

Nghiên cứu xây dựng thuật toán mã khối phục vụ việc bảo mật thông tin chiến lược :

Luận văn ThS / Nguyễn Vũ Hoàng ; Nghd. : TS. Hồ Văn Canh . - H. : ĐHCN, 2005 . - 94 tr. + Đĩa CD-ROM

Tóm tắt: Giới thiệu tổng quan về mật mã học và thực trạng an toàn thông tin hiện nay: các mức an toàn mạng, vấn đề bảo vệ thông tin bằng mật mã, việc tấn công vào các dữ liệu được mã hóa và các mối đe dọa mất an toàn. Nêu vai trò của mật mã, quy trình mã hóa dữ liệu, hàm mã hóa và khóa, khái niệm và ý nghĩa của mật mã khối. Đề xuất và sử dụng thuật toán dãy bit giả làm một hệ mã khối mới và nêu một số tiêu chuẩn đánh giá chất lượng khóa

Trang phụ bìa

Mục lục

1

Danh mục các ký hiệu, các chữ viết tắt

3

Danh mục các bảng

4

Danh mục các hình vẽ, đồ thị

5

MỞ ĐẦU

6

CHƯƠNG 1. TỔNG QUAN VỀ MẬT MÃ HỌC

8

1.1. Mật mã học

8

1.2. Thuật ngữ

9

1.3. Phân tích mật mã

10

.....

1.4. Lịch sử	12
1.5. An ninh thông tin	13
1.6. Khoá đối xứng	14
1.7. Khoá công khai	15
1.8. Các vấn đề khác.	16
CHƯƠNG 2. THỰC TRẠNG AN TOÀN THÔNG TIN TRÊN CÁC MẠNG MÁY TÍNH	18
2.1. Thực trạng an toàn thông tin hiện nay.	18
2.2. Các mức bảo vệ an toàn mạng	22
2.3. Bảo vệ thông tin bằng mật mã.	24
2.4. Tấn công vào các dữ liệu được mã hoá	26
2.5. Các mối đe dọa mất an toàn	27
CHƯƠNG 3. BẢO VỆ THÔNG TIN BẰNG MẬT MÃ HOÁ	31
3.1. Vai trò của mật mã:	31
3.2. Quy trình mã hoá dữ liệu	32
3.3. Hàm mã hoá và khoá	34
3.4. Tạo các dãy bit giả ngẫu nhiên và ứng dụng trong việc mã hoá dữ liệu	35
CHƯƠNG 4. MẬT MÃ KHỐI VÀ Ý NGHĨA CỦA NÓ	39
4.1. Thế nào là một hệ mã khối	39
4.2. Ý nghĩa của mật mã khối	43
4.3. Quan sát một số hệ mật mã khối đang được sử dụng rộng rãi trên thế giới.	44
4.3.1. DES (Data Encryption Standard)	44
4.3.2 PGP (Pretty Good Privacy)	56

.....

4.3.3. AES (<i>Advanced Encryption Standard</i>)	60
CHƯƠNG 5. ĐỀ XUẤT MỘT HỆ MÃ KHỐI MỚI	66
5.1. Thuật toán tạo dãy giả ngẫu nhiên.	66
5.2. Phương pháp mã/dịch	72
5.3. Ví dụ.	75
5.4. Một số tiêu chuẩn để đánh giá chất lượng khoá mã.	80
KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU TIẾP THEO	90
Tài liệu tham khảo	93

.....