## 9.2 Symmetric vs. Asymmetric Cryptosystems

The shift cipher just presented is an example of the symmetric cryptosystem. The term “symmetric” refers to the fact that the rule for encryption can easily be used to derive the rule for decryption. For example, if you know that the ciphertext was encrypted with the Caesar cipher, then it is clear how the decryption works: the plain text is obtained by translating each letter into the corresponding numerical value, subtracting the same value from each number and then converting the results back into a sequence of letters. Even if you do not know the agreed key, there is a very manageable number of possibilities − exactly 26, because there are only 26 different possible keys. So you can crack the code just by trying it out. From this we can draw a first important conclusion: The longer the key that is used, the better. It is not without reason that today’s cryptographic procedures often use keys with a length of 128, 256 or even greater bit length. With a 128-bit key, for example, there are already 3.4028236692093846346337460743177e+38 possibilities of how the key could look.

A big advantage of symmetric cryptography is that they are often very easy to carry out and therefore very performant.

However, they also have serious disadvantages. Apart from the problem that certain systems are easy to crack, there is the particular problem that we have to exchange the jointly agreed upon key via a secure channel in advance and then keep it secret. If the key falls into the wrong hands, the messages can easily be decrypted and read by unauthorized persons. Anyone who can encrypt can also decrypt and vice versa.

To counter these disadvantages, asymmetric cryptosystems have been developed. This is also known as public key cryptography. In contrast to symmetric cryptosystems, the communicating parties do not have to agree on a common secret key. Instead, each participant who wants to communicate with another participant via this system generates a key pair. This consists of a secret part, the private key, and a public part, the public key. The private key is kept secret and is not given to anyone. The public key is made freely accessible to every subscriber of the system—similar to a kind of telephone book where every subscriber publishes his public key.

Algorithms in asymmetric cryptosystems use the public key to encrypt a message. The decryption, i.e., the re-transformation of a ciphertext into the original plaintext, is done

Public key cryptography This type of cryptography uses a pair of keys: a public key, which is widely available, and a private key, known only to the user.

using the private key. It can only be decrypted with the exact private key that matches the public key that was used for encryption. Messages are therefore encrypted with the public key of the recipient and can only be decoded again with the corresponding private key of the recipient.

If subscriber A wants to send an encrypted message to subscriber B, he first searches for the public key of B. The message is then encrypted using the public key of subscriber B. A then sends the encrypted ciphertext to B. Subscriber B now uses his private key to decrypt this message and restore the original plaintext. No other participant in the system can decrypt the message, because this requires the secret key that only participant B knows.

The advantage of this system is obvious: The a priori key exchange is not necessary within asymmetric cryptosystems. Any number of participants can communicate with each other without the need for prior security-critical key agreements.

Unfortunately, asymmetric cryptosystems generally require significantly more computing time and memory than symmetric procedures. For this reason, both methods are sometimes combined by first transmitting the symmetric keys via a public-key cryptosystem and then transmitting the actual messages with a symmetric cryptosystem.

As a popular example of a public-key cryptosystem, we will introduce the RSA method in the following sub-unit.