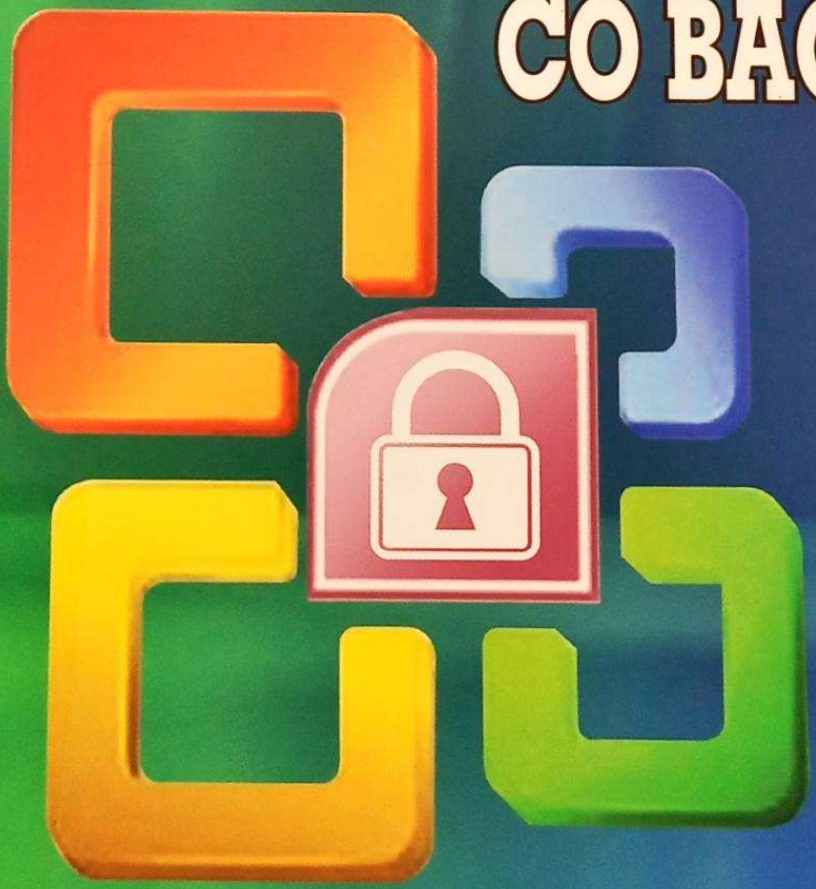
TS. HỒ VĂN CANH, TS. NGUYỄN VIẾT THẾ

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

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

Chương 1

KHÁI NIỆM VỀ MÃ THÁM

1.1. MỞ ĐẦU

Trong phần trình bày này, chúng ta tạm phân mã đối xứng làm hai phần, mật mã cổ điển và mật mã "hiện đại". Ở đây chúng ta phân biệt khái niệm "hiện đại" trong hệ thống mật mã đối xứng được dùng trong cuốn sách này với khái niệm "hiện đại" trong hệ mật mã bất đối xứng. Trong phạm vi cuốn sách này, ta hiểu mật mã "hiện đại" là hệ mật khoá đối xứng nhưng nó đã phát triển ở mức cao, đặc biệt là tự động hoá trong việc mã dịch. Mật mã này hiện nay đang phát triển mạnh như mật mã với khoá thuật toán DES; 3DES; IDEA; FEAL; AES,... Chính vì vậy, chúng ta gọi mật mã như vậy là mật mã hiện đại. Còn mật mã cổ điển là mật mã được mã/dịch bằng thủ công, mật mã loại này ra đời sớm nhất, nó được sử dụng, phát triển lâu đời và đến nay nó chỉ tồn tại ở một số nước đang phát triển và cũng chỉ trong một phạm vi hẹp, ở những nơi khó khăn trong ứng dụng công nghệ điện/điện tử (ví dụ trong lực lượng quân sự hoạt động phân tán, trong vùng nông thôn, rừng núi hoặc trong các đơn vị tình báo...). Tuy nhiên, chính mật mã loại này lại là nền tảng cho sự phát triển của mật mã hiện đại (theo nghĩa của cuốn sách này).

MỤC LỤC