

TS. HỒ VĂN CANH, TS. NGUYỄN VIỆT THẾ

Nhập môn

PHÂN TÍCH THÔNG TIN

CÓ BẢO MẬT

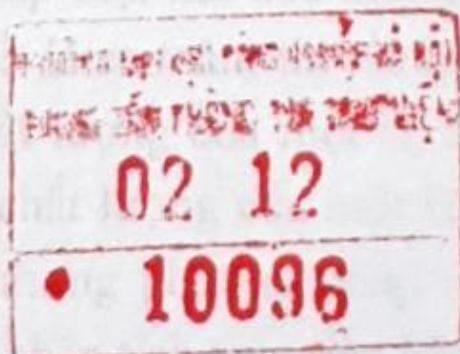


NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

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

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 Việt 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

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 vần 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 281

7.1. Mở đầu 281

7.2. Một số nhận xét 282

7.3. Các thuật toán 287

7.4. Các ví dụ 292

Phụ lục 1 305

Phụ lục 2 317

Tài liệu tham khảo 321

in xong và nộp tài liệu tháng 5 năm 2010
Số duyệt của xuất bản: 1340D-KXB-TTT ngày 13 tháng 7 năm 2010
Số đăng ký kế hoạch xuất bản: 18A-2010/CXB/9 - BVT/TTT
in 1000 bản khổ 14 x 20,5 cm tại Công ty TNHH sản xuất và Thương mại Việt