A New Popular Science Book about Cryptography

Keith Martin

I have just written another book about cryptography. Why?

It's a good question! Maybe because I enjoy writing. Maybe because I felt I had something to say. Maybe, also, because I think cryptography matters to everyone, but not everyone realises.

My first book, Everyday Cryptography, is, at heart, a textbook. I decided to write it because I encountered a steady stream of requests from students on the Introduction to Cryptography module of Royal Holloway's MSc Information Security asking for recommended background reading, and I struggled to suggest any. This module adopts a non-mathematical approach to cryptography but most books tackle this subject as an application of mathematics, so were not suitable. Fred Piper and Sean Murphy wrote an excellent Very Short Introduction to Cryptography, but it is exactly what it claims to be on the cover: very short! It's a useful early read, but does not provide enough detail to support students on a postgraduate programme. Everyday Cryptography provides this missing resource. Writing such a book is a huge task and by the time I had prepared the second edition of Everyday Cryptography, I felt I was done with book writing…

Wrong! The motivation to start the whole process all over again came from three very different places.

While Everyday Cryptography is primarily a textbook and guide for security professionals trying to get to grips with cryptography, I also entertained a vague hope that a (keen) general interest reader might be able to engage with it. I soon realised this was a fantasy, particularly after my father (who has a mathematical background) confessed to having started to read it, but eventually found it too heavy going. A more general reader would clearly need a different kind of book.

In December 2015, I attended a talk by the BBC's security correspondent Gordon Corera, author of the superb book Intercept, which discusses the history of surveillance. Although he clearly had a deep appreciation of the importance of cryptography, I was struck by his deference and hesitation whenever he strayed close to discussing cryptographic technology itself. This reaction is one I have seen repeatedly among professionals working in cybersecurity. It made me think: if these guys are uncomfortable with their own understanding of cryptography, what hope is there for everyone else? Could I write a book that could help to demystify the role of cryptography, not just for professionals such as Gordon Corera, but for the public at large?

Then in 2016, I was asked to contribute some lessons on cryptography as part of a Coursera MOOC (Massive Open Online Course), designed to introduce the wider public to information security. These lessons consist of six ten-minute videos. Could I present cryptography in just one hour to a general audience? I thus developed a concise six-segment narrative that explained the role cryptography plays in cybersecurity. These lessons have proved popular, with over 100,000 unique visitors and almost 30,000 enrolments, and provided the launch pad for a new book.

So what, in essence, is this new book about?

Well, it's not a textbook. In a UK bookshop it will belong on the shelves associated with "popular science". The aim of the book is to open readers' eyes to the critical role cryptography plays in supporting our everyday lives. It examines why we need cryptography in cyberspace, what it does, how we use it, and what its limitations are. One of main purposes of doing so is to use the explanation of cryptography to provide readers with a more profound perspective on their own personal security when they are operating in cyberspace. I also want to help readers adopt a more informed position about the post-Snowden world. The book thus discusses the role cryptography plays in the wider social debates concerning how society should balance personal freedom with control of information.

Early in the writing process I had dinner with a former colleague. When I told him I was writing a popular science book about cryptography he replied, "Why bother? Didn't Simon Singh already do that?" Well, yes, he did. The Code Book is a very accessible 1990's book about cryptography, which many of you may have read. But The Code Book takes a much more historical perspective and predates the rise of cyberspace as a place where we live our everyday lives. The Code Book essentially presents cryptography as cool science with an interesting past. I have chosen to present cryptography from the perspective of our contemporary need for security in cyberspace. I see The Code Book as complementary, and certainly not a direct rival. I would love all The Code Book fans, however, to read my book and see cryptography in modern light.

Writing any type of book is not a fast process, but writing a "trade book" of this type has been painfully slow and quite different to academic publishing. I started writing in autumn 2016 and developed the first draft over the subsequent twelve months. I soon learned that getting visibility with publishers requires having an agent. After a false start, I was very lucky to make contact with Peter Tallack at the Science Factory, who helped me prepare a formal book proposal in autumn 2017. By spring 2018 I had a draft that I was willing to share, and several friends and colleagues, including Fred Piper, provided valuable feedback. In autumn 2018 Peter took the book proposal to market and I secured conversations with several publishers, eventually formalising a deal with WW Norton, an independent employee-owned publisher in New York. The book then journeyed through the pre-publication process in 2019, including editorial review, copy-editing, proof-editing and the thorny issues of title and cover design. I spend much of my working life "red-penning" student manuscripts, but in 2019 I got a healthy dose of my own medicine!

The last words were tinkered with in December 2019 and the book is finally due to be published in May 2020 in the US, the following month in the UK. There's even a Chinese and a Korean edition already commissioned, but I'm certainly not offering to proof-read either of them. I hope the book will achieve its aims, but only readers can deliver the verdict on that.