MỜI CÁC BẠN TÌM ĐỌC

1. GIÁO TRÌNH NGÔN NGỮ LẬP TRÌNH C/C++
2. GIÁO TRÌNH NGÔN NGỮ LẬP TRÌNH PASCAL
3. GIÁO TRÌNH CƠ SỞ DỮ LIỆU
4. GIÁO TRÌNH CƠ SỞ DỮ LIỆU PHÂN TÁN
5. GIÁO TRÌNH CƠ SỞ DỮ LIỆU: LÝ THUYẾT VÀ THỰC HÀNH
6. NHẬP MÔN PHÂN TÍCH THÔNG TIN CÓ BẢO MẬT
7. KỸ NGHỆ PHẦN MỀM
8. LÝ THUYẾT HỆ THỐNG VÀ ĐIỀU KHIỂN HỌC
9. SÁNG TẠO TRONG THUẬT TOÁN VÀ LẬP TRÌNH (3 TẬP)
10. KỸ THUẬT PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG THÔNG TIN HƯỚNG CẤU TRÚC

Giá: ...đ

TS. THÁI THANH TÙNG

GIÁO TRÌNH MẬT MÃ HỌC VÀ AN TOÀN THÔNG TIN

NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

TS. THÁI THANH TÙNG

Giáo trình
MẬT MÃ HỌC & AN TOÀN THÔNG TIN

(CRYPTOGRAPHY AND SECURED INFORMATION)

NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

TS. THÁI THANH TÙNG

Giáo trình

MẬT MÃ HỌC
&
HỆ THỐNG THÔNG TIN AN TOÀN

(CRYPTOGRAPHY AND SECURE INFORMATION SYSTEM)

NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

GD 15 HM 11

LỜI GIỚI THIỆU

Với sự bùng nổ của Công nghệ thông tin vào cuối thế kỷ XX đầu thế kỷ XXI, nhân loại đang bước vào một thời đại mới: Thời đại của nền kinh tế thông tin toàn cầu hóa. Mọi hoạt động xã hội, chính trị, kinh tế trong thời đại mới hiện nay xét cho cùng, thực chất đều là những hoạt động thu thập, xử lý, lưu trữ và trao đổi thông tin. Trong bối cảnh đó An toàn và Bảo mật thông tin luôn là mối quan tâm hàng đầu trong mọi giao dịch xã hội, đặc biệt là giao dịch điện tử trên môi trường Internet, một môi trường mở, môi trường không được tin cậy.

TS. Thái Thanh Tùng dựa trên kinh nghiệm bản thân trong quá trình nhiều năm nghiên cứu, giảng dạy và hoạt động thực tế trong lĩnh vực an ninh mạng máy tính và bảo mật thông tin, đã tập hợp một số tài liệu cơ sở xuất bản trên thế giới trong những năm gần đây, đồng thời cập nhật những thành tựu mới nhất trong lĩnh vực nói trên để xây dựng nên cuốn sách này.

Cuốn sách được trình bày hợp lý với nội dung khá hoàn chỉnh, không những giúp cho người bắt đầu làm quen dễ tiếp thu những kiến thức cơ bản nhất của một lĩnh vực chuyên môn khó mà còn gợi mở những hướng ứng dụng thực tế phong phú cho những người muốn nghiên cứu sâu hơn.

Những phụ lục được sưu tầm chọn lọc đưa ra trong phần cuối cuốn sách có ý nghĩa bổ sung cho các phần trình bày chính và cũng là một sự hỗ trợ rất tốt về nguồn tư liệu cho những người muốn đi sâu nghiên cứu.

Giáo trình *Mật mã học và Hệ thống thông tin an toàn* của tác giả Thái Thanh Tùng đã được Ban Công nghệ *Viện Nghiên cứu và phát*

triển Tin học ứng dụng (*AIRDI*) thuộc Liên hiệp các Hội Khoa học và Kỹ thuật Việt Nam giới thiệu và *Hội đồng tư vấn ngành Công nghệ thông tin Viện Đại học Mở Hà Nội* đã chấp nhận sử dụng làm giáo trình chính thức để giảng dạy học phần *An ninh và Bảo mật thông tin* trong chương trình đào tạo Kỹ sư Công nghệ thông tin cũng như *Khoa Quốc tế Đại học Quốc gia Hà Nội* sử dụng trong chương trình đào tạo Cao học Quản lý Thông tin liên kết với *Đại học Lunghwa - Đài Loan*.

Xin trân trọng giới thiệu cùng bạn đọc!

Hà Nội, tháng 7 năm 2011

TS. TRƯƠNG TIẾN TÙNG

Trưởng Ban Công nghệ

Viện NC & PT Tin học Ứng dụng

LỜI MỞ ĐẦU

Con người luôn sống trong môi trường trao đổi thông tin hàng ngày, hàng giờ. Người thợ săn hú gọi bạn trong rừng thẳm, người đốc công niêm yết lệnh phân công trên bảng tin tức của công trường, người khách gửi đơn đặt hàng đến cửa hàng, con cái đi xa gọi điện thoại, gửi thư về báo tình hình cho bố mẹ,... tất cả những chuyện thường ngày đó đều chính là trao đổi thông tin.

