Mã hóa thông tin và Ứng dụng

PGS.TS. Trần Minh Triết

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Giới thiệu chung

- Môn học này nhằm cung cấp cho các sinh viên:
  - các kiến thức cơ bản và nền tảng về kiến trúc, tính chất, ý nghĩa và công dụng của các nhóm thuật toán chính trong lĩnh vực an toàn thông tin (mã hóa đối xứng, mã hóa bất đối xứng, chữ ký điện tử, hàm băm mật mã);
  - trình bày và phân tích một số bài toán và giải pháp phổ biến trong lĩnh vực an toàn thông tin (trao đổi khóa, chứng nhận khóa công khai, an toàn thông tin trong giao dịch trên mạng, quản lý định danh, bảo vệ tính riêng tư).

Mục tiêu môn học

- Sinh viên nắm vững được tính chất, ý nghĩa và công dụng của các nhóm thuật toán chính trong lĩnh vực an toàn thông tin : mã hóa đối xứng, mã hóa bất đối xứng, chữ ký điện tử, hàm băm mật mã.
- Sinh viên có khả năng phân tích yêu cầu bảo vệ thông tin trong hệ thống phần mềm, từ đó có khả năng thiết kế giải pháp, giao thức, quy trình để bảo vệ thông tin trong hệ thống phần mềm.
- Sinh viên có khả năng phân tích, đánh giá ưu điểm và hạn chế của các giải pháp, giao thức, quy trình bảo vệ thông tin trong hệ thống phần mềm.

Giới thiệu chung

- Trình độ: Sinh viên năm 3-4
- Số tín chỉ: 4
- Thời lượng lý thuyết: 45 tiết

Hình thức kiểm tra

- Lý thuyết: 50%
  - Câu hỏi trắc nghiệm + Bài tập (đề đóng)
- Bài tập trong quá trình học: 10%
  - ~2-10 bài tập nhỏ
  - Dành cho mỗi sinh viên
  - Nộp theo cột mốc quy định trong học kỳ
- Đồ án thực hành cuối khóa: 15%
  - Làm theo nhóm (tối đa 2SV)
- Đồ án lý thuyết giữa kỳ: 15%
  - Làm theo nhóm (tối đa 2SV)
- Tìm hiểu các chuyên đề mới: 10%
  - Nhóm gồm tối đa 4 SV
  - Những nhóm tìm hiểu tốt được chọn trình bày seminar

Nội dung (1)

- Chủ đề 1: Tổng quan về An toàn thông tin & Ứng dụng
- Chủ đề 2: Các hệ thống mật mã đối xứng (cổ điển)
- Chủ đề 3: Lý thuyết Shannon
- Chủ đề 4: Các hệ thống mã hóa đối xứng mới (DES, AES…)
- Chủ đề 5: Các chế độ hoạt động, các chiến lược padding
- Chủ đề 6: Các hệ thống mật mã bất đối xứng
- Chủ đề 7: Chữ ký điện tử
- Chủ đề 8: Hàm băm mật mã
- Chủ đề 9: Chứng nhận khóa công
- Chủ đề 10: Secured Socket Layer

Nội dung (2)

- Chủ đề 11: Phân tích yêu cầu, thiết kế quy trình, giao thức bảo vệ thông tin trong hệ thống phần mềm
- Chủ đề 12: Một số giao thức trong mạng không dây (WEP, WPA, WPA2…)
- Chủ đề 13: Tính riêng tư
- Chủ đề 14: Một số vấn đề khác (Single Sign-On, Trust Negotiation, Kerberos, Blind-Signature, e-Voting, e-Cash…)

Tài liệu tham khảo

- Dương Anh Đức, Trần Minh Triết, *Mã hóa và Ứng dụng*, NXB Đại học Quốc gia, 2005
- Bùi Doãn Khanh, Nguyễn Đình Thúc, *Mã hoá thông tin : phương pháp và ứng dụng*, 2005

Tài liệu tham khảo

- Douglas R. Stinson, Cryptography – Theory and Practice, 3rd edition, CRC Press, 2005.

  http://www.cacr.math.uwaterloo.ca/~dstinson/CTAP3/CTAP3.html

- William Stallings, Cryptography and Network Security: Principles and Practice, 5th Edition, Prentice Hall, 2005.

  http://williamstallings.com/Crypto/Crypto5e.html

- Alfred J. Menezes, Paul C. van Oorschot , Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997

  http://cacr.math.uwaterloo.ca/hac/

- Bruce Schneier, Schneier on Security, Wiley, 2008

  http://www.schneier.com/book-sos.html

Tài liệu tham khảo

- Rolf Oppliger, Contemporary Cryptography, Artech House Publishers, 2005

  http://www.esecurity.ch/Books/cryptography.html

- Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2009

  http://wiki.crypto.rub.de/Buch/slides_movies.php

- Phil Windley, Digital Identity, O'Reilly, 2005

  www.windley.com/

- Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography, Chapman and Hall/CRC Press, August 2007.

  http://www.cs.umd.edu/~jkatz/imc.html

Tài liệu tham khảo

- Henk van Tilborg (Editor), Encyclopedia of Cryptography and Security , Springer-verlag, 2005

  http://www.springer.com/computer/security+and+cryptology/book/978-0-387-23473-1

- Oded Goldreich, Foundations of Cryptography: Basic Tools. Cambridge University Press.

  http://www.wisdom.weizmann.ac.il/~oded/foc-book.html

- Bruce Schneier, Applied Cryptography (Second Edition), John Wiley & Sons, 1996

  http://www.schneier.com/book-applied.html