Preface to the Second, Extended Edition

New topics have been included in the second edition. They reflect recent progress in the field of cryptography and supplement the material covered in the first edition. Major extensions and enhancements are the following.

- A complete description of the Advanced Encryption Standard AES is given in Chapter 1 on symmetric encryption.
- In Appendix A, there is a new section on polynomials and finite fields. There we offer a basic explanation of finite fields, which is necessary to understand the AES.
- The description of cryptographic hash functions in Chapter 2 has been extended. It now also includes, for example, the HMAC construction of message authentication codes.
- Bleichenbacher's 1-Million-Chosen-Ciphertext Attack against schemes that implement the RSA encryption standard PKCS#1 is discussed in detail in Chapter 2. This attack proves that adaptively-chosen-ciphertext attacks can be a real danger in practice.
- In Chapter 8 on provably secure encryption we have added typical security proofs for public-key encryption schemes that resist adaptively-chosen-ciphertext attacks. Two prominent examples are studied – Boneh's simple-OAEP, or SAEP for short, and Cramer-Shoup's public key encryption.
- Security proofs in the random oracle model are now included. Full-domain-hash RSA signatures and SAEP serve as examples.

Furthermore, the text has been updated and clarified at various points. Errors and inaccuracies have been corrected.

We thank our readers and our students for their comments and hints, and we are indebted to our colleague Patricia Shiroma-Brockmann and Ronan Nugent at Springer for proof-reading the English copy of the new and revised chapters.

Nürnberg, December 2006 Hans Delfs, Helmut Knebl