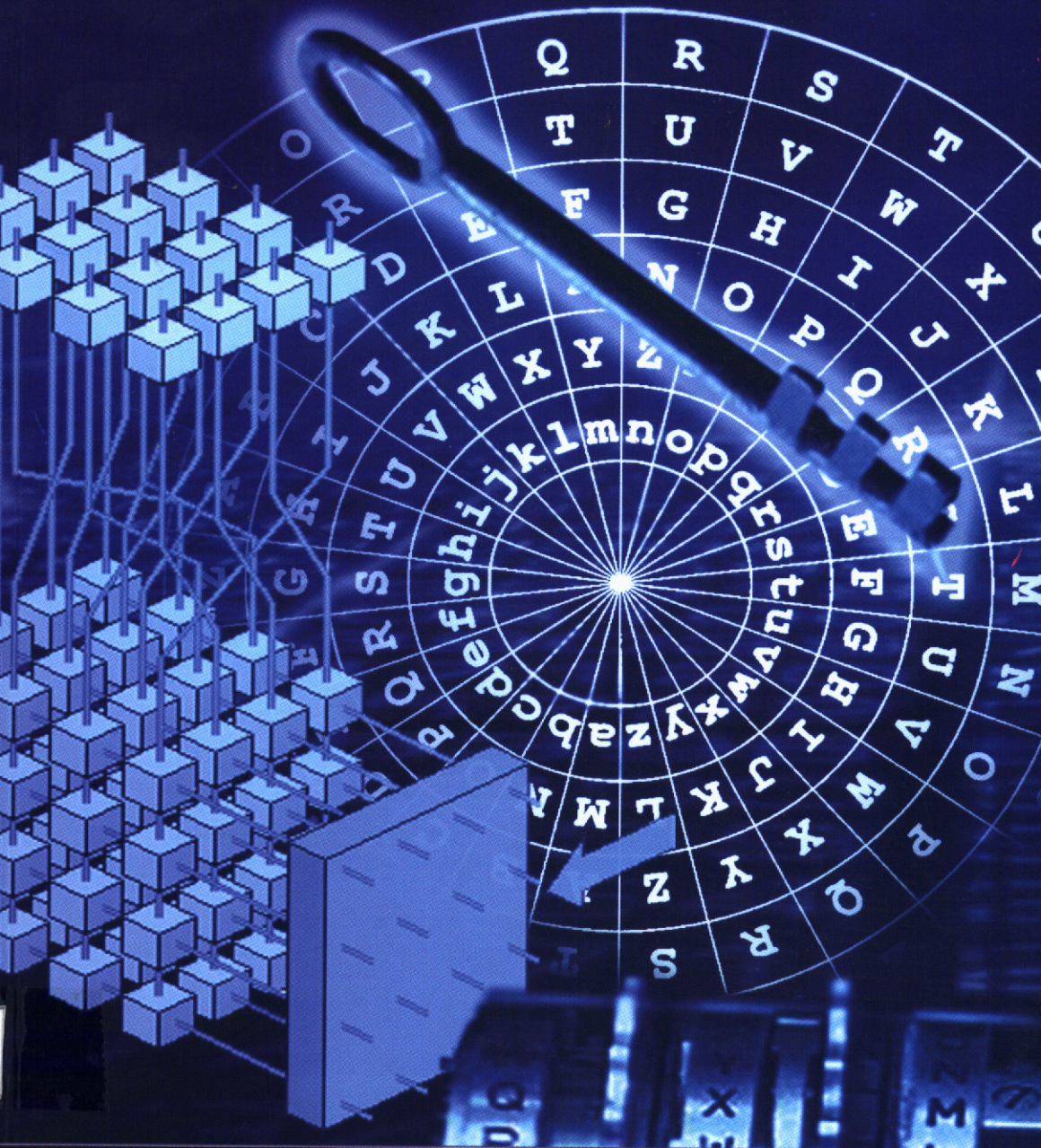
COLLECTION TECHNIQUE ET SCIENTIFIQUE DES TÉLÉCOMMUNICATIONS

Codage, cryptologie et applications

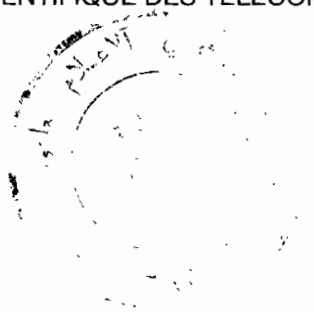
Bruno Martin



PRESSES POLYTECHNIQUES ET UNIVERSITAIRES ROMANDES

Codage, cryptologie et applications

COLLECTION TECHNIQUE ET SCIENTIFIQUE DES TÉLÉCOMMUNICATIONS



Codage, cryptologie et applications

Bruno Martin

PRESSES POLYTECHNIQUES ET UNIVERSITAIRES ROMANDES

Dans la même collection:

VHDL
Langage, modélisation et synthèse
R. Airiau, J.-M. Bergé, V. Olive & J. Rouillard

Objets réactifs en Java
Frédéric Boussinot

Egalement disponibles aux Presses polytechniques et universitaires romandes

Programmation séquentielle avec ADA 95
Pierre Breguet, Luigi Zaffalon

Programmation concurrente et temps réel avec Ada 95
Luigi Zaffalon, Pierre Breguet

Algorithmes et structures de données avec Ada, C++ et Java
Abdelali Guerid, Pierre Breguet, Henri Rothlisberger

Programmation orientée objets en C++
Une approche évolutive
Marylène Micheloud
Medard Rieder

Illustration de couverture réalisée par Atelier Isatis, Dijon.

Le catalogue des publications des Presses polytechniques et universitaires romandes
peut être obtenu par courrier à l'adresse suivante, EPFL – Centre Midi, CH-1015 Lausanne,
par E-Mail à ppur@epfl.ch, par téléphone au (0)21 693 41 40, ou par fax au (0)21 693 40 27.

http://www.ppur.org

ISBN 2-88074-569-1

Imprimé en Italie

Préface

Au cours de nos premiers pas dans le domaine de la cryptologie, nous sommes tous confrontés à la subtile nuance entre "codage" et "chiffrement". Il est vrai que l'usage courant de la langue française nous induit souvent en erreur. D'un point de vue formel, le "codage" se réfère à une représentation, quelle qu'elle soit, de l'information. D'un point de vue plus technique, on cherche à y