CHAPTER 17

An Application Example: The RSA Cryptosystem

> The next question was the obvious one, "Can this be done with ordinary encipherment? Can we produce a secure encrypted message, readable by the authorised recipient without any prior secret exchange of the key etc?" . . . I published the existence theorem in 1970.
>
> —J. H. Ellis, "The Story of Non-Secret Encryption"

AS WE APPROACH THE END of our story we would like to investigate the possibility of testing what we have labored over chapter by chapter against a realistic and current example, one that clearly demonstrates the connection between the theme of cryptographic application and the deployment of our programmed functions. We shall make a brief excursion into the principle of asymmetric cryptosystems and then turn our attention to the RSA algorithm as the classic example of such a system, which was published in 1978 by its inventors/discoverers, Ronald Rivest, Adi Shamir, and Leonard Adleman (see [Rive], [Elli]), and which by now has been implemented worldwide.[1] The RSA algorithm is patented in the United States of America, but the patent expired on 20 September 2000. Against the free use of the RSA algorithm stood the claims of RSA Security, who possessed rights to the trade name "RSA," which triggered vehement discussion in connection with work on the standard P1363 [IEEE], with in some cases rather grotesque results, for example, the suggestion of rechristening the RSA procedure "biprime cryptography." There have also appeared less serious suggestions, such as FRA (former RSA algorithm), RAL (Ron, Adi, Leonard), and QRZ (RSA − 1). Upon expiry of their patent RSA Security weighed in with its opinion:

> Clearly, the terms "RSA algorithm," "RSA public-key algorithm," "RSA cryptosystem," and "RSA public-key cryptosystem" are well established in standards and open academic literature. RSA Security does not intend to prohibit the use of these terms by individuals or organizations that are implementing the RSA algorithm ("RSA-Security—Behind the Patent," September 2000).[2]

[1] According to `http://www.rsasecurity.com` by 1999 over three hundred million products containing RSA functions had been sold.

[2] `http://www.rsasecurity.com/solutions/developers/total-solution/faq.html`.

17.1 Asymmetric Cryptosystems

The fundamental idea behind asymmetric cryptosystems was published in 1976 by Whitfield Diffie and Martin Hellman in the groundbreaking article "New Directions in Cryptography" (see [Diff]). Asymmetric cryptosystems, in contrast to symmetric algorithms, do not use a secret key employed both for encryption and decryption of a message, but a pair of keys for each participant consisting of a public key E for encryption and a different, secret, key D for decryption. If the keys are applied to a message M one after another in sequence, then the following relation must hold:

$$D\,(E\,(M)) = M. \tag{17.1}$$

One might picture this arrangement as a lock that can be closed with one key but for which one needs a second key to unlock it.

For the sake of security of such a procedure it is necessary that a secret key D not be able to be derived from the public key E, or that such a derivation be infeasible on the basis of time and cost constraints.

In contrast to symmetric systems, asymmetric systems enable certain simplifications in working with keys, since only the public key of a participant A need be transmitted to a communication partner B for the latter to be in a position to encrypt a message that only participant A, as possessor of the secret key, can decrypt. This principle contributes decisively to the openness of communication: For two partners to communicate securely it suffices to agree on an asymmetric encryption procedure and exchange public keys. No secret key information needs to be transmitted. However, before our euphoria gets out of hand we should note that in general, one cannot avoid some form of key management even for asymmetric cryptosystems. As a participant in a supposedly secure communication one would like to be certain that the public keys of other participants are *authentic*, so that an attacker, with the nefarious goal of intercepting secret information, cannot undetected interpose him- or herself and give out *his* or *her* key as the public key under the guise of its being that of the trusted partner. To ensure the authenticity of public keys there have appeared surprisingly complex procedures, and in fact, there are already laws on the books that govern such matters. We shall go into this in more detail below.

The principle of asymmetric cryptosystems has even more far-reaching consequences: It permits the generation of *digital signatures* in which the function of the key is turned on its head. To generate a digital signature a message is "encrypted" with a secret key, and the result of this operation is transmitted together with the message. Now anyone who knows the associated public key can "decrypt" the "encrypted" message and compare the result with the original message. Only the possessor of the secret key can generate a digital signature that can withstand such a comparison. We note that in the case of digital signatures