アルゴリズム論特論（特講）　(塩田)

2008 年 7 月 17 日の課題

課題

1. 以下のファイルをダウンロードせよ：
   - 関数定義部 crypto.py （ 前回までと同じ ）
   - 中国剰余アルゴリズムを利用した秘密分散スキームの復号プログラム SSDecode.py
   - 公開鍵のデータファイル SSKey.dat
   - 分散情報のデータファイル SSShare.dat
2. SSDecode.py を実行して分散情報からの復号を試みよ。

提出期限：7 月 24 日（木）　（ 512 号室ポストまで ）

参考
- 鍵生成プログラム SSKey.py
- 分散情報作成プログラム SSShare.py
- 中国剰余アルゴリズムを用いた秘密分散スキーム 多項式版の実行例 SSPol.txt

発展課題　SSKey.py のパラメータ （ 分割数 t，しきい値 k，ブロック長 sSize 等 ）の値を変えて、秘密分散実験を行え ：

1° SSKey.py を実行して鍵を生成 （ SSKey.dat が更新される ）

2° 平文のテキストファイル SSPlain.dat を作成

3° SSShare.py を実行して分散情報を作成 （ SSShare.dat が更新される ）

4° SSDecode.py を実行