PUBLIC KEY CRYPTOGRAPHY

CRYPTOGRAPHIC SIGNIFICANCE OF THE KNAPSACK PROBLEM

PLUS EXERCISES AND SOLUTIONS

by
Luke J. O'Connor
and
Jennifer Seberry

From Aegean Park Press
Preface

This work on the *Knapsack in Cryptography* was written during Luke O'Connor'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 O'Connor 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 it 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 intractability 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

1. ALGORITHMS AND COMPLEXITY .............................................. 1
   1.1 PROBLEMS AND ALGORITHMS .................................. 3
   1.2 THE CLASSES $P$ AND $NP$ ...................................... 6
   1.3 COMPLEXITY OF SELECTED PROBLEMS USED IN CRYPTOLOGY .............. 12
      1.3.1 Factorization Problems .................................. 12
      1.3.2 Discrete Logarithm Problem .............................. 15
      1.3.3 Knapsack Problem .................................... 21
2. A NOTE ON INFORMATION THEORY ........................................ 25
3. SECURITY AND CRYPTOGRAPHY .......................................... 35
4. CRYPTOSYSTEMS .......................................................... 43
   4.1 CLASSICAL CRYPTOSYSTEMS ...................................... 43
   4.2 PUBLIC KEY CRYPTOSYSTEMS .................................... 45
      4.2.1 One Way Functions ...................................... 45
      4.2.2 Public Key Cryptography ................................. 46
      4.2.3 The Public Key Approach ................................. 47
      4.2.4 Comments on Public Key Cryptography .................... 48
5. THE KNAPSACK PROBLEM .................................................. 53
   5.1 DEFINITION AND ORIGINS ......................................... 53
   5.2 APPLICATIONS TO CRYPTOGRAPHY ................................. 57
6. KNAPSACKS AND SECRECY ................................................ 63
   6.1 PROPOSED CRYPTOALGORITHMS ................................... 63
7. KNAPSACKS AND AUTHENTICATION ...................................... 75
8. AN EXAMINATION OF MODULAR TRANSFORMATIONS .......................... 87
9. THE FIRST CRYPTANALYSIS ............................................. 99
   9.1 THE WORK OF SHAMIR ........................................... 99
   9.2 CIRCUMVENTING SHAMIR'S ATTACK ................................ 104
   9.3 ANOTHER WAY TO INVERT A MERKLE-HELLMAN KNAPSACK ............... 105
10. BASIS REDUCTION AND SHORT VECTORS ................................ 109
11. PARTIAL CRYPTANALYSIS ................................................. 115
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>LOW DENSITY KNAPSACKS</td>
<td>115</td>
</tr>
<tr>
<td>11.2</td>
<td>COMMENTS ON THE MULTIPLICATIVE KNAPSACK</td>
<td>118</td>
</tr>
<tr>
<td>11.3</td>
<td>COMMENTS ON THE MULTI-ITERATED KNAPSACK</td>
<td>120</td>
</tr>
<tr>
<td>12.</td>
<td>CONCLUSION</td>
<td>123</td>
</tr>
<tr>
<td>13.</td>
<td>CURRENT RESEARCH AND WHAT THE FUTURE HOLDS</td>
<td>129</td>
</tr>
<tr>
<td></td>
<td>APPENDIX 1</td>
<td>133</td>
</tr>
<tr>
<td></td>
<td>APPENDIX 2</td>
<td>135</td>
</tr>
<tr>
<td></td>
<td>APPENDIX 3</td>
<td>157</td>
</tr>
<tr>
<td></td>
<td>BIBLIOGRAPHY</td>
<td>161</td>
</tr>
<tr>
<td></td>
<td>INDEX</td>
<td>175</td>
</tr>
<tr>
<td></td>
<td>AUTHOR INDEX</td>
<td>177</td>
</tr>
</tbody>
</table>