Giới thiệu môn học Lý thuyết mã hoá thông tin

ThS. Nguyễn Thành Nhựt

Trường ĐH Khoa học Tự nhiên - ĐHQG TP. HCM

Ngày 20 tháng 9 năm 2009

Giới thiệu môn học

1. Tên môn học
   - Lý thuyết mã hoá thông tin (Cryptography).
   - Thám mã (Cryptanalysis).
   - Mật mã học (Cryptology).
2. Thuộc lĩnh vực
   - Toán học (Đại số - Lý thuyết số).
   - Khoa học máy tính (Bảo mật thông tin, Lý thuyết thông tin, Thuật toán và độ phức tạp thuật toán).
3. Kiến thức tiên quyết
   - Toán cao cấp.
   - Số học thuật toán.
   - Đại số đại cương.
   - Cấu trúc dữ liệu và thuật toán.
   - Lập trình tính toán.

Nội dung môn học

- Các khái niệm cơ bản của Lý thuyết mật mã và ứng dụng trong Bảo mật thông tin
  1. Các hệ mã cổ điển.
  2. Hệ mã DES và hệ mã RSA.
  3. Số học thuật toán về số nguyên tố.
  4. Hệ mã ElGamal và bài toán logarit rời rạc.
  5. Hệ mã dùng đường cong elliptic.
  6. Các giao thức ký số.
  7. ...
- Tài liệu
  1. Douglas R. Stinson, *Cryptography: Theory and Practice*, 3rd ed., Chapman & Hall/CRC, 2006.
  2. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2001.
  3. Neal Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed., Springer, 1994.

Tổ chức lớp học

- 15 buổi học trên lớp (Từ tuần 7/9 đến tuần 14/12/2009). Sáng thứ bảy, từ 9g10 đến 11g20 phòng E401.
- Học theo nhóm tối đa 3 SV/nhóm.
- Tin tức môn học được post trên trang web `http://sites.google.com/site/nhutcourses/`.
- Trao đổi học tập trên forum `http://www.toantin.org`.

Đánh giá kết quả học tập

1. Trong quá trình học (70%, tính theo nhóm)
   - Thi giữa kỳ (20%).
   - Bài tập lý thuyết và thực hành (25%).
   - Thuyết trình nhóm (25%)
2. Thi cuối kỳ (50%, cá nhân)

Mục tiêu học tập

1. Kiến thức
   - Các khái niệm và kỹ thuật mã hoá cơ bản trong mật mã học.
   - Các bài toán quan trọng trong mật mã học.
   - Nguyên lý hoạt động của các ứng dụng trong thực tế.
2. Kỹ năng
   - Học nhóm.
   - Thu thập và xử lý thông tin.
   - Lập trình tính toán.
   - Trình bày kết quả nghiên cứu.
   - Đọc viết tiếng Anh.

Phương pháp học tập

Quy luật 80/20

1. Tự học (80%)
   - Đọc sách tại nhà và thư viện.
   - Tra cứu thông tin trên internet (Google) khi gặp vấn đề mới.
   - Trao đổi học hỏi trên diễn đàn môn học với thầy và bạn.
   - Email / gặp trực tiếp hỏi chuyên gia trong và ngoài nước.
   - Tìm đọc hiểu và tự cài đặt các thuật toán.
   - Tham gia các semina có liên quan đến môn học.
   - Để ý các thông tin thời sự liên quan đến môn học.
   - Cố gắng đọc, viết, nghe, nói bằng tiếng Anh.
2. Nghe giảng, ghi chép tại lớp.
3. Cập nhật thông tin môn học.

Công cụ học tập

1. Phần mềm
   - Cryptool (`www.cryptool.org`).
   - Maple/Mathematica, Python.
   - Các thư viện mã hoá bằng C++/Java.
   - Internet.
2. Phần cứng
   - Máy vi tính.
   - Tài liệu.

