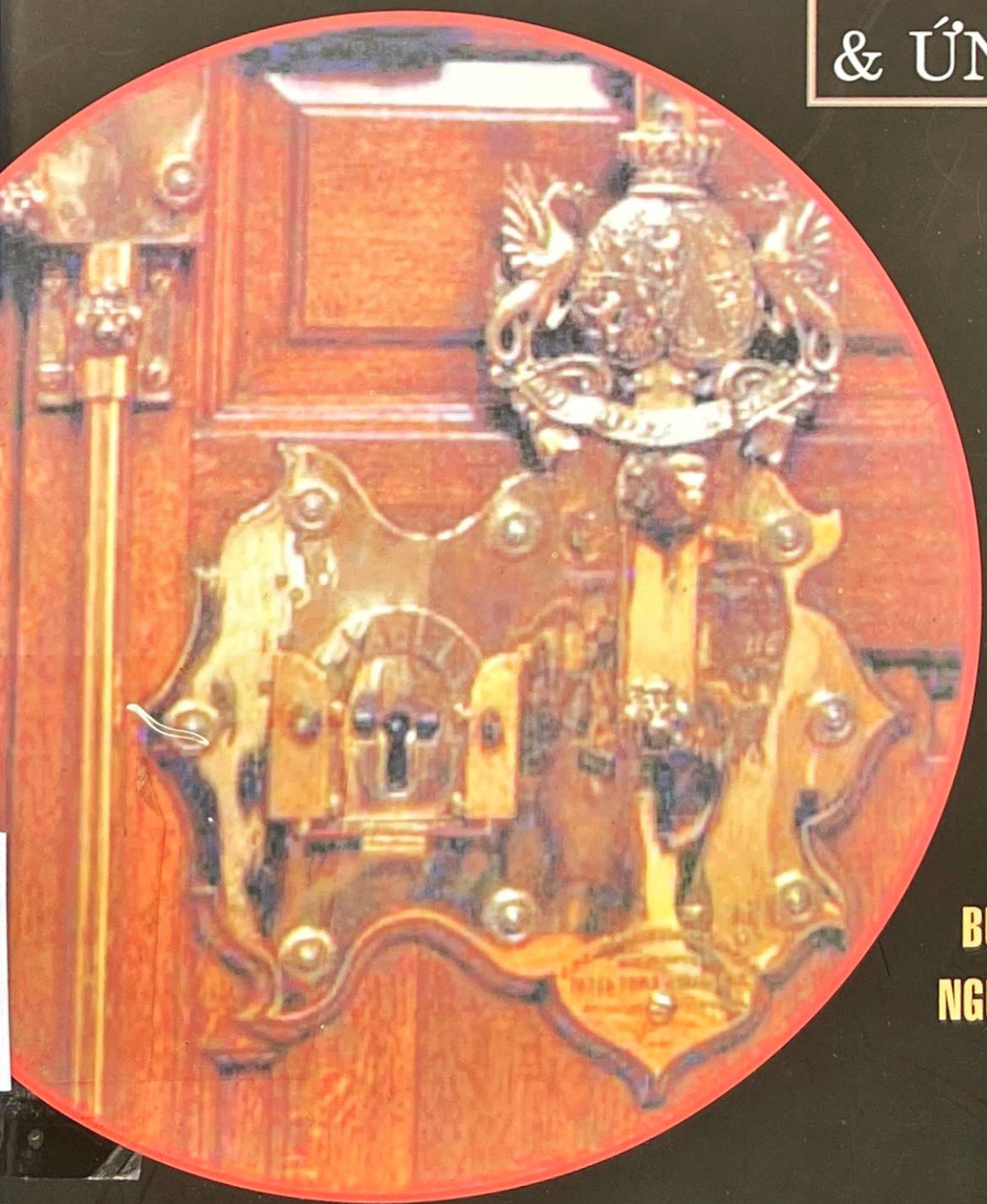
UEF

Giáo trình

Mã hóa Thông tin

LÝ THUYẾT & ỨNG DỤNG



BÙI DOÃN KHANH
NGUYỄN ĐÌNH THÚC

NHÀ XUẤT BẢN LAO ĐỘNG XÃ HỘI

BÙI DOÃN KHANH
NGUYỄN ĐÌNH THÚC
HOÀNG ĐỨC HẢI

Giáo trình Mã hóa Thông tin

LÝ THUYẾT & ỨNG DỤNG

NHÀ XUẤT BẢN LAO ĐỘNG XÃ HỘI

Lời nói đầu

Mã hóa thông tin là một mảng kiến thức quan trọng trong chương trình đào tạo Công nghệ Thông tin, Mạng máy tính, Viễn thông, Toán-Tin,...Tuy nhiên tài liệu về mã hoá thông tin chưa nhiều và chưa đáp ứng được nhu cầu học tập, nghiên cứu của sinh viên, chuyên viên. Tài liệu này được biên soạn như một giáo trình nhằm mục đích giảng dạy và học tập cho các khoa Công nghệ thông tin, Tin học, Toán tin, Tin học Viễn thông,...

