Chapter 4

Cryptography Primer

4.1 BASIC CRYPTOGRAPHIC MECHANISMS

In modern cryptology, there are some basic mechanisms, which are essential to achieve security in distributed systems and hence in e-postage systems. We introduce these mechanisms at a conceptual level, which explains their security properties and how their cryptographic keys, if any, shall be managed. This will prepare our understanding of the existing e-postage systems in Chapter 6 on page 127, Chapter 7 on page 167 and the particular threats that apply to these systems (see Chapter 8 on page 183). Readers who are interested in a more detailed description and analysis of these mechanisms are referred to the Handbook of Applied Cryptography of Menezes, Oorschot and Vanstone [54], the Encyclopedia of Security and Cryptography of van Tilborg [74], or the reference work Applied Cryptography by Schneier [70].

The basic classes of cryptographic mechanisms include the following: Encryption mechanisms achieve message confidentiality. Message authentication codes protect the integrity of data and its originator. Digital signature mechanisms protect the integrity of data, its originator and achieve non-repudiation, i.e., provide evidence that no-one else than the claimed signer is the originator of a signed message. Until the 20th century, encryption was the primary if not the only purpose of cryptography [43]. Since the discovery of public key cryptography in the early 1970s, however, message authentication codes and digital signature mechanisms have become at least as important as encryption. In e-postage systems, for example, they are used to protect the individual indicia.

The users of a cryptographic mechanism employ individual *cryptographic keys* to establish and maintain their privileges. For example, only users whose e-postage devices hold a suitable cryptographic key can produce valid indicia. History has shown that any secret can be broken, be it an unknown cipher mechanism or an unknown cryptographic key. It is only a matter of time, effort and determination as David Kahn has shown by numerous examples in his book "The Codebreakers" [43]. The security of a cryptographic mechanism will thus be measured in terms of a minimum effort an attacker takes to break it. In order to maintain a cryptographic mechanism over a period of time it should allow for increasing its security, thus anticipating the simultaneously increasing power of potential attackers. An ideal security mechanism has a *security parameter* that determines the minimum amount of effort required to

break it, and a proof that it cannot be broken with less effort. The larger security parameter is chosen, the more effort is required to break the mechanism. Such an ideal mechanism can be laid open for public review and be used as a firm security feature for everyone to use with her or his individual keys. This is the security mantra of modern cryptology: Rest the security of a cryptographic mechanism only on keeping the respective cryptographic keys secret, and do not rely on obscuring the mechanisms themselves from the prying eyes of potential attackers.

The grain of salt is, however, that all the practical and useful cryptographic mechanisms known today are just approximations of the above ideal. For the most efficient mechanisms, mathematical proofs are rare, and for the less efficient but still practical ones, all the mathematical proofs of security known today rest on more or less realistic but unproven assumptions and most of them use controversial computational abstractions, such as the random oracle model [74]. Although the situation is unsatisfactory and needs improvement, there are many cryptographic mechanisms available that have sufficient evidence of security to them, and these are subject to ongoing standardization and regular review processes.

The security problems of real systems employing standardized cryptographic mechanisms come most probably from wrong implementations [44], use of insecure random generators, or poor key management. To put it in perspective, problems at the cryptographic mechanism layer are much less frequent than the notorious security problems filling the news headlines such as ill-handled PINs and passwords, ill-configured firewalls and virus scanners, and security holes in operating systems. See all the subsections entitled "What Goes Wrong" in a large variety of real systems [1] by Anderson.

We will now look at each class of cryptographic mechanisms one by one.

4.2 CONFIDENTIALITY AND PRIVACY

Confidentiality is the security property of whether a sender can transmit a message to a recipient such that the message is intelligible only by the recipient, but not to an intelligent attacker such as an intruder and eavesdropper. In order to achieve data confidentiality, the sender must transform the plaintext into some ciphertext, such that the ciphertext reveals no information about the plaintext to an attacker. Only the intended recipient(s) of the message can transform the ciphertext back into plaintext.

One way to achieve data confidentiality is to use a conventional, also called *symmetric encryption mechanism*. Another is to use a public key, also called *asymmetric encryption mechanism*.