Các khái niệm mở đầu

Định nghĩa

1. *Lý thuyết mã hoá (Cryptography)* nghiên cứu các kỹ thuật toán học liên quan đến các yếu tố của *bảo mật thông tin (information security)*.
2. *Thám mã (Cryptanalysis)* nghiên cứu các kỹ thuật toán học nhằm tấn công (phá) các kỹ thuật mã hoá.
3. *Mật mã học (Cryptology)* nghiên cứu cả mã hoá lẫn thám mã.

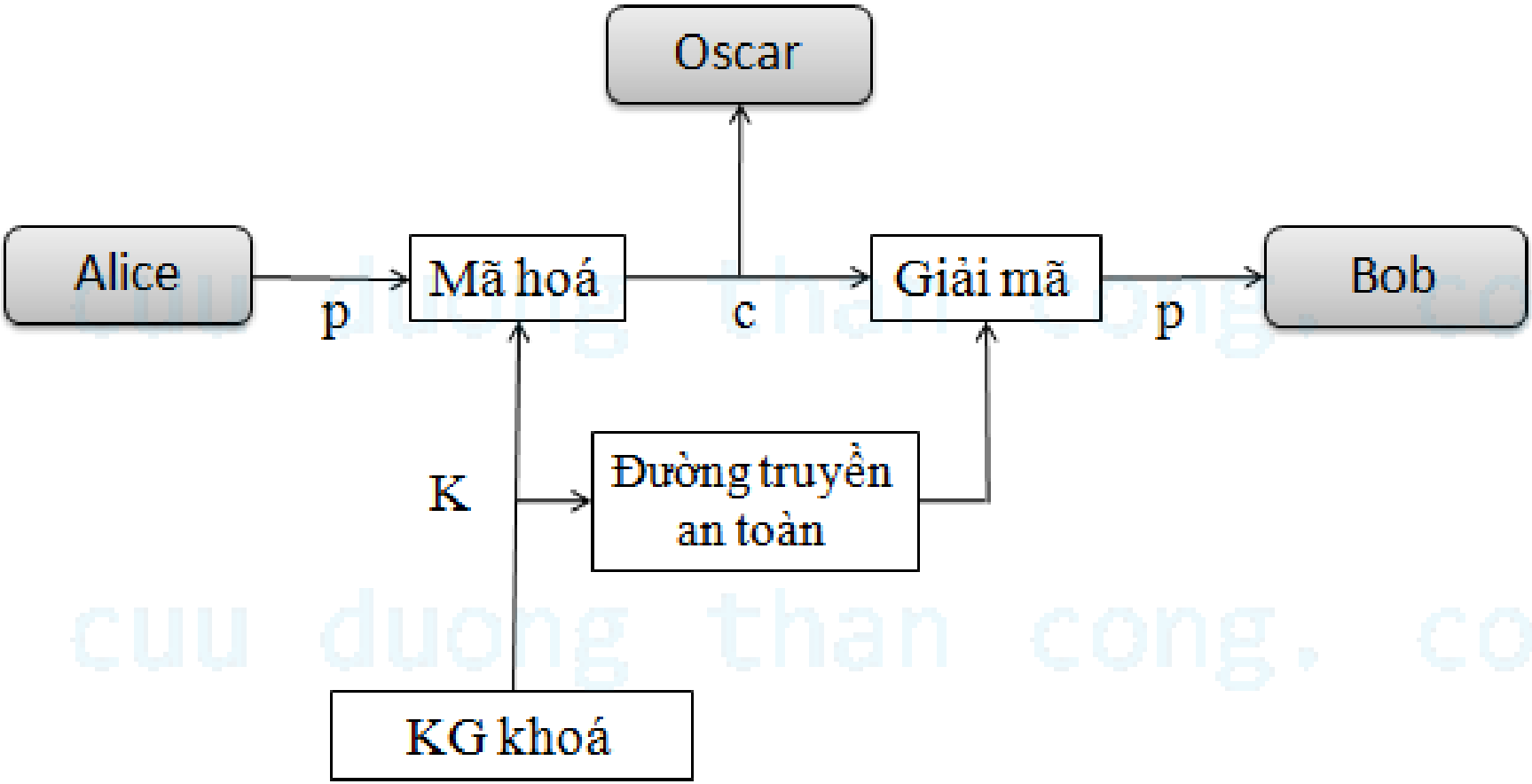
- Mục đích của việc mã hoá thông tin có thể là *bảo mật (privacy/confidentiality)*, đảm bảo *tính toàn vẹn dữ liệu (data integrity)*, tính *xác thực (authentication)*, hay *nhận diện (identification)*, ...
- Mục đích cơ bản của mật mã học là cho phép sự trao đổi thông tin giữa hai người được bảo mật trên các kênh truyền không an toàn.
- Một người bất kỳ khác nếu lấy được thông tin mã hoá đang truyền thì vẫn không hiểu được.