Lý thuyết số và Đại số hiện đại đóng một vai trò rất quan trọng trong các phương pháp mã hoá thông tin do hầu hết các hệ mã hiện đại được xây dựng dựa trên việc khai thác các tính chất của các số lớn. Vì thế, trước khi trình bày về các hệ mã, chúng tôi giới thiệu các kiến thức toán học quan trọng sẽ được sử dụng trong các hệ mã. Nội dung của giáo trình gồm 4 chương. Chương 1 trình bày cơ sở toán học cho mã hoá thông tin. Chương 2 và chương 3 phát triển các lý thuyết trình bày trong chương 1 để xây dựng các phép toán nhanh trên số nguyên lớn và để khảo sát các bài toán quan trọng trong lý thuyết số như: kiểm tra, tạo số nguyên tố lớn. Cuối cùng, chương 4 sử dụng kết quả lý thuyết của 3 chương đầu để khảo sát một số hệ mã hiện đại cũng như để ứng dụng mã hoá thông tin trong thương mại điện tử, trong an toàn dữ liệu.

Mặc dù có nhiều cố gắng, giáo trình này không thể tránh khỏi những sai sót. Các ứng dụng của mã hoá thông tin và một số hệ mã còn chưa được trình bày trong giáo trình. Các tác giả mong nhận được những đóng góp quí báu của độc giả để giáo trình ngày càng hoàn thiện hơn.

Thành phố HCM, ngày 1/12/2004

Bùi Doãn Khanh – Nguyễn Đình Thúc

THƯ NGỎ

Kính thưa quý Bạn đọc gần xa!

Trước hết, Ban xuất bản xin bày tỏ lòng biết ơn và niềm vinh hạnh được đông đảo Bạn đọc nhiệt tình ủng hộ tủ sách MK.PUB.

Trong thời gian qua chúng tôi rất vui và cảm ơn các Bạn đã gửi e-mail đóng góp nhiều ý kiến quý báu cho tủ sách.

Mục tiêu và phương châm phục của vụ chúng tôi là:

- *Lao động khoa học nghiêm túc.*
- *Chất lượng và ngày càng chất lượng hơn.*
- *Tất cả vì Bạn đọc.*

Một lần nữa, Ban xuất bản MK.PUB xin kính mời quý Bạn đọc tiếp tục tham gia cùng chúng tôi để nâng cao chất lượng sách. Cụ thể:

Trong quá trình sử dụng sách, xin quý Bạn ghi chú lại các sai sót (*dù nhỏ, lớn*) của cuốn sách hoặc các nhận xét của riêng Bạn. Sau đó xin gửi về địa chỉ:

E-mail: *mk.book@minhkhai.com.vn* hoặc *mk.pub@minhkhai.com.vn*

Hoặc gửi về: **Nhà sách Minh Khai**

249 Nguyễn Thị Minh Khai, Q.I, Tp. Hồ Chí Minh

Nếu bạn ghi chú trực tiếp lên cuốn sách, rồi gửi cuốn sách đó cho chúng tôi thì chúng tôi xin hoàn lại cước phí bưu điện và gửi trả lại Bạn cuốn sách khác.

Ngoài ra, chúng tôi còn gửi tặng Bạn một cuốn sách khác trong tủ sách MK.PUB. Bạn có thể chọn cuốn sách này theo danh mục thích hợp sẽ gửi tới Bạn.

Với mục đích ngày càng nâng cao chất lượng tủ sách MK.PUB, chúng tôi rất mong nhận được sự hợp tác nhiệt tình của quý Bạn đọc gần xa.

"MK.PUB cùng Bạn đọc đồng hành" để nâng cao chất lượng sách.

Một lần nữa chúng tôi xin chân thành cảm ơn.

MK.PUB

Mục lục

Chương 1

Các Khái Niệm Cơ Bản

1. Thuật giải Euclide và thuật giải Bezout

Định nghĩa 1.1

Gọi Z là tập các số nguyên {0, 1, -1, 2, -2,... } và $N = \{n \in Z; n \geq 0\}$, $N^* = \{ n \in Z; n \geq 1\}$.

Cho $a,b \in Z$. Nếu $\exists c \in Z: b = ac$ ta nói a là ước của b và b là bội của a, ký hiệu $a \mid b$.

Ví dụ 1.2

Ta có $-3 \mid 69$, $3 \mid 0$ do $69 = (-3)(-23)$ và $0 = 3*0$.

Định lý 1.3

Với $a,b,c,x,y \in Z$, ta có:

a) $a \mid a$, $1 \mid a$;

b) $a \mid b, b \mid c \Rightarrow a \mid c$;

c) $a \mid b, a \mid c \Rightarrow a \mid (bx + cy)$;

d) $a \mid b, b \mid a \Rightarrow a = \pm b$;

e) $a \mid b \Rightarrow (-a) \mid b, a \mid (-b), (-a) \mid (-b)$.

Chứng minh

a) $a = a.1$.

b) Tồn tại $c_1, c_2 \in Z$ sao cho: $b = c_1a$, $c = c_2b$, vì thế $c = c_1c_2a$ hay $a \mid c$.

c) Tồn tại $c_1, c_2 \in Z$ sao cho: $b = c_1a$, $c = c_2a$ vì thế $bx + cy = (c_1x + c_2y)a$ hay $a \mid (bx + cy)$.