représenter l'information de manière aussi efficace que possible pour communiquer, archiver, calculer. Le "chiffrement" peut être vu comme un cas particulier du codage : son objectif est également la représentation de l'information. Il est aussi la protection contre l'accès de personnes non habilitées et mal intentionnées. "Chiffre" est par conséquent synonyme de "code secret". Il est donc naturel en apparence d'englober la cryptographie dans les sciences des techniques de codage.

Ce serait pourtant ignorer leurs différences fondamentales. La cryptographie doit faire face à un adversaire malicieux. On cherche à savoir s'il parviendra sans effort à percer le système. La théorie de la complexité permet de quantifier la notion d'effort et joue donc un rôle central. En revanche, l'adversaire du codage (non cryptographique) est un phénomène aléatoire : un "bruit". On cherche donc à coder ou à comprimer mieux sur un support donné. C'est ici la théorie de l'information qui permet de quantifier le bruit et la capacité à le surmonter. Codage et cryptographie font donc face à des adversaires différents au moyen de théories différentes.

Pourquoi alors traiter ces deux disciplines dans un même ouvrage ? Comme les chapitres suivants le démontrent, ce sont en fait les applications et leurs outils qui les rassemblent. Tous les systèmes de communication (téléphone, courrier électronique, Internet ...) et les systèmes de stockage de données (disque compact, DVD, carte à puce ...) utilisent le codage. La plupart utilisent aussi des moyens cryptographiques pour sécuriser les données ou protéger la propriété intellectuelle. Les outils fondamentaux proviennent de l'algèbre discrète et combinatoire et de l'algorithmique. On utilisera donc corps finis, polynômes et espaces vectoriels, mais aussi arbres, graphes et automates.

