アルゴリズム論特論（特講）　(塩田)

2008 年 5 月 15 日の課題

課題　1. 暗号関数定義部
`http://lupus.is.kochi-u.ac.jp/~shiota/mc08/crypto080515.py`
および、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/mc08/L05.py`
をダウンロードせよ。

(`crypto080515.py` には

- 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）

が含まれているので、第 3 回・第 4 回の課題をまだやっていない諸君はそちらを先に。)

2. `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。また、検算が合っていることを必ず確認すること。）

提出期限：5 月 22 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/mc08/L05.c`