アルゴリズム論特講 （塩田）

2008年7月10日の課題

課題 Pohlig-Hellman 法のサンプルプログラム ph.py を、

- $p-1$ の素因数の限界
- p のビット数

を変えて実行し、その有効範囲を探れ。

提出期限：7月17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がある。

- 関数定義部
  crypto.py
- Pohlig-Hellman 法のサンプルプログラム
  ph.py