

アルゴリズム論特講 (塩田)

2007年6月28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5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/mc07/> 配下に以下のプログラムがある。

- 関数定義部 (前回と同じ)
`crypto070621.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`