# コンピュータ概論 A/B

-- セキュリティ / 暗号化 --

数学科 栗野 俊一

# 伝言

## 私語は慎むように !!

- 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

# 追加のお知らせ

- 講議録画
  - 毎週、講議の内容が録画され Network 経由で公開されます。
  - URL

    http://10.9.74.133/video (学内からのみ)

    http://edu-gw2.math.cst.nihon-u.ac.jp:10082 (学外からも[暫定])
  - 認証(メモってよい:その内、情報センターの ID/PW にします)
    - ID: m23b
    - PW: 3cdfa4747

# 先週の復習

- 先週の内容
  - 講義
    - Mathematica による関数定義:関数の再帰的定義
    - コーディング:自然数 (ペアノの公理)の定義
- 講義内容
  - 関数の定義
    - 代入文によって関数の値が定義できる
    - パターン：具体的な方が選択される
    - 再帰的定義：関数の定義にこれから定義する関数が利用できる
  - コーディング
    - 新しい要素(集合)を、旧知の要素(集合)で表現する:なんでも表現可能
    - 新しい要素の操作は旧知の要素の操作で実現できる:なんでも実現可能
    - 計算機が「万能」な理由：万能エミュレーション機械

# 本日の予定

- 講義
  - セキュリティと暗号化
- 実習
  - [演習 1] truecrtpt のインストール
  - [演習 2] truecrtpt の使い方
  - [演習 3] 課題の作成

# 本日の課題 (2011/11/08)

- 先週 (2011/11/01) の課題
  - 次のファイルを提出しなさい
    - 表題 : ペアノの方法による「有理数の差」の関数 qsub を定義しなさい
    - ファイル名 : 20111025-QQQQ.nb (QQQQ は学生番号)
    - 詳しくは、配布した nat.txt/sample-20111101.nb の内容を参照
    - ファイル名が 20111025 (20111101 でない..)であることに注意
- 今週 (2011/11/08) の課題
  - 次のファイルを truecrypt のボリュームとして作成し、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 : 20111108-QQQQ.tc (QQQQ は学生番号)
    - 詳しくは、配布した sample-20111108.tc の内容を参照

# セキュリティホールの話

- □ セキュリティとは？
  - ○「安全性」の事
    - ▹ これが守られれば、安全？
- □ セキュリティを守るには
  - ○ 己を知り、敵を知り、地の理を得れば、百戦危うしからず？
    - ▹ 己を知り：自分が守りたいものはなに => 情報 / システム
    - ▹ 敵を知り：クラッカーは何を / どこ狙っている？
    - ▹ 地の理(?)：どうやれば、それを守る事ができる？
  - ○ コンピュータウィルス対策の例
    - ▹ 己：ウィルスに感染されない状況にしたい
    - ▹ 敵：ソフトウェアの穴(セキュリティホール)を狙っている
    - ▹ 地：ウィルス対策ソフト ( cf. MSE ) に導入
- □ セキュリティホール
  - ○ セキュリティが守られていない欠点
    - ▹ 人間は失敗が避けられないので、どうしてもできてしまう
    - ▹ 発見された時点で、それをふさぐ必要がある (update する)

# PC セキュリティ

- 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
    - ▷ その規則がわか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)
  - ○ 変化(操作)
    - ▷ 暗号化：平文を暗号文にすること
    - ▷ 平文化：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
    - ▷ 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ワードを設定する
    - 暗号化ボリュームは暗号化されていてパスワード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ワードが必要
    - マウントすると、ドライブ(USB メモリみたいなもの)になり、普通にファイルが扱える
    - 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ワード
  - 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、パスワードが必要
    - パスワードは、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 1: truecrypt

- [実習 1.1] 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 1.2] truecrypt の動作確認
  - sample-20111108.tc をディスクトップにダウンロード
  - truecrypt を起動 (sample-20111108.tc をダブルクリックでもよい)
    - sample-20111108.tc を d: にマウントする
    - パスワードは 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
  - 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 / パスワード : 自分で決める
- [実習 2.2] 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ワードを友人におくる
- [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ワードを利用して 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
  - truecrypt で、新規ボリュームを作成する
    - サイズ / ファイル名 / パスワード : message.txt を参照
- [実習 3.2] 課題の作成
  - truecrypt で、実習 2.1 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
  - 20111108-QQQQ.tc を提出