Preface

The origins of this book are part of an interesting period of my life. A period that saw me move from a shy and disorganized young adult, into a software developer who has toured various parts of the world, and met countless new friends and colleagues. It all began in December of 2001, nearly five years ago. I started a project that would later become known as LibTomCrypt, and be used by developers throughout industry worldwide.

The LibTomCrypt project was originally started as a way to focus my energies on to something constructive, while also learning new skills. The first year of the project taught me quite a bit about how to organize a product, document and support it and maintain it over time. Around the winter of 2002 I was seeking another project to spread my time with. Realizing that the math performance of LibTomCrypt was lacking, I set out to develop a new math library.

Hence, the LibTomMath project was born. It was originally merely a set of patches against an existing project that quickly grew into a project of its own. Writing the math library from scratch was fundamental to producing a stable and independent product. It also taught me what sort of algorithms are available to do operations such as modular exponentiation. The library became fairly stable and reliable after only a couple of months of development and was immediately put to use.

In the summer of 2003, I was yet again looking for another project to grow into. Realizing that merely implementing the math routines is not enough to truly understand them, I set out to try and explain them myself. In doing so, I eventually mastered the concepts behind the algorithms. This knowledge is what I hope will be passed on to the reader. This text is actually derived from the public domain archives I maintain on my www.libtomcrypt.com Web site.

When I tell people about my LibTom projects (of which there are six) and that I release them as public domain, they are often puzzled. They ask why I did it, and especially why I continue to work on them for free. The best I can explain it is, “Because I can”–which seems odd and perhaps too terse for adult conversation. I often qualify it with “I am able, I am willing,” which perhaps explains it better. I am the first to admit there is nothing that special with what I have done. Perhaps others can see that, too, and then we would have a society to be proud of. My LibTom projects are what I am doing to give back to society in the form of tools and knowledge that can help others in their endeavors.

I started writing this book because it was the most logical task to further my goal of open academia. The LibTomMath source code itself was written to be easy to follow and learn from. There are times, however, where pure C source code does not explain the algorithms properly–hence this book. The book literally starts with the foundation of the library and works itself outward to the more complicated algorithms. The use of both pseudo–code and verbatim source code provides a duality of “theory” and “practice” the computer science students of the world shall appreciate. I never deviate too far from relatively straightforward algebra, and I hope this book can be a valuable learning asset.

This book, and indeed much of the LibTom projects, would not exist in its current form if it were not for a plethora of kind people donating their time, resources, and kind words to help support my work. Writing a text of significant length (along with the source code) is a tiresome and lengthy process. Currently, the LibTom project is five years old, composed of literally thousands of users and over 100,000 lines of source code, TEX, and other material. People like Mads Rassmussen and Greg Rose were there at the beginning to encourage me to work well. It is amazing how timely validation from others can boost morale to continue the project. Definitely, my parents were there for me by providing room and board during the many months of work in 2003.

Both Greg and Mads were invaluable sources of support in the early stages of this project. The initial draft of this text, released in August 2003, was the project of several months of dedicated work. Long hours and still going to school were a constant drain of energy that would not have lasted without support.

Of course this book would not be here if it were not for the success of the various LibTom projects. That success is not only the product of my hard work, but also the contribution of hundreds of other people. People like Colin Percival, Sky Schultz, Wayne Scott, J Harper, Dan Kaminsky, Lance James, Simon Johnson, Greg Rose, Clay Culver, Jochen Katz, Zhi Chen, Zed Shaw, Andrew Mann, Matt Johnston, Steven Dake, Richard Amacker, Stefan Arentz, Richard Outerbridge, Martin Carpenter, Craig Schlenter, John Kuhns, Bruce Guenter, Adam Miller, Wesley Shields, John Dirk, Jean–Luc Cooke, Michael Heyman, Nelson Bolyard, Jim Wigginton, Don Porter, Kevin Kenny, Peter LaDow, Neal Hamilton, David Hulton, Paul Schmidt, Wolfgang Ehrhardt, Johan Lindt, Henrik Goldman, Alex Polushin, Martin Marcel, Brian Gladman, Benjamin Goldberg, Tom Wu, and Pekka Riikonen took their time to contribute ideas, updates, fixes, or encouragement throughout the various project development phases. To my many friends whom I have met through the years, I thank you for the good times and the words of encouragement. I hope I honor your kind gestures with this project.

I'd like to thank the editing team at Syngress for poring over 300 pages of text and correcting it in the short span of a single week. I'd like to thank my friends whom I have not mentioned, who were always available for encouragement and a steady supply of fun. I'd like to thank my friends J Harper, Zed Shaw, and Simon Johnson for reviewing the text before submission. I'd like to thank Lance James of the Secure Science Corporation and the entire crew at Elliptic Semiconductor for sponsoring much of my later development time, for sending me to Toorcon, and introducing me to many of the people whom I know today.

Open Source. Open Academia. Open Minds.

Tom St Denis
Toronto, Canada
May 2006