アルゴリズム論特論（特講）　(塩田)

2008 年 6 月 26 日の課題

課題　● 今日のデモで用いた RSA 暗号攻撃のサンプルプログラムで遊んでみよ。

提出期限：7 月 3 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 （各サンプルプログラムで import ）
  crypto.py
- Fermat 法（２つの素因数 p, q が近いときに有効）
  FermatMethod.py
- $p-1$ 法（$p-1$ の素因数が全て小さいときに有効）
  p-1Method.py
- $p-1$, $q-1$ の素因数が全て小さいときに有効な方法
  SmallFactor.py
- $p-1$, $q-1$ の最大公約数が大きいときに有効な方法
  LargeGCD.py