## Introduction

As the title of this lesson suggests, the focus is on practical aspects and on the application of the procedures. We will therefore dispense with proof of the facts presented.

The word cryptography comes from the Greek and is a composition of the words “secret”/ “hidden” and “write.” Historically, cryptography is the encryption of texts, i.e., the conversion of a plaintext into an encrypted text, the ciphertext. The decryption is accordingly the reversal of the process, i.e., the restoration of the original plaintext from a ciphertext. How exactly this encryption and decryption works is determined by an algorithm called cipher or cypher. All encryption methods (also called cryptosystems) use different algorithms.

The goal of all cryptosystems is of course to hide the contents of the plaintext from unauthorized persons by encryption. Accordingly, the strength or quality of a cryptosystem is determined by the ease with which unauthorized persons are able to restore the corresponding plaintext from a ciphertext.

Especially in today’s information age, cryptography plays an important role with regard to the security of information systems, e.g., in data transmission or the encryption of passwords. However, the idea of encrypted data transmission is much older. Many thousands of years ago, primitive cryptosystems were already being used to exchange messages and to encrypt messages. In medieval Europe, secret writings were also used to protect diplomatic correspondence. ENIGMA—a machine used by the German military for encrypting message traffic—also became very well-known during the Second World War.

In the following unit we want to introduce a very well-known and easy to understand encryption method, which was used by the famous Roman statesman and commander Gaius Julius Caesar (100 BC—44 BC), among others. Caesar used this system to encrypt military messages. Although he was demonstrably not the first to use this system, he made it more popular and is therefore often referred to as the Caesar cryptosystem or Caesar cipher.