Review of the book

"Introduction to Cryptography with Open-Source Software"

by Alasdair McAndrew

Victoria University, Melbourne, Australia

CRC Press, Taylor & Francis Group, 2011

ISBN: 978-1-4398-2570-9

Abderrahmane Nitaj
LMNO, Université de Caen Basse Normandie, France

February 2014

1 Summary of the review

Introduction to Cryptography with Open-Source Software is a well written text book covering many aspects: an introduction to cryptography, a clever use of the open source algebra system Sage and various exercises on cryptography and Sage. It provides a very good understanding of practical cryptography. Many mathematical algorithms and cryptographic schemes are discussed in detail and illustrated with comprehensible examples and tables as well as the corresponding codes with Sage. The mathematics are very easy to follow which makes the book more readable for the advanced undergraduate or graduate student. It will also be of interest to professionals looking for a clear and concise introduction to cryptography.

2 Summary of the book

The book is organized into 14 chapters and contains two appendices.

- **Chapter 1: Introduction to cryptography.** Chapter 1 is an introduction, containing a high-level overview of cryptography. This includes basic definitions, some cryptographic problems and protocols, as well as an introduction to computer security. The chapter presents some simple ciphers and contains a glossary of the most used terms in cryptography.

- **Chapter 2: Basic number theory.** Chapter 2 presents the basic tools from number theory that are used in cryptography. The chapter investigates the basic properties of prime numbers, factorization and modular arithmetic. More number theoretical properties and theorems are presented. This includes Fermat's theorem, Euler's totient function and theorems, the Chinese remainder theorem, the Euclidean algorithm and the Euclidean extension algorithm, quadratic residues, Legendre's symbol and some methods for primality testing including the Miller-Rabin test.

- **Chapter 3: Classical cryptosystems.** Chapter 3 presents some classical well known cryptosystems. The objective of this chapter is to introduce the reader with very simple cryptographic systems. This includes the Caesar cipher, the translation ciphers, the transposition ciphers, the Vigenère cipher and its cryptanalysis, the permutation ciphers, and the matrix ciphers and their cryptanalysis. Each cipher is presented with an introduction, Sage examples and cryptanalysis.

- **Chapter 4: Introduction to information theory.** Chapter 4 is devoted to introduce the information theory which serves as a formal measurement of the usefulness of a cryptosystem. In this short chapter, the following notions are discussed: entropy, how to quantify the secrecy of a cryptosystem, the redundancy of English, and unicity distance of a ciphertext.

- **Chapter 5: Public-key cryptosystems based on factoring.** Chapter 5 presents a detailed description of the main cryptosystems based on factorization including the RSA and the Rabin cryptosystems. Also, the chapter describes the most known and popular attacks on these cryptosystems. Moreover, the chapter presents general notions of security of a public-key cryptosystem. Finally, the chapter presents some methods for factoring large integers, including Pollard's rho method.

- **Chapter 6: Public-key cryptosystems based on logarithms and knapsacks.** This chapter discusses the most popular public key cryptosystems where the problem of the discrete logarithm is involved. Its starts with the El Gamal cryptosystem and its use with Sage and presents the Shanks baby step, giant step method for computing the discrete logarithm. The well know Diffie-Hellman key exchange is then presented as well as the principles of the knapsack cryptosystems and the way to break them using the LLL algorithm.

- **Chapter 7: Digital signatures.** This chapter introduces the theory of digital signatures. Digital signatures are very important in modern cryptography. The chapter gives the basic requirements of a digital signature and describes in detail the digital signature schemes based on the RSA, Rabin and El Gamal cryptosystems as well as the Digital Signature Algorithm (DSA).

