アルゴリズム論特講 （塩田）

2007年5月17日の課題

課題 1．暗号関数定義部
http://lupus.is.kochi-u.ac.jp/~shiota/mc07/crypto070517.py
をダウンロードせよ。

2．crypto070517.py に

- ユークリッドのアルゴリズム拡張版（第3回の課題）
- 法演算関数 mod，modadd，modsub，modmul（第4回の課題）

を貼り付けよ。

3．法演算における逆数計算の雛形プログラム
http://lupus.is.kochi-u.ac.jp/~shiota/mc07/L05.py
をダウンロードせよ。

4．L05.py の未完成部分（ modinv ）を完成し実行して、単純検索との計算時間の違いを実感せよ。（待ってても答えが出ないときは適当に強制終了するように。）

提出期限：5月24日（木） （ 512号室ポストまで ）

参考 C言語での実装例は
http://lupus.is.kochi-u.ac.jp/~shiota/mc07/L05.c