Assignment 3: Protocol Design and Analysis

1 Problem

You are to write a design document for a “secure” multiparty chat protocol. Your design document should specify which security properties your protocol achieves. The document should also provide an analysis detailing how these security properties are achieved. Include a discussion of the mayhem different kinds of adversaries (Eve, Mallory) could cause in your system.

Detail the protocol for users discovering, joining and leaving the chat; detail messages for determining members currently participating in the chat and sending messages to individual members or the entire group in the same style as used in the textbook. Your particular protocol may not require or support every single one of these operations; your design document only needs to specify the required operations.

It is up to you to decide which security properties your protocol is supposed to provide. You will be graded on correctness (of the design), quality of the security analysis, simplicity of the design, scope of the chosen security properties and protocol efficiency.

Suggested security properties include (in no particular order):

- Message integrity
- Message authenticity
- Message confidentiality
- Message ordering / timestamping
- Nonrepudiation – or repudiation
- Anonymity

Note that you should define precisely what the meaning of these security properties is in the context of your protocol.

2 Submission

You must submit the design and analysis in LaTeX format to your subversion repository to the directory `courses/comp3704/s2007/$USER/p3/`. Do not include generated files.

- `protocol.tex`
- `Makefile`

You must check that the submitted LaTeX file compiles by invoking `make`, producing a file `protocol.pdf` (use `pdflatex` in your makefile).