Các khái niệm cơ bản

Định nghĩa

- Thông tin mà một người A muốn gửi cho một người B được gọi là *văn bản gốc (plaintext)* hay *thông điệp (message)*.
- *Người gửi (sender) mã hoá (encrypt)* thông điệp bằng một *khoá (key)* (được thống nhất trước với người nhận) và gửi *văn bản mã (ciphertext)* cho *người nhận (receiver)*.
- B đã thống nhất trước với A khoá K nên có thể *giải mã (decrypt)* văn bản mã trở lại thông điệp.

Mô hình trao đổi thông tin mật



Hệ mã

Định nghĩa

Một *hệ mã (cryptosystem)* là một bộ năm (P, C, K, E, D) thoả các tính chất sau:

- P là tập hữu hạn các thông điệp.
- C là tập hữu hạn các văn bản mã.
- K, *không gian khoá (keyspace)*, là tập hữu hạn các khoá có thể có.
- Với mỗi khoá $k \in K$, có một *phép mã hoá (encryption)* $e_k \in E$ và một *phép giải mã (decryption)* $d_k \in D$. Mỗi phép mã hoá $e_k : P \longrightarrow C$ và phép giải mã $d_k : C \longrightarrow P$ xem như các hàm số thoả $d_k(e_k(x)) = x$ với mọi văn bản $x \in P$.

Thông tin về mật mã học

- Từ khoá "cryptography".
- Trang web `iacr.org`.
- Triển vọng nghề nghiệp
  - *Nhà mật mã học (cryptanalyst)* là một nghề 'hot' nhất hiện nay ở các nước phát triển, đặc biệt ở Mỹ.
  - Chuyên gia bảo mật tại các công ty lớn, ngân hàng, các ngành nghề có thanh toán điện tử, dịch vụ web, ... và đặc biệt là trong an ninh quốc phòng.
  - Chuyên gia nghiên cứu làm việc tại các trường đại học lớn trên thế giới.
- Nghiên cứu
  - Mật mã học có các hướng nghiên cứu rất đa dạng và phong phú, từ lý thuyết đến ứng dụng rất hấp dẫn, thu hút nhiều nhà toán học và khoa học máy tính.
  - Có nhiều nhóm nghiên cứu, tạp chí chuyên ngành và hội nghị quốc tế hoạt động rất sôi nổi.

Một số địa chỉ quan trọng

- *Hiệp hội quốc tế về nghiên cứu mật mã (International Association for Cryptologic Research)* `http://www.iacr.org/`. Thông tin về:
  - Các hội nghị, hội thảo, sự kiện quốc tế quan trọng về mật mã hàng năm.
  - Các tạp chí quốc tế chuyên về mật mã.
  - Chia sẻ các bản thảo bài báo mới.
  - Nghề nghiệp, học bổng sau đại học.
- Free book *Handbook of Applied Cryptography* `http://www.cacr.math.uwaterloo.ca/hac/`