The University of North Carolina at Greensboro
CSC 580: Cryptography and Security in Computing
Prof. Stephen R. Tate

Handout 2
January 17, 2017

CSC 580 Ongoing Project – Basic Information

During the course of the semester, you will develop the core communication/management library for a secure online chat system. This library will be implemented in Java, using the Java Cryptography Architecture (JCA), which is standard and common across desktop, server, and mobile Java platforms (including Android). The project is broken into pieces, assigned every 2–3 weeks, that will involve design and analysis of security and efficiency, experimental testing of algorithms and JCA components to aid in design decision-making, and implementation of core functionality. The project will focus on information and communication issues, and we will not spend time working on a user interface. You can view this as a secure communication library that could be used by any user front-end. The chat clients will make use of a "chat hub," which is a server that can connect and provide services to users. The exact functionality and trust requirements of the hub will be determined in the design phase.

There are certain requirements that the system must meet, as well as some decisions that will be made after in-class discussion. At each "decision point" we will take the best ideas from the class, and standardize on that design for everyone moving forward.

Security Requirements: The system must

- Support message sizes from small SMS-sized text messages to large multimedia messages (e.g., pictures)
- Protect the confidentiality of messages so that only the intended recipients can get any meaningful information about message contents
- Protect the integrity of messages so that the recipient has assurance that the message they view is the same message the sender sent
- Provide assurance that the person you are chatting with is the person you are intending to chat with

Other Considerations: Questions to resolve through class discussion include

- How much should the chat hub be trusted with identities and keys?
- Is there a way to securely back up secret keys and identities?
- Should the system disguise who is chatting with whom?
- Should it be possible to see old messages (technically, do we provide forward security)?