Mật mã và độ phức tạp thuật toán (Complexity and Cryptography) Chủ đề 0: Giới thiệu học phần MI4100

PGS.TS. Nguyễn Đình Hân
(Mobile: 0915.046.320; Email: han.nguyendinh@hust.edu.vn)

Viện Toán ứng dụng và Tin học
Trường Đại học Bách khoa Hà Nội

Giới thiệu học phần MI4100

1. Giới thiệu học phần
   - Vai trò và ý nghĩa của học phần
   - Cơ hội việc làm
   - Mục tiêu của học phần
   - Nội dung của học phần
   - Tài liệu học tập
2. Các chủ đề tiểu luận

Giới thiệu học phần

Lý thuyết tính toán (Theory of computation) có 3 lĩnh vực truyền thống, trọng tâm:

- Lý thuyết ôtômat/otomat (Automata theory): đề cập đến việc xây dựng các mô hình toán học về tính toán.
- Lý thuyết về khả năng tính toán (Computability theory): có mục tiêu là phân chia các bài toán thành lớp các bài toán giải được và lớp các bài toán không giải được.
- Lý thuyết độ phức tạp tính toán (Complexity theory): phân chia các bài toán giải được thành các lớp khác nhau theo mức độ khó khăn khi giải chúng.

Giới thiệu học phần

Sự ra đời và phát triển của Lý thuyết độ phức tạp tính toán:

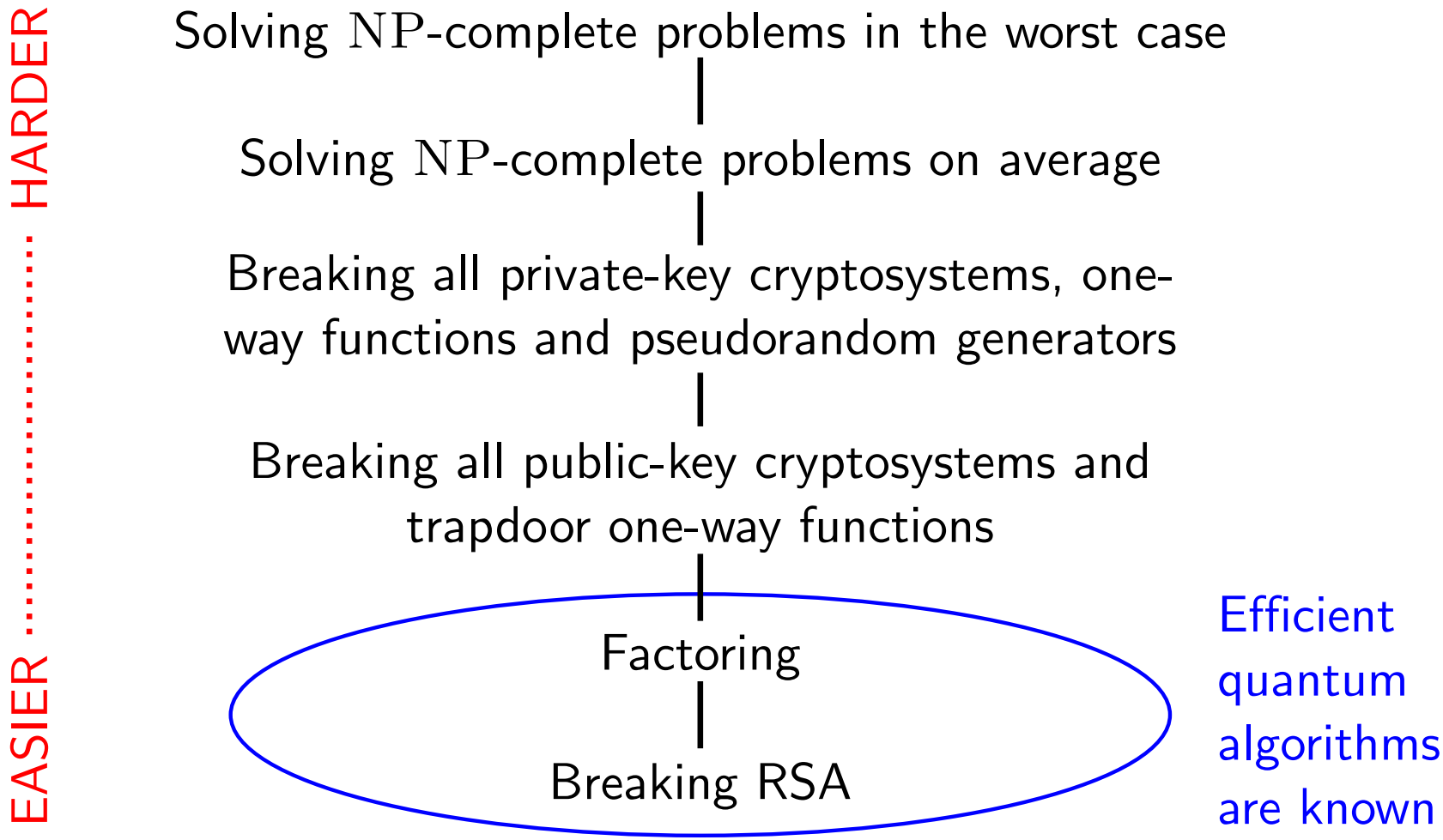
> Những năm 40 và 50 của thế kỷ XX:

