コンテンツセキュリティ実験 追加課題

情報理工学域　II類
渡邉洋平　阿波拓海　淺野京一

追加課題 1

最初に乱数行列を共有する際，特殊な行列（単位行列など）を使用した場合に，計算過程から互いのテーブルが漏洩してしまう可能性があります．この問題点を改善するために，次のような処理を加えてください．

1. 中学側は，整数の 6×6 乱数テーブルを作成し，それらのハッシュ値を計算し，
   6×6 のハッシュ値テーブルを得る．
2. 中学側は，予備校側に対して，乱数テーブルとハッシュ値テーブルの両方を送る．
3. 予備校側は，乱数テーブルをキーとしてハッシュ関数に入力し，
   その出力テーブルが受け取ったハッシュ値テーブルと一致することを確認する．
4. 以降，ハッシュ値テーブルを乱数テーブルとして，アルゴリズムを実行する．

使用するハッシュ関数については，既存の Java ライブラリを使用して頂いて構いません．
作成したプログラムは，kadai3 フォルダに格納し，programs の下に格納してください．

追加課題 2

上記の改善を加えても，互いのテーブルを任意の大きさに拡張した場合（k×m と m×l），セキュリティには未だ問題点が残されています．問題点の考察と，解決方法の提案を行い，レポートに追加記述してください．