CMSC 414 Spring 2001
Individual Course Project Description

This document describes the requirements for the individual course project for CMSC 414 (Spring 2001).

Your task is to design and implement a means to play cards via a network. Your protocol should support an arbitrary number of players, but in practice you may assume that at most only four players will ever play in the same game.

The next section details the specific requirements for the project. Finally, we conclude with deliverable instructions.

NOTE: Attached to this handout is a Xerox from Applied Cryptography explaining how to do Coin Flipping Using Public-Key Cryptography.

1 Requirements

The following are the requirements for the individual project:

1. It is your choice as to what card game your system will play. All that is required is that ALL players can determine the same winner when presented with the results of the game.

2. The implementation must be written in Java 1.3 using the IAIK JCE cryptographic toolkit. The IAIK toolkit is free for educational use and can be found at `http://jcewww.iaik.tu-graz.ac.at/download.html`. You want to download version 2.61 of the IAIK-JCE. IAIK supports both UNIX and Windows.

3. Your implementation must use the network to communicate. We will provide a simple client/server example after spring break to assist you if needed. Our code will allow you to send *blobs*[1].

4. It must not be possible for a player (including the dealer) to cheat in any way. At the end of each hand, each player must validate the results to ensure fairness.

2 Deliverables

The following are the deliverables for the project along with their due dates.

1. **Design Document.** Your design document will include the following sections:

[1] Blob is slang for a bit-string

(a) *Introduction.* You must introduce and explain the problem you are trying to solve.

(b) *Assumptions.* You must explicitly state your assumptions.

(c) *Design.* You must explicitly describe your design such that a classmate could implement it, i.e. you must show and explain the format of your messages, and you must show the message flow (think of the Bob and Alice diagrams in class).

(d) *Security Analysis.* You must perform a security analysis of your design. This analysis **must** include an attack tree.

(e) *Testing methodology.* Explain how you plan on testing the design and the implementation.

(f) *Conclusions.*

The hardcopy of your design document is due April 5, 2001 at the beginning of class. *NOTE: Your implementation may deviate from your design document, but you MUST document the reasons for the deviation in the source code.*

The design document is an extremely important part of this project. The project itself is relatively simple given the information provided in class.

2. **Source code.** The complete and commented source code for your project must be emailed to cmsc414@cs.umd.edu by midnight May 18, 2001. You must Winzip or tar the files into an archive with your name as the filename, e.g. smith.zip. You must include a README file that provides detailed step by step instructions on how to install and use your system.

3. **Testing results.** Explain how you tested the system and show transcripts of the tests. This description must be placed in an electronic file and included with the source code archive above before submission on May 18.