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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Exam: Semester 2, 2010

Course Title: CSS322 Security and Cryptography

Instructor: Steven Gordon

Date/Time: Wednesday 29 December 2010; 9:00–12:00

Instructions:

- This examination paper has 11 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).
- The space on the back of each page can be used if necessary.

CSS322 Midterm Hints

- 3 hour exam
- 9 questions, each with multiple parts
- 70 marks
- Covering topics up until and including Public Key Cryptography (but NOT including RSA, that is, slide 16 and onwards are NOT covered)
- You must remember classical ciphers (there will be at least one questions on one of the following: Caesar, monoalphabetic, Vigenere, OneTimePad, Rows/Column, RailFence, Playfair).
- You must remember the modes of operation covered in lecture (ECB, CBC, CTR). However there is NO question on CFB or OFB.
- You DO NOT have to remember details of DES, S-DES or RC4. They would be given. You do need to know how to apply them.
- You DO NOT have to remember Fermat's theorem or Euler's theorem. They would be given.
- Previous exams give a good indication of the types of questions.