Preface

Nowadays cryptography permeates our lives, even if it is largely transparent and most people are blissfully unaware of its crucial role. Cryptography, and in particular "modern cryptography," forms one of the foundations of the information society. It is thus hard to imagine that only a few decades ago cryptography was the sole preserve of governments, spies, diplomats, and the military. In the 1960s, when David Kahn conceived the idea of penning a history of secret writing, it was virtually impossible to find an account of the subject, let alone a readable one. Virtually no research was conducted in the "open," academic world and no university offered courses on cryptography. Of course, work went on in the making and breaking of codes in secret in the world's intelligence agencies: NSA, GCHQ, the KGB etc., but none of this saw the light of day.

Thus, Kahn's idea to write a major history of the subject was audacious and ambitious, and indeed prescient. It is hard to gauge the impact of the book, but it seems clear that many people who went on to contribute to the development of modern cryptography had their appetite whetted by reading *The Codebreakers*; certainly this is true of many of the contributors to this book. Kahn's book is remarkable in having a blend of technical detail mixed with tales of daring and adventure. It is a superb piece of scholarship, minutely researched but without the dryness that so often comes with scholarship.

In 2010 David turned 80 and a number of us decided to arrange a Fest in Luxembourg to honour the event (http://www.codebreakers2010.uni.lu/index.html). The event was highly successful and enjoyable, with talks by many of the world's leading cryptographers and security experts. Several of the talks resulted in chapters in this Festschrift. A highlight of the event was a fine banquet in Luxembourg's Chateau de Bourglinster.

Since the publication of *The Codebreakers*, the world has changed dramatically: We learnt of the breaking of the German Enigma, which heralded the age of the computer, and witnessed the advent of public key cryptography and enabled the Internet to become the medium of social and commercial interaction it is today. Cryptography and information assurance now form major academic disciplines with thousands of researchers and a proliferation of conferences and courses. The discovery in the 1970s of public key cryptography revolutionized the subject and brought it out of the shadows. The realization that the ability to encrypt does not necessarily entail the ability to decrypt overturned (implicit) assumptions that had held sway for centuries. Arguably this insight is comparable in its impact on cryptography as that of Einstein's Theory of Relativity, with the realization that space is not absolute, on physics.

We felt it appropriate therefore to call the present Festschrift *The New Codebreakers* to pay homage to Kahn's groundbreaking contribution and to carry the story forward into the new era.

It is now five years since the Fest in 2010, and David is now 85, so this Festschrift serves to honour this later anniversary. We are delighted to have been able to gather 33 chapters from distinguished members of the cryptography, security, and history of intelligence communities. The chapters cover a wide range from theoretical cryptography to security applications and from the history of intelligence to recreational applications. We hope you will all enjoy reading this as we enjoyed reading David's book all those years ago.

We would like to thank again all those who attended David's Fest in 2010, especially those who gave talks, and all those who contributed chapters to this volume.

November 2015

David Naccache
Peter Y.A. Ryan
Jean-Jacques Quisquater

http://www.springer.com/978-3-662-49300-7

The New Codebreakers
Essays Dedicated to David Kahn on the Occasion of His 85th Birthday
Ryan, P.Y.A.; Naccache, D.; Quisquater, J.-J. (Eds.)
2016, XIV, 551 p. 135 illus., Softcover
ISBN: 978-3-662-49300-7