アルゴリズム論特講 （塩田）

2008年7月3日の課題

課題
- 単純検索による離散対数計算プログラム DLP.py を実行して、何ビットまでが我慢の限界か試してみよ。

提出期限：7月10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 （ 前回と同じ ）
  crypto.py
- 単純検索による離散対数計算プログラム
  DLP.py
- 離散対数のデモプログラム
  DL.py
- Diffie-Hellman 鍵交換システムのデモプログラム
  DHKeyExchange.py