高度セキュリティPBL2

28G23027　川原尚己

練習問題１

比較的処理に時間がかかる．例えば，完全準同型暗号では暗号文は「平文+ノイズ」という形で表され，演算処理を行う度にノイズが増加してしまう．復号ができなくなる前に「ブートストラップ」という処理によってノイズを除去する必要があるが，この処理に非常に時間がかかり，効率が悪い．

練習問題２

（講義資料42ページ）

一般のの場合，行列が上記の形になることを示せ．

**回答**

に対し，

となるようなを考える．において，の次数が及びとなるときにに関係することに注意すると，は以下のように表すことができる．

以上より，が問題文のように書けることがわかる．

練習問題３

以上の(i),(ii)を示せ．

**回答**