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

Sirindhorn International Institute of Technology
Thammasat University

Final Exam: Semester 2, 2014

Course Title: CSS322 Security and Cryptography

Instructor: Steven Gordon

Date/Time: Friday 15 May 2015; 13:30–16:30

Instructions:

- This examination paper has 22 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 Final Exam Hints

- 9 questions, each with multiple parts
- 90 marks in total
- Covered topics:
  - Diffie-Hellman (from Public Key Cryptography)
  - MAC and Authentication
  - Hash Functions
  - Key Distribution
  - Internet Security: SSL and SSH
- In Authentication topics (MAC and Hash) there were many pictures in the lecture slides show different schemes (e.g. source A takes message M, calculates H and concatenates with M, then sends to B). You do not need to memorise these schemes. However there may be questions that show these (or similar schemes) and will require you to answer questions about it. Same applies for Key Distribution topics.
- Past exams are excellent practice and examples of questions. Note however past years included topics of firewalls and passwords - we did not cover these topics this year.
- Quizzes and homeworks are good practice and examples of questions
- A calculator is recommended