Trong phần lớn trường hợp trao đổi thông tin giữa hai đối tác, người ta không hề muốn để thông tin bị lộ cho người thứ ba biết vì điều đó có thể gây ra những tổn thất cả về vật chất cũng như về tinh thần. Một báo cáo về một phát minh khoa học công nghệ mới, một bản phân tích tình hình giá cả hàng hóa ở một thị trường, một bộ hồ sơ dự thầu, nếu bị lộ ra trước khi đến tay người nhận thì thiệt hại kinh tế thật khó lường! Một vị nguyên soái gửi lệnh điều binh đến cho tướng lĩnh dưới quyền: chuyện gì sẽ xảy đến cho toàn quân nếu thông tin đó bị lộ cho kẻ địch biết?

Để bảo vệ bí mật cho thông tin của mình được gửi đi trong một môi trường "mở" tức là môi trường có thể có nhiều tác nhân tiếp cận ngoài hai đối tác trao đổi thông tin, người ta phải dùng mật mã tức là dùng những phương pháp biến đổi làm cho nguyên bản gốc của thông tin (*plaintext*) ở dạng thông thường ai cũng có thể hiểu được biến thành một dạng bí mật (*ciphertext*) mà chỉ có những người nắm được quy luật mới có thể biến đổi ngược lại thành dạng nguyên gốc ban đầu để đọc.

Mật mã học là khoa học nghiên cứu cơ sở lý thuyết và công nghệ để thực hiện việc xây dựng và sử dụng các hệ thống mật mã.

Mật mã học (*cryptography*) là một lĩnh vực liên quan đến các kỹ thuật ngôn ngữ học và toán học để đảm bảo an toàn thông tin, cụ thể là trong thông tin liên lạc. Quá trình mã hóa được sử dụng chủ yếu để đảm bảo tính bí mật của các thông tin quan trọng, chẳng hạn trong công tác tình báo, quân sự hay ngoại giao cũng như các bí mật về kinh tế, thương mại hay cả đến những thông tin cá nhân riêng tư.

Trong những năm gần đây, lĩnh vực hoạt động của mật mã hóa đã được mở rộng: mật mã hóa hiện đại cung cấp cơ chế cho nhiều hoạt động hơn là chỉ duy nhất việc giữ bí mật thông tin và còn có một loạt các ứng dụng quan trọng như: chứng thực khóa công khai, chữ ký số, thanh toán điện tử hay tiền điện tử. Ngay cả những người không có nhu cầu cao về tính bí mật và không có kiến thức về lập mật mã, giải mật mã cũng có thể sử dụng các công nghệ mật mã hóa, thông thường được thiết kế và tích hợp sẵn trong các cơ sở hạ tầng của công nghệ tính toán và liên lạc viễn thông.

Mật mã học là một ngành có lịch sử từ hàng nghìn năm nay. Trong phần lớn thời gian phát triển của mình (ngoại trừ mấy thập kỷ gần đây), lịch sử mật mã học chính là lịch sử của những phương pháp mật mã học cổ điển - các phương pháp mật mã hóa với bút và giấy, đôi khi có hỗ trợ từ những dụng cụ cơ khí đơn giản. Vào đầu thế kỷ XX, sự xuất hiện của các cơ cấu cơ khí và điện cơ, chẳng hạn như *máy Enigma*, đã cung cấp những cơ chế phức tạp và hiệu quả hơn cho mật mã hóa.

Sự ra đời và phát triển mạnh mẽ của ngành điện tử và máy tính trong những thập kỷ gần đây đã tạo điều kiện để mật mã học phát triển nhảy vọt lên một tầm cao mới.

Sự phát triển của mật mã học luôn đi kèm với sự phát triển của các kỹ thuật phá mã (hay còn gọi là *thám mã*). Các phát hiện và ứng dụng của các kỹ thuật phá mã trong một số trường hợp đã có ảnh hưởng đáng kể đến các sự kiện lịch sử. Một vài sự kiện đáng ghi nhớ bao gồm việc phát hiện ra bức điện Zimmermann đã khiến Hoa Kỳ tham gia Thế chiến II và việc phá mã thành công hệ thống mật mã của Đức quốc xã góp phần làm đẩy nhanh thời điểm kết thúc Thế chiến II.

Cho tới đầu thập kỷ 1970, các kỹ thuật liên quan tới mật mã học hầu như chỉ nằm trong tay các chính phủ. Hai sự kiện đã khiến cho mật mã học trở nên thích hợp cho mọi người, đó là: sự xuất hiện của tiêu chuẩn mật mã hóa dữ liệu DES (*Data Encryption Standard)* và sự ra đời của các kỹ thuật mật mã hóa khóa công khai.

