Preface

Here we are, in the preface of my 2nd text. I do not know exactly what to tell you, the reader, other than this one is more dramatic and engaging than the last. I do not want to leak too many details, but let's just say that RSA has an affair with SHA behinds MD5's back. In all seriousness, let's get down to business now.

As I write this, nearly on the eve of the print date, I anticipate the final product and hope that I have hit my target thesis for the text. This text is the product of a year's worth of effort, spanning from early 2006 to nearly November of 2006. I spent many evenings writing after work; my only hope is that this text reaches the target audience effectively. It certainly was an entertaining process, albeit at times laborious, and like my first text, well worth it.

First, I should explain who the authors are before I go into too much depth about this text. This text was written mostly by me, Tom St Denis, with the help of my co-author, Simon Johnson, as a technical reviewer. I am a computer scientist from Ontario, Canada with a passion for all things cryptography related. In particular, I am a fan of working with specialty hardware and embedded systems.

My claim to fame and probably how you came to know about this text is through the LibTom series of projects. These are a series of cryptographic and mathematic libraries written to solve various problems that real-life developers have. They were also written to be educational for the readers. My first project, *LibTomCrypt*, is the product of nearly five years of work. It supports quite a few useful cryptographic primitives, and is actually a very good resource for this text. Continuing the line of cryptographic projects, I started *LibTomMath* in 2002. It is a portable math library to manipulate large integers. It has found a

home with *LibTomCrypt* as one of the default math providers, and is also integral to other projects such as *Tcl* and *Dropbear*. To improve upon *LibTomMath*, I wrote *TomsFastMath*, which is an insanely fast and easy to port math library for cryptographic operations.

I wrote all of these projects to be free, not only in the sense that people can acquire them free of charge, but also in the sense that there are no strings attached. They are, in fact, all public domain. For me, at least, it was not enough just to provide code. I also provide documentation that explains how to use the projects. Even that was not enough. I also document and clean the source code; the code itself is of educational value. The first project to be used in this manner was the *LibTomMath* project. In 2003, I wrote a text, *BigNum Math: Implementing Cryptographic Multiple Precision Arithmetic* (ISBN:1597491128), which Syngress Publishing published in 2006. The project literally inserts code from the project into the text. Coupled with pseudo-code, the text teaches how to manipulate large integers quite effortlessly.

The LibTom projects are themselves guided by a simple motto that I've developed over the years.

"Open Source. Open Academia. Open Minds"

What this means is that, by providing source code along with useful documentation and supporting material, we can educate others and open their minds to new ideas and techniques. It extends the typical open source philosophy in an educational capacity. For instance, it is nice that the GNU Compiler Collection (GCC) is open source, but it is hardly an educational project. Enough of this though; this line of thinking is the subject of my next text (due sometime in 2009).

I continue to work on my LibTom projects and am constantly vigilant so as to promote them whenever possible. I regularly attend conferences such as Toorcon to spread the word of the LibTom philosophy in hopes of recruiting new open-source developers to the educational path.

So, who is Simon? Simon Johnson is a computer programmer from England. He spends his days reading about computer security and cryptographic techniques. Professionally, he is a security engineer working with C# applications and the like. Simon and I met through the Usenet wasteland that is sci.crypt, and have collaborated on various projects. Throughout this text, Simon played the role of technical reviewer. His schedule did not quite afford

him as much time to help on this project as he would have liked, but his help was still crucial. It is safe to say we can expect a text or two from Simon in the years to come.

So what is this book about? *Cryptography for Developers*. Sounds authorative and independent: Right and wrong. This text is an essential *guide* for developers who are not cryptographers. It is not, however, meant to be the only text on the subject. We often refer to other texts as solid references. Definitely, you will want a copy of "BigNum Math." It is an essential text on implementing the large integer arithmetic required by public key algorithms. Another essential is *The Guide to Elliptic Curve Cryptography* (ISBN 038795273X), which covers, at a nice introductory level, all that a developer requires to know about elliptic curve algorithms. It is our stance that we do you, the reader, more good by referring to well-read texts on the subject instead of trying to duplicate their effort. There are also the standards you may want to pick up. For instance, if you are to implement RSA cryptography, you really need a copy of *PKCS #1* (which is free). While this text covers PKCS #1 operations, having the standard handy is always nice. Finally, I strongly encourage the reader to acquire copies of the LibTom projects to get first-hand experience working with cryptographic software.

Who is this book for? I wrote this book for the sort of people who send me support e-mail for my projects. That is not to say this text is *about* the projects, merely about the problems users seem to have when using them. Often, developers tasked with security problems are not cryptographers. They are bright people, who, with careful guidance, can implement secure cryptosystems. This text aims to guide developers in their journey towards solving various cryptographic problems. If you have ever sat down and asked yourself, "Just how do I setup AES anyways?" then this text is for you.

This text is **not** for people looking at a solid academic track in cryptography. This is not the Handbook of Applied Cryptography, nor is it the Foundations of Cryptography. Simply put, if you are not tasked with implementing cryptography, this book may not be for you. This is part of the thinking that went into the design and writing of this text. We strived to include enough technical and academic details as to make the discussions accurate and useful. However, we omitted quite a few cryptographic discussions when they did not fit well in the thesis of the text.

I would like to thank various people for helping throughout this project. Greg Rose helped review a chapter. He also provided some inspiration and insightful comments. I would like to thank Simon for joining the project and contributing to the quality of the text. I would like to thank Microsoft Word for giving me a hard time. I would like to thank Andrew, Erin, and the others at Syngress for putting this book together. I should also thank the LibTom project users who were the inspiration for this book. Without their queries and sharing of their experiences, I would never have had a thesis to write about in the first place.

Finally, I would like to thank the pre-order readers who put up with the slipped print date. My bad.

—Tom St Denis
Ottawa, Ontario, Canada
October 2006