Introduction

Number theory is not only an old and beautiful branch of mathematics, but is also (surprise!) practically useful in an everyday sense. When you pay with a credit card or connect to a website, cryptographic protocols using number-theoretic tools operate behind the scenes.

In this chapter, we discuss some of these tools.

The most popular number-theoretic cryptographic protocol, RSA (invented by Rivest, Shamir and Adleman and published around 1977) is based on our ability to generate large prime numbers and on our inability to factor large integers in a reasonable time. We will discuss this algorithm in detail later. Currently, it is under attack because quantum computers may be able to factor large integers at some point in the future.

That said, the danger is (for now) mostly theoretical, and the RSA protocol continues to be widely used. It is an exciting time to be learning number theory, when advanced cryptographic attacks need to be deterred and many potential replacement protocols (thought to be more secure against quantum attacks) are rooted in number-theoretic concepts.