Từ hơn mười năm trước, cứ vào tháng giêng hàng năm một số nhà nghiên cứu hàng đầu thế giới có một cuộc gặp gỡ trao đổi tại thung lũng Silicon được gọi là Hội thảo An ninh RSA – *RSA security Conference* (*John Kinyon*). Trong những năm đầu chỉ có một số ít nhà Toán học, Mật mã học, các Tư tưởng gia tiên phong trong những lĩnh vực liên quan đến an ninh dữ liệu cho máy tính điện tử và bảo mật thông tin trong giao dịch điện tử tham gia. Trong những năm cuối của thiên niên kỷ trước, vào thời kỳ bùng nổ của Công nghệ thông tin và Internet, vai trò quan trọng của các hội thảo an ninh điện tử đó ngày một nổi bật lên và hàng năm ngoài hội thảo an ninh RSA còn có hàng chục hội thảo an ninh thông tin điện tử và an ninh mạng khác được tiến hành, tập hợp sự tham dự và đóng góp của những tài năng kiệt xuất nhất trong kỷ nguyên công nghệ thông tin này.

Có thể khẳng định rằng, nếu không giải quyết được vấn đề an toàn dữ liệu cho máy tính điện tử, an ninh giao dịch điện tử (đặc biệt

là trên Internet) thì hầu như phần lớn thành quả của công nghệ thông tin, của mạng Internet đều trở thành vô nghĩa!

Do vậy, mọi kỹ sư, kỹ thuật viên, nhà nghiên cứu, người ứng dụng công nghệ thông tin đều cần được trang bị những kiến thức cơ bản tối thiểu về Mật mã học. Nhằm mục đích đó, tác giả đã sử dụng những tư liệu, giáo trình đã giảng dạy về mật mã học cho bậc đại học, cao học ngành công nghệ thông tin, toán tin ở Đại học Bách khoa Hà Nội, Viện Đại học Mở Hà Nội, tham khảo những công trình công bố quốc tế và trong nước trong vòng mười năm gần đây (xem tài liệu tham khảo) để biên soạn thành cuốn sách này. ***Giáo trình mật mã học và hệ thống thông tin an toàn*** là sự sắp xếp trình bày theo quan điểm của tác giả, có tham khảo nhiều tài liệu nhưng không dựa theo khuôn mẫu của một tư liệu nào cùng chuyên ngành đã công bố trước đây. Tác giả không dám hy vọng trình bày được thật chi tiết đầy đủ và đi sâu vào những vấn đề toán học rất phức tạp, mà chỉ mong đáp ứng phù hợp với nhu cầu của đông đảo sinh viên, kỹ sư, nhà nghiên cứu trong việc tìm hiểu một cách căn bản về một ngành học đang có hàng loạt ứng dụng quan trọng trong công nghệ thông tin và truyền thông hiện nay.

Nội dung giáo trình trình bày những khái niệm và định nghĩa chung về bảo mật thông tin, đi sâu phân tích 2 loại mã hóa: mã khóa bí mật cùng các giao thức, thuật toán trao đổi khóa mã và mã bất đối xứng hay mã khóa công khai và khóa riêng với những ứng dụng cụ thể của nó. Bên cạnh đó, nội dung giáo trình giới thiệu đến một vấn đề rất có ý nghĩa hiện nay trong các giao dịch thương mại điện tử, ngân hàng trực tuyến đó là: *Chữ ký điện tử, chữ ký số và vấn đề phân phối khóa công khai với các hệ thống hạ tầng cơ sở khóa công khai PKI và chuẩn X509 cũng như hệ thống mạng lưới tin cậy và giao thức PGP*. Đặc biệt phần cuối giới thiệu các giao thức và chuẩn mã

hóa thông dụng nhất trên Internet trong các dịch vụ bảo mật thư điện tử như *S/MIME*, những giao thức và chuẩn mã hóa sử dụng để bảo đảm an toàn thông tin đặc biệt quan trọng trong thương mại điện tử, ngân hàng điện tử, như *SSL/TLS và HTTPS, FTPS, SET, SSH, IPsec*… Ở cuối mỗi phần lý thuyết, giáo trình cung cấp một danh mục các phần mềm ứng dụng thương mại và phi thương mại để người đọc tiện tra cứu, sử dụng.

Giáo trình được xuất bản lần đầu sẽ khó tránh khỏi những thiếu sót. Rất mong nhận được ý kiến nhận xét, góp ý của bạn đọc để giáo trình ngày càng được hoàn thiện hơn trong lần tái bản sau.

Xin chân thành cảm ơn các bạn đồng nghiệp ở Khoa Công nghệ Thông tin - Viện Đại học Mở Hà Nội đã góp ý cho tác giả trong việc biên soạn giáo trình này.

Hà Nội, tháng 7 năm 2011

Tác giả