Codage et cryptographie sont aujourd'hui omniprésents. Il est donc important de maîtriser ces technologies. Peu de livres les traitent de manière équilibrée. Le présent ouvrage présente brillamment les deux techniques. Il occulte volontairement les aspects trop techniques et offre une présentation homogène sous une forme mathématique. Ce livre est donc recommandé aux étudiants en systèmes de communication et en informatique qui cherchent à comprendre leurs mécanismes de base. Nous leur souhaitons bonne lecture.

Serge Vaudenay
Professeur à l'EPFL

Préambule

Ce livre présente de façon accessible à tous deux disciplines : la *cryptologie* (ou science du chiffre) dont l'origine remonte aux débuts de l'histoire de l'homme et celle des *codes correcteurs* qui est née pendant la seconde moitié du 20^{e} siècle, après l'invention de la théorie de l'information. Toutes deux traitent de la transmission sûre de l'information. La cryptographie (ou l'art de concevoir de bons chiffres) assure la confidentialité des communications en présence d'ennemis. Les codes correcteurs permettent de retirer d'éventuelles erreurs de transmission.

Nous avons choisi d'orienter cet ouvrage plutôt vers les applications en télécommunications numériques que vers l'abstraction théorique. Nous avons volontairement simplifié le contenu mathématique de ces disciplines dans le but de mieux comprendre certains aspects du fonctionnement d'appareils que nous utilisons tous les jours comme les téléphones cellulaires, les disques compacts et les ordinateurs. Par exemple, sans codes correcteurs et sans cryptographie, le développement des réseaux comme Internet ou bientôt des réseaux dits «ad hoc» (il s'agit des réseaux sans fil qui se construisent à la demande et qui commencent à être utilisés par les ordinateurs portables, les téléphones cellulaires, les appareils photos numériques ou les imprimantes) ne pourrait avoir lieu.

Il est d'ailleurs intéressant de noter que les différentes notions que nous présentons sont à la croisée d'un grand nombre de disciplines comme l'informatique (tant théorique que pratique), les mathématiques, mais aussi l'économie et même le droit. L'économie à cause du développement quasi continu d'Internet et de son impact social et économique et le droit qui régit l'utilisation des systèmes de chiffrement. Ce n'est que depuis quelques années que l'utilisation de chiffres est autorisée en France. La taille des clés est toujours limitée, sauf pour l'utilisation de signatures électroniques.

Présentation

Cet ouvrage est découpé en cinq parties. La première présente la *théorie de l'information* de Weaver et Shannon dont le but était de quantifier le contenu en information. A ce titre, on lui doit la notion de bit (pour *binary digit*). Il s'agit de la théorie qui permet de relier sous un cadre commun la compression des données, la théorie des codes et la cryptologie ; ces différentes disciplines sont toutes prises en compte dans les problématiques de la théorie de l'information.

La deuxième partie traite de la *compression des données*. Celle-ci devient de plus en plus présente dans notre vie quotidienne. C'est grâce à la compression

des données que nous pouvons communiquer au moyen de téléphones cellulaires, regarder des DVD, transmettre des quantités d'informations toujours plus grandes au moyen d'un modem ou même d'Internet. Nous nous limitons ici aux seuls algorithmes de compression travaillant conjointement avec les mécanismes de chiffrement dans les logiciels qui permettent d'assurer la sécurité des communications au travers d'Internet.

