Part 3

Modern Cryptography Basics

In this part we cover the basic components of modern cryptographic systems. As an overview of the chapter headings will show, modern cryptography is not just about symmetric encryption. We have other symmetric primitives such as message authentication codes, there are public key primitives such as public key encryption and digital signatures, and there are keyless primitives such as hash functions.

We also will see that behind each of these primitives is a notion of what it means for the primitive to be secure. This is the main distinction between cryptography in the twenty-first century and that which preceded it. Modern cryptography is as much about defining what we mean by something being secure as it is about actually coming up with something that achieves that security goal.