アルゴリズム論特論（特講）（塩田）

2008年6月19日の課題

課題 RSA 暗号の秘密鍵を格納するファイル RSASecKey.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 RSAPubKey.txt の２番目の数 ）から d を正しく計算して RSASecKey.txt の３行目に書き加えよ

(2) RSADecode.py を実行して暗号文ファイル RSA_C_mg.gif を復号せよ。

(3) 復号文ファイル RSA_D_mg.gif は何の画像か？

提出期限：6月26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/mc08/ 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 ）
  crypto080619.py
- RSA 暗号のサンプルプログラム
  鍵生成 RSAKey.py / 暗号化 RSAEncode.py / 復号化 RSADecode.py
- RSA 暗号の暗号文ファイルの例
  RSA_C_mg.gif
- RSA_C_mg.gif の暗号化に用いた鍵ファイル
  公開鍵 RSAPubKey.txt / 秘密鍵 RSASecKey.txt
  （ RSASecKey.txt の３行目欠落 ）

使い方 1° RSAKey.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 を生成し、ブロック長と公開鍵 n, e を RSAPubKey.txt に、秘密鍵 p, q, d を RSASecKey.txt に格納する。

2° RSAEncode.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、暗号文ファイルを RSA_C_hoge という名前で作成する。
♠ 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° RSADecode.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（ RSA_C_ は不要 ）、復号文ファイルを RSA_D_hoge という名前で作成する。