Review of the book

"Introduction to Cryptography with Maple"

by Gomez Pardo, Jose Luis

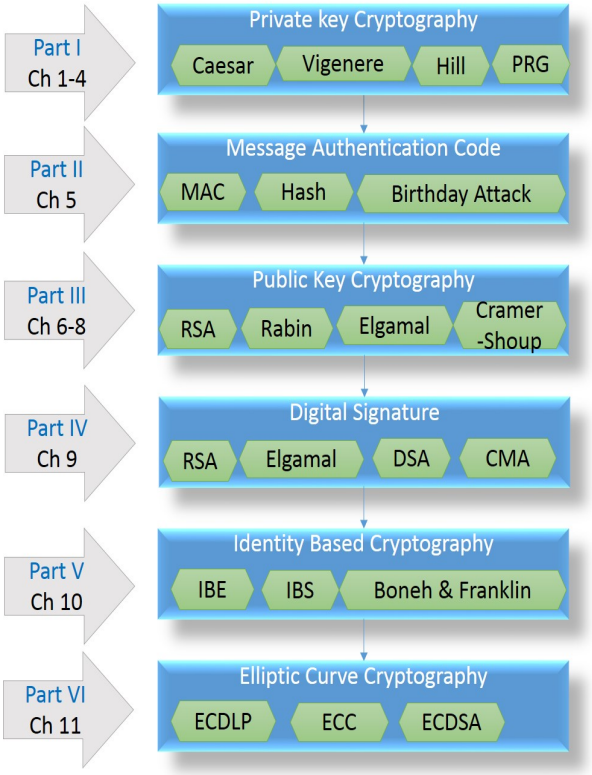
Springer, 2012

ISBN: 978-3-642-32166-5

Nishant Doshi
MEFGI, Gauridad Campus, India

1 Summary of the review

In today's e-world, everything is available as single click. Indeed, this also requires the security of the messages and also the proper authentication of it too. From the ancient era, there are various ciphers (aka security suite) proposed and analyzed by researchers. One can see that information security is one of the core subject in Undergrad and Postgrade students in various well known universities. Researchers are using various tools to perform the different ciphers. This book is first of its kind to show the use of MAPLE software to implement almost all cryptographic ciphers. One thing that I like and recommend to others that, use only one software throughout the book to implement the mentioned protocols. This is helpful for readers to be suitable with one style of programming. I suggest to add the further finding and list of real time scenarios for each chapter to be helpful at personal/organizational/researcher level. The bird eye view of the book is given in below figure.



For the researchers, this book gives the fundamentals understanding of the cryptographic protocols from the ancient era to the present. I will recommend this book to the UG students to strengthen their fundamentals on cryptography. For the PG student (and researchers too) to get the well depth understanding with further scope of improvements in the methods of cryptographic protocol analysis using MAPLE tool.

2 Summary of the book

Chapter 1 This chapter starts with cryptography from the historic *ceaser* cipher and incrementally discuss about the *vigenre* and *hill* cipher. I like the last section *Some Conclusion* which focuses on uses of these techniques in today's world. The authors have shown the MAPLE code for mentioned ciphers and also the cryptanalysis of them too.

Chapter 2 This chapter is helpful to sharpen the fundamentals of basic algebra and number theory. I suggest to not skip this chapter even if reader is familiar with the concepts. This section start with the probability, division theory with crisp introduction about the group, rings and field theory. Finally it discusses the Euler theorem and finite field in the prime order groups.

Chapter 3 After the required discussion on basics, this chapter start with perfect forward secrecy notion. Indeed, random number generator is the key part to any cipher system. It is nice to see that this book covers the various pseudo random generators before starting today's cryptographic systems. This helps the reader to understand the randomness within cipher algorithms.

Chapter 4 This chapter discusses the block cipher schemes including the today's famous AES(Advance Encryption Standard) with various modes of operation. Even though public key cryptosystem is considered as breakthrough but internally it uses ciphers like AES to minimize the calculation cost on end users.

Chapter 5 Consider a scenario in which someone changes the value of plaintext without any decryption. Indeed, the receiver assume that whatever decrypted value is correct and continue with it. *How the receiver knows that whatever decrypted is correct ?* Indeed, this chapter deals with techniques through which the receiver can assure and detect any data modification in between. This chapter deals with MAC (Message Authentication Codes) and Hash functions. Finally it discuss the *Birthday Attack* on the hash functions.

Chapter 6 As the *Chap. 2* discusses the basics for symmetric key encryption, this chapter deals with the basics for the public key cryptography which will be useful in the upcoming chapters. It is nice to see that the chapter of mathematical background is discussed in advanced for the same. It discussed the primality testing to check if given number is prime or not.Then it discussed the integer factorization problem and famous Discrete Logarithm algorithms. Indeed, the mentioned algorithms are the backbone of the many security ciphers.

Chapter 7 This chapter is considered as bridge chapter from private key to public key cryptography. This chapter discusses the famous Diffie-Hellman key exchange protocol and evaluation of it in MAPLE. Finally it analyzed the Man-In-Middle attack on the Diffie-Hellman key exchange protocol.

Chapter 8 It discussed about the Public key Cryptography and its variant. It start with the well known *RSA* scheme. Then it discusses the *Rabin, Elgamal* and *cramer-Shoup* ciphers. Finally it discuss the homomorphic evaluations of the *goldwasser-micali* and *paillier* schemes. This chapter ends with the concluding remarks on the *fully homomorphic encryption* and *lattice based cryptography* domain.

Chapter 9 In old days, people verifies the hard copy by hand written signature. With technology, researcher worked on the digital signature to verify the authenticity of the signer in digital documents. Also, it requires that no one is able to forge the same signature too. This chapter discusses the DSA (Digital Signature Algorithm) and CMA schemes. Finally, it discusses the public-key infrastructure with single and multiple certificate authorities too.

Chapter 10 *Can we remember the public key of the receiver in human readable way ?* This chapter deals with this question and methods to do this. This chapter start with notion of identity based signature and encryption schemes. Finally it gives the first practical identity based encryption scheme by boneh and franklin.

Chapter 11 Finally, the final chapter deals with the todays well known cryptography technique called *elliptic curve cryptography.* Compare to traditional techniques (based on number theoretic), it requires shorter key length and thus less computation overhead on the end users. This chapter gives the nice discussion on the elliptic curve cryptography and the various hardness problems based on it. Finally it concludes with the MAPLE code of the some of the elliptic curve based schemes.

3 Comments and Recommendations

One thing that I like about this book is *how* it proves its title in each chapter. First is to give introduction to various ciphers and second it to prove the same using the MAPLE code. Indeed, the authors have nicely given the MAPLE code for each cryptography techniques. Also, the cryptanalysis of the same is given by authors using the same MAPLE tool. I hope that in future researchers will use MAPLE to design and cryptanalysis their schemes. I suggest to give real time scenarios and research direction after each chapter to give scope of improvements for the researchers and readers.

On an average, this book gives the undergraduate students (of pre-final year), postgraduate students, researchers, scientists and so on to motivate and also to study further in the cryptographic ciphers with MAPLE and how to do the analysis of them. Surely, I will suggest this book as first hand book in cryptography for UG, PG and the researchers.

The reviewer is a faculty at Department of Computer Engineering, MEFGI, India.