Part 1

Mathematical Background

Before we tackle cryptography we need to cover some basic facts from mathematics. Much of the following can be found in a number of university "Discrete Mathematics" courses aimed at Computer Science or Engineering students, hence one hopes not all of this section is new. This part is mainly a quick overview to allow you to start on the main contents, hence you may want to first start on Part 2 and return to Part 1 when you meet some concept you are not familiar with. However, I would suggest reading Section 2.2 of Chapter 2 and Section 3.1 of Chapter 3 at least, before passing on to the rest of the book. For those who want more formal definitions of concepts, there is the appendix at the end of the book.