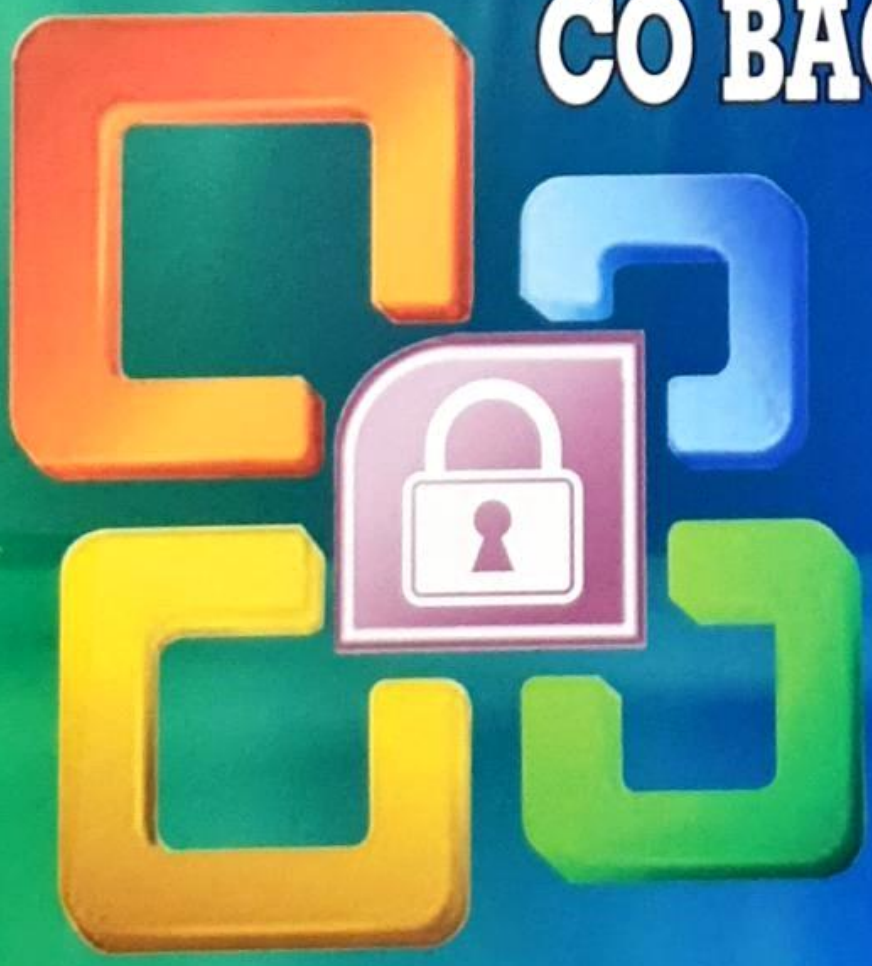
TS. HỒ VĂN CANH, TS. NGUYỄN VIẾT THẾ

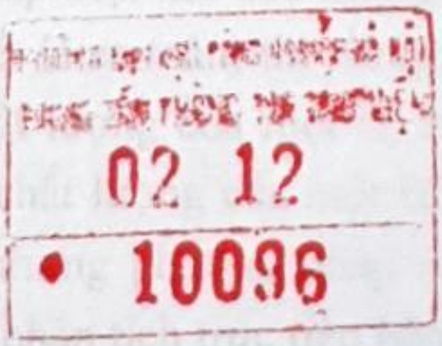
Nhập môn PHÂN TÍCH THÔNG TIN CÓ BẢO MẬT



NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

TS. HỒ VĂN CANH, TS. NGUYỄN VIẾT THẾ

Nhập môn PHÂN TÍCH THÔNG TIN CÓ BẢO MẬT



NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

LỜI NÓI ĐẦU

Như chúng ta đều biết vai trò quan trọng của an toàn thông tin (ATTT) trong thời đại bùng nổ thông tin hiện nay. Người ta chia các vi phạm ATTT trên mạng truyền dẫn nói chung, mạng máy tính nói riêng thành loại thụ động và loại chủ động. Loại vi phạm thụ động chỉ nhằm mục đích là nắm bắt thông tin, có thể chỉ tìm người gửi, người nhận, mật độ thông tin trao đổi, thời gian gửi. Vi phạm thụ động thường không làm sai lệch hoặc hủy nội dung trao đổi. Loại vi phạm chủ động có thể làm thay đổi nội dung, xóa bỏ, làm trễ thông tin đang truyền, làm biến dạng chúng, chèn thông tin giả vào thông tin thật trên mạng thậm chí có thể tìm cách phá sập một Website nào đó.

Trong số các phương pháp đảm bảo ATTT thì phương pháp mật mã hóa (Cryptography) được sử dụng rộng rãi và đảm bảo an toàn nhất. Tuy nhiên phương pháp mật mã hóa cũng có những yếu điểm quan trọng là nếu phương pháp mật mã hóa không tốt (mặc dù việc quản lý khóa mã được giả thiết là an toàn) thì rất nguy hiểm. Vậy làm thế nào để đánh giá được chất lượng của một hệ mật mã là tốt? Có nhiều phương pháp đánh giá chất lượng của một hệ mật như phương pháp Entropy của Shannon, nhưng phương pháp tốt nhất và là trực quan nhất, đó là phương pháp phân tích trực tiếp bản mã khi không có khóa mã trong tay mà người ta thường gọi là thám mã (Cryptanalysis). Đây là một bộ môn mới được công khai hóa trong thời gian gần đây. Để bước đầu làm quen với môn *"nghệ thuật"* này, NXB Thông tin và Truyền thông đã xuất bản cuốn sách ***"Nhập môn phân tích thông tin có bảo mật"*** giới thiệu đến bạn đọc. Đây là phương pháp đảm bảo

ATTT lâu đời nhất, quan trọng nhất và được nghiên cứu phát triển ngày càng rộng rãi. Nó đã trở thành một ngành khoa học được gọi là khoa học về phân tích mật mã (Cryptanalysis).

Cuốn sách được TS. Hồ Văn Canh và TS. Nguyễn Viết Thế tổng hợp và biên soạn từ nhiều kết quả nghiên cứu khoa học đã được công bố cùng với kinh nghiệm tích luỹ được sau 30 năm tìm tòi, nghiên cứu và trực tiếp giảng dạy của các tác giả. Cuốn sách gồm 7 chương:

Chương 1: Khái niệm về mã thám

Chương 2: Một số kiến thức bổ trợ

Chương 3: Các bước cơ bản để tiến hành thám mã

Chương 4: Thực hành phân tích một số luật mã thuộc hệ mật truyền thống

Chương 5: Một số phương pháp thám mã dữ liệu DES

Chương 6: Mật mã công khai và phương pháp thám mã

Chương 7: Phương pháp tấn công RSA không cần phân tích nhân tử.

Hy vọng cuốn sách sẽ thực sự hữu ích đối với các kỹ sư, kỹ thuật viên, cán bộ giảng dạy và sinh viên ngành Công nghệ Thông tin, Điện tử Viễn thông, Ngành Mật mã... khi thực hiện đề tài, đồ án, các dự án, cũng như trong giảng dạy, học tập... Ngoài ra, cuốn sách cũng là tài liệu tham khảo bổ ích cho bạn đọc quan tâm tới lĩnh vực này.

Nhà xuất bản xin giới thiệu cùng bạn đọc và rất mong nhận được ý kiến đóng góp của quý vị. Mọi ý kiến đóng góp xin gửi về ***Nhà xuất bản Thông tin và Truyền thông*** - 18 Nguyễn Du, Hà Nội.

Trân trọng cảm ơn./.

NXB THÔNG TIN VÀ TRUYỀN THÔNG

MỤC LỤC