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

Sirindhorn International Institute of Technology
Thammasat University

Final Exam: Semester 2, 2012

Course Title: CSS322 Security and Cryptography

Instructor: Steven Gordon

Date/Time: Friday 1 March 2013; 13:30–16:30

Instructions:

- This examination paper has 18 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.
- 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).
- The examination paper is not allowed to be taken out of the examination room. A violation may result in score deduction.

CSS322 Final Exam Hints 2012

- 9 questions, each with multiple parts
- 90 marks in total
- Covers topics after midterm, including:
  - Public key crypto
  - Authentication
  - Hash functions
  - MAC functions
  - Key Management
  - Passwords
  - Transport Layer Security
- Does NOT cover topics skipped during lecture, including:
  - Malicious software
- You should know and understand how important algorithms/ciphers work, e.g. RSA, Diffie-Hellman
- You should know and understand concepts, advantages, disadvantages of different ciphers, protocols, mechanisms and techniques
- You do NOT need to remember the exact protocols and mechanisms for authentication and key management. Specifically, the diagrams for message authentication (like on slide 6 of Cryptographic Hash Functions) and for key management (like on slide 24 of Key Management) will be given if necessary.
- Details of SSL and SSH (such as the message types, header sizes and exact sequence of messages) do NOT need to be memorized.
- Use past exams and quizzes as study material