東京工芸大学　7月20日オープンキャンパス
体験イベント「暗号解読に挑戦」実行手順

コンピュータ応用学科　数値シミュレーション研究室

1. 準備

(1) パソコンの立ち上げ

(a) 電源をONにします。

(b) Enterキーを押し、次にCtrl,Alt,Deleteキーを一緒に押します。

(c) お渡しした「ユーザ名」、「パスワード」を入力します。

(d) お渡ししたCDディスクをパソコンにセットします。

(e) CDのOpen7-20のFactor及びRSAをMyvolume(Z)にコピーします。

(f) コマンドプロンプトを立ち上げ、画面上でcd RSAと打ち込みます。

2. イベント１（素数に挑戦）: Factorを使用

C言語で作成したfactor.exeで30桁の素数を見つけることに挑戦します。

30桁の整数なので40回程度挑戦すると素数が得られる可能性が大です。

(a) input.txtに30桁の数を書き込みます。最後は1,3,7,9のいずれかにします。

(b) factor.exeをダブルクリックします。

(c) factor.txtに素因数分解結果が得られます。結果は追加されていきます。

因数分解されていなければ素数。因数分解されていれば(a)から(c)を繰返します。

input.txtに複数個の値（各行ごと）を与えることができます。

3. イベント２（因数分解に挑戦）

(1) 合成数の作成： コマンドプロンプト(RSAを使用)

2個の素数を作成し、それを乗算して合成数を作成します。

素数の長さはビット数で与えます。1ビットは約0.3桁の10進数になります。

(a) java Prime2と画面上に入力します。

(d) 2個の素数の長さ(ビット数)を画面から与えます。

すると、合成数(乗算結果)が画面上に表示されます。

(2) 合成数の因数分解: Factorを使用

(a) input.txtにPrime2で得られた合成数をコピーで与えます。

(b) factor.exeをダブルクリックします。

(c) factor.txtに素因数分解結果が得られます。

4. イベント３（暗号化と復号化）：コマンドプロンプト(RSA を使用)

英数字の文章を暗号化し、またそれを復号化して元の文章に戻します。

(a) java RSA と画面上に入力します。

(b) 画面から暗号化する文章の最大文字数(20～35)を入れます。

(c) 画面から暗号文（英字、数字、スペース及び.,で作成)を入れます。

(d) 暗号化し、またそれを復号化したものが画面に表示されます。

5. イベント４（暗号解読に挑戦）

(1) イベント 4 の N の値の因数分解： Factor を使用

(a) input.txt に上記暗号化の N の値をコピーで与えます。

(b) factor.exe をダブルクリックします。

(c) factor.txt に素因数分解結果が得られます。

(2) 因数分解結果を使用して暗号解読：コマンドプロンプト(RSA を使用)

(a) java Decode と画面上に入力します。

(b) 画面から解読する暗号(イベント 4 の暗号文)をコピーで入力します。

(c) 画面から暗号化に使用した e をコピーで入力します。

(d) 画面から N を分解する 2 つの数をコピーで入力します。

(e) 画面に解読されたメッセージが表示されます。

(f) 解読されて、イベント４で与えた文章になっていることを確認しましょう。

6. 誕生日検索

3 億桁πの値から 8 桁の数(誕生日)の検索：CD ディスクの「π計算」を使用

(a) CD の Open7-20 のπ計算を開きます。

(b) Pisearch.exe をダブルクリックします。

(c) 1～2 分経過すると画面に「Input YYYYMMDD」と出力されます。

(d) あなたの誕生日又は調べたい 8 桁の数字を入れてください。

(d) 画面に小数点以下 3 億桁のπからの検索結果が出力されます。

(e) 続けて検索するときは「１」を、検索終了のときは「0」を入れてください。

(注) 今回は CD から直接検索しました。

CD を一度内部ファイルにコピーして使用すると高速(約 10 秒)となります。

そのときは、Pisearchf.exe を使用してください。

検索結果が「π計算」の中の Pi300M-001.txt に出力されます。