Pour transmettre un message au travers d'un canal de communication qui peut être perturbé (ou bruité), on lui ajoute de la redondance pour qu'il soit possible de détecter, voire de corriger des erreurs de transmission. C'est le but de la *théorie des codes* qui fait l'objet de la troisième partie de ce livre. Pour présenter cette théorie qui peut devenir assez mathématique, nous avons privilégié le point de vue de l'ingénieur en informatique. Notre but est de faire comprendre les algorithmes de codage et de décodage nécessaires au bon fonctionnement du mécanisme de détection ou de correction des erreurs de différents media de communication. Nous y présentons le principe de fonctionnement du mécanisme de correction des erreurs des disques compacts, celui des téléphones cellulaires de type GSM et ceux qui régissent certaines communications par satellite. Nous nous sommes efforcés de présenter la théorie des codes de la manière la plus intuitive possible, sans trop entrer dans les détails mathématiques.

Dans la quatrième partie, nous rappelons brièvement quelques faits de *théorie de la complexité* initiée par Rabin, McNaughton, Yamada, Hartmanis et Stearns dans les années 1960. Cette théorie est constamment présente dans la problématique de la cryptographie. En effet, l'usage d'un chiffre est une course entre les utilisateurs légitimes du système de chiffrement et des adversaires qui cherchent à retrouver leurs messages. Il faut donc que le temps de calcul d'une cryptanalyse excède l'espérance de vie de la confidentialité du cryptogramme. La théorie de la complexité permet de ranger des problèmes algorithmiques dans différentes classes selon le temps de fonctionnement de leurs algorithmes de résolution. Nous y traitons la complexité de certains problèmes liés à la théorie des codes (notamment celui du décodage) et nous présentons quelques problèmes algorithmiques qui nous serviront dans la partie sur la cryptographie à clé publique, en particulier pour définir la notion de fonction à sens unique.

Enfin, nous introduisons la *cryptologie* ou science du chiffre qui permet de transmettre des messages en préservant leur confidentialité en présence d'adversaires. Cette discipline regroupe à la fois l'art de concevoir de bons chiffres (cryptographie) et celle de les cryptanalyser. Dans cette partie nous nous sommes efforcés de respecter cette interaction en proposant pour la plupart des chiffres présentés, soit leur cryptanalyse lorsque celle-ci est connue, soit des attaques qui présentent leurs principales faiblesses, tant pour les chiffres à clé secrète que pour les chiffres à clé publique. Le choix des méthodes de chiffrement repose d'une part sur leur intérêt pédagogique et sur leur intérêt «pratique» en extrayant un sous-ensemble consistant des méthodes adoptées par les différents standards. En effet, l'objectif principal de cette dernière partie est d'expliquer le fonctionnement de quelques protocoles sécurisés qui sont utilisés par Internet. Nous présentons notamment le fonctionnement d'un des

protocoles qui permettent d'assurer la sécurité des échanges du Web en chiffrant les communications. Son bon fonctionnement est généralement symbolisé par un petit cadenas verrouillé sur la fenêtre de nos navigateurs.

Utilisation

Le contenu de ce livre provient de différents enseignements dispensés à l'École Supérieure en Sciences Informatiques de l'Université de Nice Sophia-Antipolis et à l'Institut Supérieur d'Informatique et d'Automatique de l'École des Mines de Paris. Il s'inspire également de mon cours du DEA d'Informatique et de celui du DEA de Mathématiques, en collaboration avec S. Julia. C'est la raison pour laquelle il est divisé en plusieurs parties qui peuvent être lues de façon presque indépendante.

Chaque partie est découpée en plusieurs chapitres courts qui présentent une notion précise. De nombreux exemples et quelques exercices permettent d'illustrer les notions introduites et de vérifier leur bonne compréhension.

Cet ouvrage peut servir de support de cours pour des enseignements de deuxième ou de troisième cycle universitaire ou d'introduction pour des ingénieurs ou des chercheurs qui souhaiteraient se familiariser avec les différentes disciplines qui y sont présentées.

Remerciements

Tout d'abord, je dois beaucoup à la Maîtrise de Mathématiques Discrètes de l'Université de Lyon 1 et à ses enseignants-chercheurs. Ce sont eux qui m'ont fait connaître, entre autres, la théorie des codes et la cryptographie.

