Advanced Encryption Standard (AES) - An Update

[Invited Paper]

Lars R. Knudsen

University of Bergen, Norway

Abstract. On January 2, 1997, the National Institute of Standards and Technology in the US announced that they intend to initiate the development of a new world-wide encryption standard to replace the Data Encryption Standard (DES). A call for candidates was announced worldwide with the deadline of 15th June 1998. Totally, 15 candidates were submitted from the US, Canada, Europe, Asia and Australia. The author is the designer of one of the candidates, and a codesigner of another proposal.

The AES proposals are required to support at least a block size of 128 bits, and three key sizes of 128, 192, and 256 bits. The hope of NIST is that the end result is a block cipher "with a strength equal to or better than that of Triple-DES and significantly improved efficiency."

In March 1999 the first AES workshop was held in Rome, Italy. August 9, 1999, NIST announced the selection of five candidates for a final round of analysis. After a second AES workshop to be held in New York in April 2000, NIST intends to make a final selection of one or two algorithms for the Advanced Encryption Standard during the summer of year 2000.

The five algorithms selected to the final round are MARS, RC6, Rijndael, Serpent, and Twofish, which also are the candidates predicted by the author in a letter to NIST.

The winner(s) of the AES competition are likely to be used widely and for many years to come. Therefore, it is important that a candidate is chosen with a high level of security not only now, but also in 25 years time or more. It is of course impossible to predict which of the five candidates will survive attacks for such a long period, but this also speaks in favor of the choice of a candidate with a large security margin.

All AES candidates are iterated ciphers, where a ciphertext is computed as a function of the plaintext (and possibly some previous ciphertexts) and the key in a number of rounds. In the call for candidates NIST did not allow for a variable number of rounds. Although NIST allowed for possible "tweaks" (small changes), at the end of the first round (April 15, 1999) none of the designers changed the number of rounds of their algorithms. In fact of the five final ones, only the MARS designers suggested a modification to overcome a small key-schedule problem.

In our opinion, the number of rounds fixed by some of the designers is too small, and the algorithms will prove inadequate for long-term security. We believe that this narrows down the five candidates to only a few.

M. Walker (Ed.): IMA - Crypto & Coding'99, LNCS 1746, pp. 185–185, 1999.