CHAPTER 11

Rijndael: A Successor to the Data Encryption Standard

> I don't know if we have any real chance. He can multiply and all we can do is add. He represents progress and I just drag my feet.
>
> —Sten Nadolny (translated by Breon Mitchell), *God of Impertinence*

THE AMERICAN NATIONAL INSTITUTE OF Standards and Technology (NIST) launched a competition in 1997 under the aegis of an *Advanced Encryption Standard* (AES) with the goal of creating a new national standard (federal information processing standard, or FIPS) for encryption with a symmetric algorithm. Although we have concentrated our attention in this book on asymmetric cryptography, this development is important enough that we should give it some attention, if only cursorily. Through the new standard FIPS 197 [F197], an encryption algorithm will be established that satisfies all of today's security requirements and that in all of its design and implementation aspects will be freely available without cost throughout the world. Finally, it replaces the dated *data encryption standard* (DES), which, however, as *triple DES* remains available for use in government agencies. However, the AES represents the cryptographic basis of the American administration for the protection of sensitive data.

The AES competition received a great deal of attention abroad as well as in the USA, not only because whatever happens in the United States in the area of cryptography produces great effects worldwide, but because international participation was specifically encouraged in the development of the new block encryption procedure.

From an original field of fifteen candidates who entered the contest in 1998, by 1999 ten had been eliminated, a process with involvement of an international group of experts. There then remained in competition the algorithms MARS, of IBM; RC6, of RSA Laboratories; Rijndael, of Joan Daemen and Vincent Rijmen; Serpent, of Ross Anderson, Eli Biham, and Lars Knudson; and Twofish, of Bruce Schneier et al. Finally, in October 2000 the winner of the selection process was announced. The algorithm with the name "Rijndael," by Joan Daemen and

Vincent Rijmen, of Belgium, was named as the future advanced encryption standard (cf. [NIST]).[1] Rijndael is a successor of the block cipher "Square," published earlier by the same authors (cf. [Squa]), which, however, had proved to be not as powerful. Rijndael was especially strengthened to attack the weaknesses of Square. The AES report of NIST gives the following basis for its decision.

1. **Security**
   All candidates fulfill the requirements of the AES with respect to security against all known attacks. In comparison to the other candidates, the implementations of Serpent and Rijndael can at the least cost be protected against attacks that are based on measurements of the time behavior of the hardware (so-called timing attacks) or changes in electrical current use (so-called power or differential power analysis attacks).[2] The degradation in performance associated with such protective measures is least for Rijndael, Serpent, and Twofish, with a greater advantage to Rijndael.

2. **Speed**
   Rijndael is among the candidates that permit the most rapid implementation, and it is distinguished by equally good performance across all platforms considered, such as 32-bit processors, 8-bit microcontrollers, smart cards, and implementations in hardware (see below). Of all the candidates Rijndael allows the most rapid calculation of round keys.

3. **Memory requirement**
   Rijndael makes use of very limited resources of RAM and ROM memory and is thus an excellent candidate for use in restricted-resource environments. In particular, the algorithm offers the possibility to calculate round keys separately "on the fly" for each round. These properties have great significance for applications on microcontrollers such as used in smart cards. Due to the structure of the algorithm, the requirements on ROM storage are least when only one direction, that is, either encryption or decryption, is realized, and they increase when both functions are needed. Nonetheless, with respect to resource requirements Rijndael is not beaten by any of the other four contestants.

4. **Implementation in hardware**

[1] The name "Rijndael" is a portmanteau word derived from the names of the authors. Sources tell me that the correct pronunciation is somewhere between "rain doll" and "Rhine dahl." Perhaps NIST should include in the standard a pronunciation key in the international phonetic alphabet.

[2] Power analysis attacks (simple PA/differential PA) are based on correlations between individual bits or groups of bits of a secret cryptographic key and the average consumption of electricity for the execution of individual instructions or code sequences depending on the key (see, for example, [KoJJ], [CJRR], [GoPa]).