Chapter 1
Introduction to Cryptography and Data Security

This section will introduce the most important terms of modern cryptology and will teach an important lesson about proprietary vs. openly known algorithms. We will also introduce modular arithmetic which is also of major importance in public-key cryptography.

In this chapter you will learn:

■ The general rules of cryptography
■ Key lengths for short-, medium- and long-term security
■ The difference between different types of attacks against ciphers
■ A few historical ciphers, and on the way we will learn about modular arithmetic, which is of major importance for modern cryptography as well
■ Why one should only use well-established encryption algorithms
1.1 Overview of Cryptology (and This Book)

If we hear the word *cryptography* our first associations might be e-mail encryption, secure website access, smart cards for banking applications or code breaking during World War II, such as the famous attack against the German Enigma encryption machine (Fig. 1.1).

![Fig. 1.1 The German Enigma encryption machine (reproduced with permission from the Deutsches Museum, Munich)]

Cryptography seems closely linked to modern electronic communication. However, cryptography is a rather old business, with early examples dating back to about 2000 B.C., when non-standard “secret” hieroglyphics were used in ancient Egypt. Since Egyptian days cryptography has been used in one form or the other in many, if not most, cultures that developed written language. For instance, there are documented cases of secret writing in ancient Greece, namely the *scytale* of Sparta (Fig. 1.2), or the famous Caesar cipher in ancient Rome, about which we will learn later in this chapter. This book, however, strongly focuses on modern cryptographic

![Fig. 1.2 Scytale of Sparta](image)

methods and also teaches many data security issues and their relationship with cryptography.

Let’s now have a look at the field of *cryptography* (Fig. 1.3). The first thing