- **Chapter 8: Block ciphers and the data encryption standard.** In this chapter, the basic concept of a block cipher is presented. It includes the main definitions needed to study block ciphers and their security. It also describes the substitution and permutation ciphers as well as the Data Encryption Standard (DES) and Feistel ciphers. An important part of the chapter is devoted to discuss the DES algorithm including Simplified DES (sDES), the S-box substitution and the security of DES. It is a very useful description of the DES algorithm with many examples and comprehensive exercises.

- **Chapter 9: Finite fields.** Finite fields are in the heart of modern cryptography and it is important to study their properties. In this chapter, finite fields are studied, both theoretically and experimentally. The chapter starts with groups and rings and then introduces the theory of finite fields. Also, the chapter gives various examples of finite fields such as $GF(2^n)$. It describes the main arithmetic operations on finite fields including the multiplication and the inversion. Most of operations are illustrated with many working examples.

- **Chapter 10: The Advanced Encryption Standard.** This chapter is devoted to the Advanced Encryption Standard (AES), the current NIST standard for secret key encryption. It includes a historical introduction to AES as well as its basic structure, encryption and decryption. It also gives an experimental approach of AES using Sage and investigates its security.

- **Chapter 11: Hash functions.** In this chapter, the main requirements of the hash functions are studied. The chapter describes the properties to be satisfied by a hash function, the use of hash functions, their security and how to construct a hash function. Also, the chapter describes some provably secure hash functions such as Shamir's hash function, Chaum, van Heijst, Pfitzmann hash function, the Zémor-Tilich hash function and the Modular Arithmetic Secure Hash (MASH) hash functions. The chapter terminates with the description of the Message Authentification Codes (MAC) and its use in detecting message tempering and forgery.

- **Chapter 12: Elliptic curves and cryptosystems.** The theory of elliptic curves is very huge and has many applications in various areas. Elliptic curves are used in cryptography because of the hardness of the elliptic discrete logarithm problem. This chapter starts by describing the basic definitions to study an elliptic curve, and describes the point doubling and addition on an elliptic curve. It also describes the elliptic curve based cryptosystems, such as the elliptic curve version of El Gamal cryptosystem, its security and its implementation using Sage. A similar study is performed on the Menezes-Vanstone cryptosystem as well as the elliptic curve signature. The chapter terminates with a detailed study of the pairing-based cryptography which involves the arithmetic operations on elliptic curves. A Sage example is presented.

- **Chapter 13: Random numbers and stream ciphers.** In this chapter, random numbers are studied. Random numbers are used in many cryptosystems. The chapter begins by various definitions related to random numbers and random number generators (RNG). This includes pseudo-random number generators (PRNG), cryptographically secure random number generators (CSRNG), linear congruential random number generators, and ISAAC and Fortuna. The chapter describes also stream ciphers, RC4, and the Blum-Goldwasser cryptosystem.
- **Chapter 14: Advanced applications and protocols.** This chapter describes some advanced cryptographic protocols. This includes the secure multi-party computation, zero knowledge proofs, oblivious transfer, digital cash and electronic voting.
- **Appendix A: Introduction to Sage.** This appendix shows how to obtain install and run Sage under Linux, Windows or MacOS. It then gives an introduction to the Sage functionalities and various arithmetical functions. Also, it provides the basic of programming using Sage.
- **Appendix B: Advanced Computational Number Theory.** In this appendix, some useful computational number theoretical algorithms are presented such as the quadratic sieve method for factorization, the AKS primality test, and the baby step, giant step for computing discrete logarithms.

3 What is the book like (style)?

The book is well-written with clear explanations of the principles of cryptography. It does not assume any mathematical or advanced computer science background. It provides detailed insights into cryptography with many examples and experiments using the open source software Sage. Each section includes clear definitions, examples and Sage codes so that the reader can easily test most of the notions used in that section.

4 Would you recommend this book?

I recommend this book to advanced undergraduates and beginning graduate students interested in the theory and practice of cryptography. I also recommend this book to practitioners already in the business.

The reviewer is a Researcher at the Department of Mathematics at the University of Caen, France.