

アルゴリズム論特論 (塩田)

2012年6月21日の課題(要提出)

- 課題 (1) <http://lupus.is.kochi-u.ac.jp/~shiota/mc2012/> から
crypto.py, RSAD.py, RSAP.txt, RSAS.txt, RSACphoto.jpg をダウンロードせよ。ただし crypto.py, RSAD.py 以外は学生ごとに異なるので注意。(それぞれの内容についてはホームページ参照。)
- (2) 秘密鍵を格納するファイル RSAS.txt には p, q, d の順で鍵が格納されるはずだが、わざと d を消してある。 p, q, e (e は RSAP.txt の3番目の数) から d を正しく計算して RSAS.txt の3行目に書き加えよ
- (3) RSAD.py を実行して暗号文ファイル RSACphoto.jpg を復号せよ。
- (4) 復号文ファイル RSADphoto.jpg は何の画像か?

提出期限: 7月12日(木) (512号室ポストまで)