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

Sirindhorn International Institute of Technology
Thammasat University

Final Exam: Semester 2, 2010

Course Title: CSS322 Security and Cryptography

Instructor: Steven Gordon

Date/Time: Wednesday 2 March 2011; 9:00–12:00

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.
- Students are not allowed to have communication devices (e.g. mobile phone) in their possession.
- 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 2010

- 10 questions, each with multiple parts
- Total marks: 75
- Covers topics from after midterm:
  - RSA and public key crypto
  - Diffie Hellman
  - Hash functions
  - Digital signatures
  - MAC functions
  - Authentication
  - Key management
  - Certificates
  - SSL, HTTPS, SSH
  - Viruses
  - DDoS
- Some basic knowledge from topics before midterm is assumed (e.g. security services, mod arithmetic)
- Topics (from previous years) not covered: IPsec, VPNs, Buffer overflow attacks, firewalls
- Use previous years exams and quizzes for study
- Most, if not all exam questions this year are new (compared to previous years); but still covering same concepts
- At least 1 question refers to a tcpdump/Wireshark packet capture