アルゴリズム論特論 （塩田）

2010年7月1日の課題

課題 RSA 暗号の秘密鍵を格納するファイル RSAS.txt には p, q, d の順で鍵が格納されていたが、うっかり d を消してしまった。

(1) p, q, e（ e は RSAP.txt の2番目の数 ）から d を正しく計算して RSAS.txt の3行目に書き加えよ

(2) RSAD.py を実行して暗号文ファイル RSACsh.jpg を復号せよ。

(3) 復号文ファイル RSADsh.jpg は何の画像か？

提出期限：7月8日（木） （ 512号室ポストまで ）

サンプルプログラム

http://lupus.is.kochi-u.ac.jp/~shiota/mc2010/ 配下に以下のプログラム・サンプルデータがある。

- 関数定義部（ 以下のプログラムで import ）
  crypto.py
- RSA 暗号のサンプルプログラム
  鍵生成 RSAK.py / 暗号化 RSAE.py / 復号化 RSAD.py
- RSA 暗号の暗号文ファイルの例
  RSACsh.jpg
- RSACsh.jpg の暗号化に用いた鍵ファイル
  公開鍵 RSAP.txt / 秘密鍵 RSAS.txt
  （ RSAS.txt の3行目欠落 ）

使い方 1° RSAK.py を実行し鍵サイズ（ビット長）を入力すると、鍵 p, q, n, e, d が生成され、ブロック長と公開鍵 n, e は RSAP.txt に、秘密鍵 p, q, d は RSAS.txt に格納される。

2° RSAE.py を実行し暗号化したいファイルのファイル名 hoge を入力すると、暗号文ファイルが RSAChoge という名前で作成される。
♠ ファイルはテキスト、画像、音声、何でも構わない。
♢ ドット等の特殊文字を含むファイル名は ’ ’ で括って入力せよ。
♣ 暗号化には 100KB で数十秒時間が掛かることがある。

3° RSAD.py を実行し復号化したいファイルのファイル名 hoge を入力すると（ RSAC は不要 ）、復号文ファイルが RSADhoge という名前で作成される。