Je voudrais remercier J. Gruska pour m'avoir suggéré d'écrire ce livre à partir de mes notes de cours, C. Peyrat pour m'en avoir relu des versions préliminaires et H. Ben Azza pour ses encouragements.

Plusieurs personnes ont contribué à cet ouvrage : J. Leroux m'a fourni des explications sur la théorie de l'information ; P. Solé et Ling San ont répondu aux nombreuses questions que je leur ai posées sur les codes correcteurs, J. Bond, M. Bronstein et M. Santha ont éclairci des points d'algorithmique et de complexité. Je remercie également mes étudiants ; c'est grâce à leurs questions et à leurs réactions que le contenu de mes notes de cours s'est peu à peu enrichi.

Enfin, un grand merci à S. Julia. Son soutien, ses relectures et nos discussions m'ont permis de mener à bien l'écriture de ce livre.

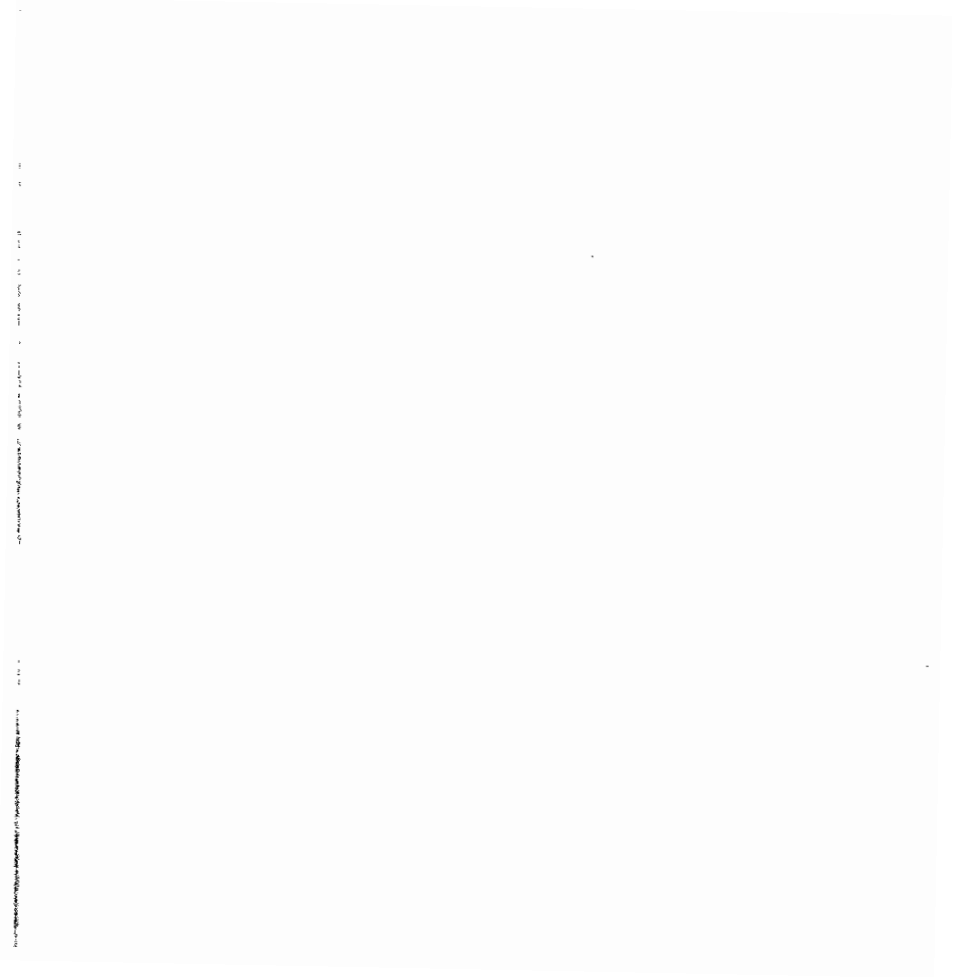


Table des matières