps",「図」]
    - ▹ それぞれのファイルは「ドキュメント」下に保存されるので、TeX の場所に移動する
  - ○ TeX でのファイルの取込
    - ▹ 式のファイルの取込 : \input{expr.tex}
    - ▹ 図のファイルの取込 : \includegraphics{graph.eps}
  - ○ タイプセット / PDF への変換方法を身に付ける
    - ▹ platex foobar.tex : foobar.tex から foobar.dvi を作成する
    - ▹ dvipdfmx foobar.dvi : foobar.dvi から foobar.pdf を作成する

本日(2016/11/29)の予定

- 本日(2016/11/29)の予定
  - 暗号化と VeraCrypt
- 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 (2016/11/29) の課題

- 前回 (2016/11/22) の課題 (前々回の課題)
  - CST Portal に以下のファイを提出しなさい
    - ファイル名 : 20161122-QQQQ.tex (QQQQ は学生番号)
    - 表題 : TeX で Mathematica の図を利用する
    - 内容 : TeX で Mathematica で作成した図を利用する
    - 条件 : 名前と学生番号は自分のものにすること
    - 形式 : テキストファイル (sample-20161122.tex 参照)
- 今回 (2016/11/29) の課題 (二つあるので注意)
  - 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 : 20161129-QQQQ.hc (QQQQ は学生番号)
    - 詳しくは、配布した sample-20161129.hc の内容を参照
  - 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 : 20161129-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

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(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 (gpg)

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

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
    - ▹ 対称鍵を公開鍵暗号方式で暗号化

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
    - 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...

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
    - 右クリックメニューから、「管理者として実行」すること
  - 日本語化
    - [Settings] -> [Language] -> [日本語]
- [実習 1.2] VeraCrypt の動作確認
  - sample-20161129.hc をディスクトップにダウンロード
  - VeraCrypt を起動 (sample-20161129.hc をダブルクリックでもよい)
    - sample-20161129.hc を e: 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 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 / 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 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
  - 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 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 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 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
  - 20161129-QQQQ.hc を CST Portal に提出

実習 4: Kleopatra の利用 (1)

- [実習 4.1] Kleopatra のインストール
  - gpg4win-2.3.3.exe をダウンロードし、実行する
    - Kleopatra がインストールされる
- [実習 4.2] Kleopatra の起動 : [ウィンドウズボタン] -> [Kleopatra]
- [実習 4.3] 自分の Key Pair の作成
  - [File] -> [New Certificate..] -> 上をクリックして -> [Next]
    - Name : 名前 / Email : NuApps のメール / Comment : 不要(好きにして良い) -> [Next]
    - [Create Key] -> パスフレーズ(自分で決める)(->それでもこれを使う)->パスフレーズ(先刻決めた同じ物)
    - [Make a Backup Of Your key Pair] -> ASCII armor にチェック ->
    - フォルダを指定->[ディスクトップ]->QQQQ->[Enter]->[OK]->[OK]->[Finish]

実習 4: Kleopatra の利用 (2)

- [実習 4.4] 自分の公開鍵の取出し
  - [自分の鍵を選択(右クリック)]->[Export Certificates]->[ディスクトップ]->20161129-QQQQ.asc->[保存]
    - 出来たファイルを skype 等で、友達に送る / skype で送ってみよう
- [実習 4.5] 他人の公開鍵の取り込み
  - 鍵ファイルを Kleopatora に Drag&Drop する -> [Import Certicates] -> [OK]
    - 栗野の公開鍵(kurino-pubkey.asc) をダウンロードして取り込む
- [実習 4.6] 他人に暗号ファイルを送る
  - 平文のファイルを作る -> D&D -> [Encrypt] -> [Text output ASCII] -> [Next]
    - [送り先を選ぶ] -> [Add] -> [Encrypt] -> [Finish]
    - その人に暗号化したファイルを送る / skype で 栗野に送ってみよう
- [実習 4.7] 自分に届いた暗号ファイルの平文化
  - 暗号ファイルを D&D -> [Decrypt] -> [Decrypt] -> パスフレーズ
- [実習 4.8] 友人同士で、暗号化したファイルを交換してみよう