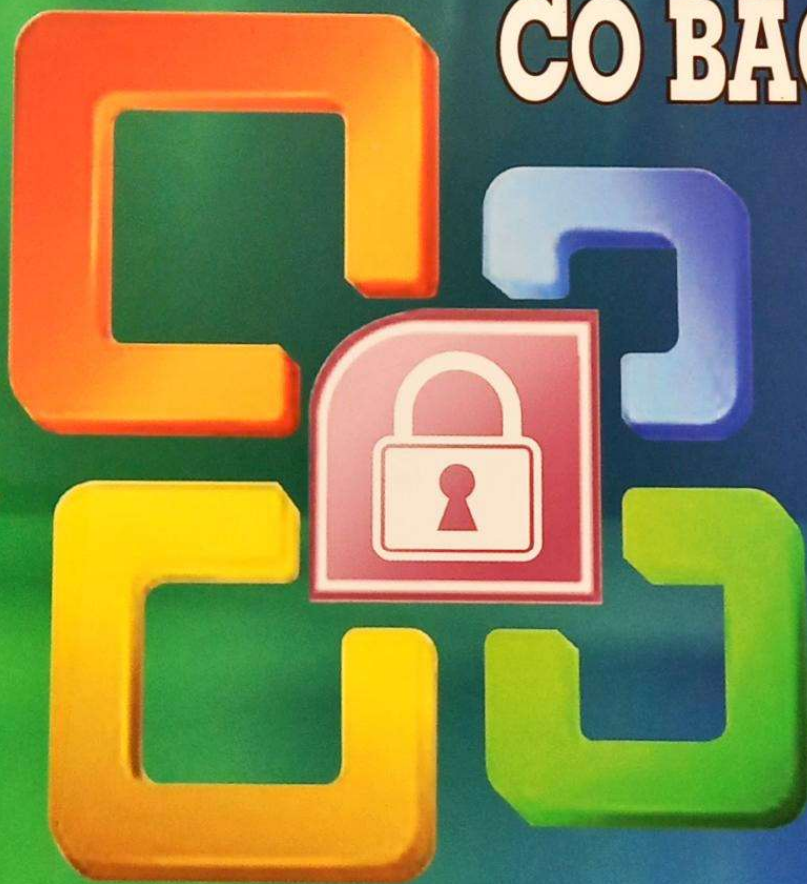


TS. HỒ VĂN CANH, TS. NGUYỄN VIỆT THẾ

Nhập môn PHÂN TÍCH THÔNG TIN CÓ BẢO MẬT

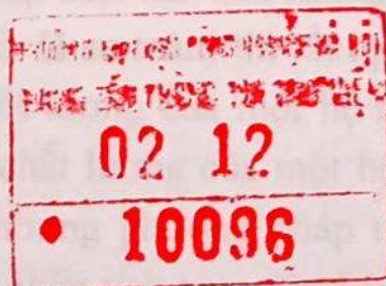


NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

TS. HỒ VĂN CANH, TS. NGUYỄN VIỆT THẾ

LỜI NÓI ĐẦU

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 lũy 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 THẨM

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

Lời nói đầu	3
Chương 1. Khái niệm về mã thám	5
1.1. Mở đầu.....	5
1.2. Các thuật ngữ cơ bản về mật mã và mã thám.....	6
1.3. Đặc trưng cơ bản của bản rõ.....	10
Chương 2. Một số kiến thức bổ trợ	21
2.1. Mở đầu.....	21
2.2. Một số khái niệm.....	21
2.3. Giải bài toán phân lớp các đối tượng và ứng dụng vào công tác thám mã.....	30
2.4. Độ phức tạp thuật toán	47
2.5. Các tiêu chuẩn thống kê	51
2.6. Năm tiêu chuẩn thống kê cơ bản	54
Chương 3. Các bước cơ bản để tiến hành thám mã	61
Chương 4. Thực hành phân tích một số luật mã thuộc hệ mật truyền thống	71
4.1. Mở đầu.....	71
4.2. Mã pháp thay thế đơn và phương pháp thám mã	72

4.3. Luật mã Ceasar và phương pháp thám.....	88
4.4. Luật mã Playfair và phương pháp thám.....	98
4.5. Thám bản mã thay thế nhiều vắn chữ cái (hay còn gọi là thay thế định kỳ)	112
4.6. Mã pháp chuyển vị đơn và phương pháp thám.....	126
Chương 5. Một số phương pháp thám mã dữ liệu DES.....	153
5.1. Thám mã vi sai đối với DES và các hệ mã khối lặp giống DES	153
5.2. Thám mã tuyến tính đối với hệ DES.....	175
5.3. Thám mã phi tuyến	189
5.4. Tấn công vi sai bậc cao	206
5.5. Tấn công nội suy.....	212
5.6. Tấn công khóa quan hệ	218
5.7. Các đặc trưng an toàn cơ bản của một hệ mã khối	228
Chương 6. Mật mã công khai và phương pháp thám mã	231
6.1. Mở đầu	231
6.2. Hệ mã hóa RSA	232
6.3. Tính an toàn của hệ mật mã	236
6.4. Các kiểu thám mã.....	238
6.5. Một số sơ hở dẫn đến việc tấn công hệ mật RSA	240
6.6. Xây dựng thuật toán phân tích tham số RSA.....	261

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

7.1. Mở đầu.....	281
7.2. Một số nhận xét.....	281
7.3. Các thuật toán.....	282
7.4. Các ví dụ.....	287
Phụ lục 1.....	292
Phụ lục 2.....	305
Tài liệu tham khảo.....	317
	321

in xong và nộp lưu chiểu tháng 7 năm 2011
số quyết định xuất bản: 134/QĐ-NXB TTTT ngày 13 tháng 7 năm 2011
số đăng ký và hoạt động xuất bản: 187-2010/CXB/9-80/TTTT
in 1000 bản, khổ 14 x 20,5 cm tại CP TNHH sản xuất và Thương mại Trí Việt