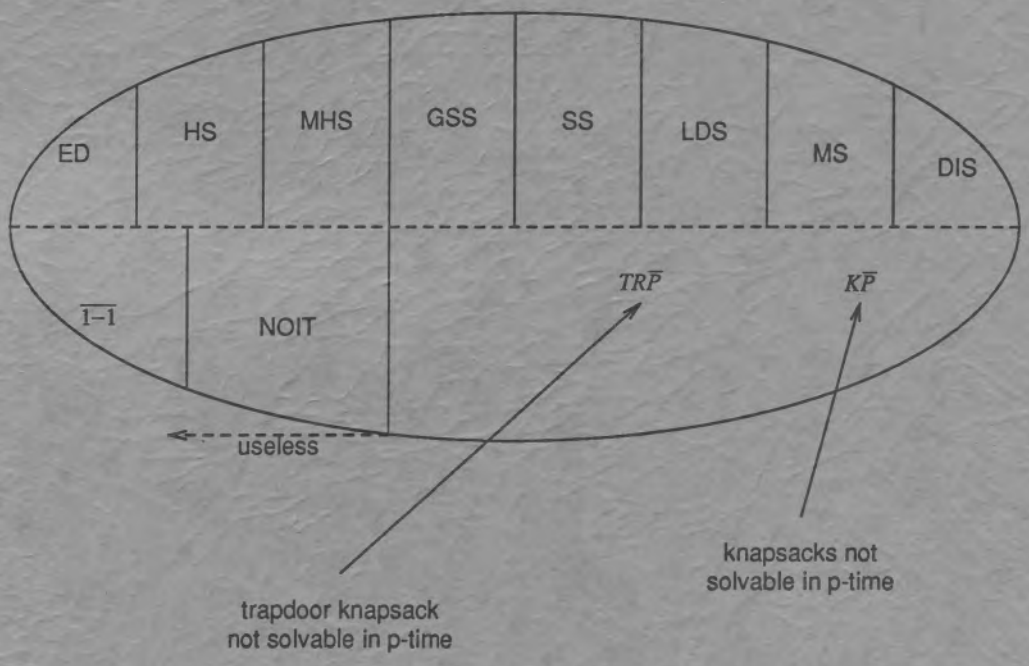
A CRYPTOGRAPHIC SERIES

50

PUBLIC KEY CRYPTOGRAPHY

CRYPTOGRAPHIC SIGNIFICANCE OF THE KNAPSACK PROBLEM

PLUS EXERCISES AND SOLUTIONS



by
Luke J. OConnor
and
Jennifer Seberry

From Aegean Park Press

Luke OConnor
Graduate Student
c/o Department of Computer Science
University College
The University of New South Wales
Australian Defence Force Academy
Canberra, ACT 2600
AUSTRALIA

Jennifer Seberry
Professor
Department of Computer Science
University College
The University of New South Wales
Australian Defence Force Academy
Canberra, ACT 2600
AUSTRALIA

ISBN: 0-89412-150-2 (soft cover)
ISBN: 0-89412-151-0 (library binding)

AEGEAN PARK PRESS
P.O. Box 2837
Laguna Hills, California, U.S.A.
tel. (714) 586-8811

Manufactured in the United States of America

Preface

This work on the *Knapsack in Cryptography* was written during Luke OConnor's honours year in the Basser Department of Computer Science at the University of Sydney.

Both authors have now moved on to other places – Luke OConnor to graduate studies at the University of Manitoba and Jennifer Seberry to Professor and Head of the Department of Computer Science at the Australian Defence Forces Academy, The University of New South Wales, Canberra.

The current exposition has been greatly improved by the extensive comments of Dr. Josef Pieprzyk and Mr. Christopher Jack and the tireless efforts of Mr. Ray Loyzaga of the Basser Department of Computer Science, to whom we express our deepest gratitude.

The original version of this thesis was typeset using the UNIX operating system on the Basser Department of Computer Science's VAX 11/780. The final version was produced commercially under Mr. Loyzaga's expert guidance.

Jennifer Seberry

INTRODUCTION

Cryptography is an art that has been practised down through the centuries, yet the knowledge that has been acquired over this period concerning its nature and misgivings is far from complete. The principal pursuit of cryptography is to provide a means by which people can communicate secretly. Though simply stated, this pursuit has proved more elusive than its humble followers had expected. History speaks well on this point. The instances of proposed solutions to the problem of secrecy that have been only partial answers or totally spurious are numerous. This is a shortcoming of an inexact science that fails to inherit the precision of the fields if borrows from. Repeatedly the insights of one person have been frustrated by those of another, and through this ongoing exchange of claim and refutation, cryptography has managed to perpetuate itself by continually postponing its own obsolescence.

Cryptography will draw upon any area that offers the potential of secrecy. Thus any method or notion that can either directly or indirectly furnish secrecy, is of interest to cryptographers. One method that has been considered is derived from the knapsack problem. Interest in the applications of the knapsack problem to cryptography has arisen with the advent of public key cryptosystems. It may seem odd that in attempting to solve one problem another is introduced, but this is consistent with the public key approach. The knapsack problem is a well documented problem and all research into its properties have lead to the conjecture that it is difficult to solve. What is hoped is that the apparent difficulty of the knapsack problem may be harnessed and used in turn to provide a basis for secret and secure communication.

This paper is a thorough treatment of the knapsack problem with respect to cryptography, and other related topics. At present there is a great deal of doubt concerning whether the knapsack problem can function reliably and efficiently in a public key environment. The main undertaking of this study is to examine if this doubt is well founded. And if this doubt is well founded, then is there any future for knapsack systems in cryptography? This examination will include an investigation of

- the inherent difficulty of the knapsack problem
- the virtues of the knapsack problem with respect to cryptography
- the known flaws of knapsack cryptosystems
- potential and possible flaws of the knapsack cryptosystems

The authors assume that the reader is a novice in the field of cryptography. Chapter 1 introduces basic complexity theory and the classes P and NP, and the notion of intractiblity is established. If the reader feels comfortable with these concepts then this section should skipped. Chapter 2 makes some comments on the work of Shannon and Information Theory. Chapter 3 explains the fundamental concepts of cryptography, especially the terms cryptosystem and

cryptanalysis. The certificational attacks are dealt with, and the critical notions of security and intractability are related. Chapter 4 then reviews classical cryptosystems and highlights their shortcomings. One way functions are described and their importance to the concept of public key cryptosystems is explained. Chapter 5 introduces the knapsack problem, describing its origins and variants. Its application to cryptography is demonstrated. In Chapter 6 the knapsack cryptoalgorithms are explained, such as the Merkle-Hellman and Graham-Shamir systems. Chapter 7 shows how the knapsack problem may be used to authenticate messages. Chapter 8 is an examination of modular transformations and their properties. Chapter 9 begins the criticism of the knapsack systems, starting with the single-iterated Merkle-Hellman system. Chapter 10 examines basis reduction which is the fundamental tool cryptanalysts of knapsack systems have utilised. Also the cryptanalysis of the Graham-Shamir knapsack is presented. Chapter 11 describes some attacks that achieve partial success including low density knapsacks, multiplicative knapsacks and iterative knapsacks.

Chapter 13 tells of current research and the future.

TABLE OF CONTENTS