6.1 One-Way Functions

We continue to use the informal definition from 4.1. An exact approach is given in Appendix B.5.

Application A natural application of one-way functions is one-way encryption. This means:

- *Everyone* can encrypt.
- *No one* can decrypt.

What is it good for if no one can decrypt? There are several meaningful applications for one-way functions, in particular for the special case of hash functions, see 6.2:

- Password management, for instance in Unix or MS Windows. No one must be able to read the password. But the operating system must be able to compare an entered password with the one it has in its data base in encrypted form. **("cryptographic matching")**
- A similar application is **pseudonymization**: Data of a person should be combined with data from the same person stored elsewhere or at other times without revealing the identity of this person.
- Another application is making **digital signatures** faster, see 6.2.
- The crucial property of asymmetric encryption is that nobody can derive the private key from the public one. However the direct naive application of one-way functions doesn't work, as we saw already for the ElGamal cipher in 4.5.

Examples of conjectured one-way functions:

1. The discrete exponential function, see 4.1.
2. Consider a bitblock cipher

   $$F\colon M \times K \longrightarrow C$$

   that resists an attack with known plaintext. A standard trick to get a one-way function $f\colon K \longrightarrow C$ from it works as follows:

   $$f(x) := F(m_0, x).$$

   In words: We take a fixed plaintext m_0—maybe the all-zero block—and encrypt it with a key that is exactly the block x to be one-way encrypted. Inverting this function amounts to an attack with known plaintext m_0 on the cipher F.

3. Let $n \in \mathbb{N}$ be a composite module. From 5.2 we know that—at least in the case where n is the product of two large prime numbers—computing square roots $\bmod n$ is probably hard. Hence the squaring map $x \mapsto x^2 \bmod n$ is a probable one-way function of the residue class ring $\mathbb{Z}/n\mathbb{Z}$. Note that calculating the inverse map is possible with additional information in form of the prime factors of n. Such an additional information is called a "trapdoor". The function is then called a "trapdoor one-way function". This is the crucial security feature of the Rabin cipher.

4. The same conclusion holds for the RSA function $x \mapsto x^e \bmod n$ with an exponent e that is coprime with $\lambda(n)$ (oder $\varphi(n)$).