- Những kết quả sâu sắc về các bài toán không giải được
- Sự triển khai những tư tưởng về các mô hình lý thuyết của máy tính
- Sự ra đời của máy tính thực tế

> Cuối thập niên 60 của thế kỷ XX:

- Lý thuyết độ phức tạp tính toán được hình thành
- Khám phá sự phụ thuộc giữa "kích cỡ" của bài toán với thời gian thực hiện thuật toán cũng như dung lượng bộ nhớ mà máy tính cần sử dụng
- Có được cách nhìn thống nhất về độ phức tạp của các thuật toán

Giới thiệu học phần



Hình 0.1 Mối liên hệ giữa độ phức tạp tính toán và mật mã

Vai trò và ý nghĩa của học phần

Mật mã và độ phức tạp thuật toán là học phần cơ sở, bắt buộc của chương trình đào tạo. Học phần này được thiết kế với mục đích:

- Cung cấp kiến thức nền tảng về lý thuyết độ phức tạp tính toán, lý thuyết mã và ứng dụng của các lý thuyết này trong lĩnh vực biểu diễn thông tin, mật mã, truyền thông dữ liệu.
- Giới thiệu những kết quả, thành tựu tiêu biểu của mật mã học trong việc bảo đảm an ninh, an toàn thông tin.
- Trang bị những hiểu biết liên quan đến các tiêu chuẩn, công nghệ mật mã; cách thức thiết kế, cài đặt các hệ mật và các giao thức bảo mật; phân tích, đánh giá hiệu quả hoạt động cũng như độ an toàn của các hệ mật và các sơ đồ ứng dụng mật mã.

Cơ hội việc làm

Highly skilled security professionals are in high demand. No organization is immune to cybercrime, meaning that all need to make computer security a top priority. The first step is finding the most qualified professionals to lead the way.

SIMPLILEARN, *https://www.simplilearn.com/*

- Vai trò của chuyên gia bảo mật? Thu nhập?
- Công việc/trách nhiệm của chuyên gia bảo mật?
- Các kỹ năng cần có? Chứng chỉ bảo mật?

Mục tiêu của học phần

Sau khi kết thúc Học phần, người học có khả năng:

(1) Trình bày được cơ sở toán học và ứng dụng của lý thuyết độ phức tạp tính toán, lý thuyết mã;

(2) Nêu được vai trò của lý thuyết độ phức tạp tính toán, lý thuyết mã đối với sự phát triển của mật mã học;

(3) Ứng dụng các kết quả, thành tựu của lý thuyết độ phức tạp tính toán, lý thuyết mã để thiết kế, triển khai các hệ mật, các giao thức bảo mật; các sơ đồ ứng dụng mật mã trong biểu diễn thông tin và truyền thông dữ liệu;

(4) Phân tích, đánh giá hiệu quả hoạt động, độ an toàn của các hệ mật và các sơ đồ ứng dụng mật mã;

(5) Tư vấn về các giải pháp ứng dụng mật mã trong bảo vệ thông tin, hệ thống thông tin của các tổ chức, cá nhân.

Nội dung của học phần

Nội dung của học phần được cấu trúc thành các chủ đề (nhưng không hạn chế) bao gồm:

- Lý thuyết độ phức tạp tính toán và ứng dụng;
- Lý thuyết mã và ứng dụng;
- Các hệ mật khóa đối xứng;
- Các hệ mật khóa công khai;
- Các sơ đồ ứng dụng mật mã;
- Tấn công thám mã.

Tài liệu học tập/tham khảo

Giáo trình:

1. John Talbot and Dominic Welsh (2010) *Complexity and Cryptography: An Introduction*. Cambridge University Press.

Sách tham khảo:

2. Douglas R. Stinson (2019) *Cryptography Theory and Practice*. Fourth Edition. Taylor & Francis.
3. William Stallings (2017) *Cryptography and Network Security: Principles and Practice*. Seventh Edition. Pearson Education, Ltd.
4. J. Berstel, D. Perrin and C. Reutenauer (2010) *Codes and Automata*. Cambridge University Press.
5. Lê Công Thành (2013) *Lý thuyết độ phức tạp tính toán*. Nhà xuất bản Khoa học Tự nhiên và Công nghệ.

Các chủ đề tiểu luận

Nhóm 1 (giảng viên gợi ý):

1. Mã đàn hồi/mã luân phiên/mã của các từ vô hạn: *cấu trúc, đặc trưng, tiêu chuẩn kiểm định, ứng dụng*
2. Các hệ mật xác suất/các hệ mật đa trị và nhập nhằng
3. Blockchain
4. Tấn công các hệ mật khóa đối xứng
5. Tấn công các hệ mật khóa công khai
6. Tấn công các lược đồ chữ kí số

Các chủ đề tiểu luận

Nhóm 2 (sinh viên đề xuất):

1. ...
2. ...
3. ...

TRÂN TRỌNG CẢM ƠN!