Name .... ID .... Section ...... Seat No ......

Sirindhorn International Institute of Technology
Thammasat University

Final Exam: Semester 2, 2013

Course Title: CSS322 Security and Cryptography

Instructor: Steven Gordon

Date/Time: Thursday 13 March 2014; 13:30–16:30

Instructions:

- This examination paper has 17 pages (including this page).
- Conditions of Examination: Closed book; No dictionary; Non-programmable calculator is allowed
- Students are not allowed to be out of the exam room during examination. Going to the restroom may result in score deduction.
- Turn off all communication devices (mobile phone etc.) and leave them at the front of the examination room.
- The examination paper is not allowed to be taken out of the examination room. A violation may result in score deduction.
- Write your name, student ID, section, and seat number clearly on the front page of the exam, and on any separate sheets (if they exist).

CSS322 2013 Final Exam Hints

- 10 questions, each with multiple parts
- 100 marks total
- Covering topics:
  - Diffie-Hellman (from Public Key Crypto)
  - Message Authentication Code, e.g. general authentication concepts, use of MACs for authentication
  - Hash Functions, e.g. properties, requirements, use for authentication
  - Firewalls, e.g. packet filtering firewall rules, SPI
  - Key Management and Distribution, e.g. key hierarchies, different distribution schemes, certificates
  - Passwords, e.g. entropy, password storage, password selection, attacks
- Specific topics NOT in the exam:
  - Rainbow tables and detailed analysis of why salted passwords prevent them being used
  - Firewall proxies
  - Algorithms/steps for attacks on MACs
- If there is a question about a specific algorithm, authentication scheme or key distribution scheme, I provide (full or partial) details of the algorithm/scheme in the question. That is, you don't need to memorise the schemes; you just need to be able to interpret and understand them.
- Use past exams and quizzes as practice, but note that in previous years, different topics may have been covered than this year (e.g. this year we covered firewalls, but did not cover malicious software or transport security).
- A calculator is recommended.