DES, Triple-DES and AES

Lars Knudsen
Katholieke Universiteit Leuven, Belgium

Abstract

The Data Encryption Standard (DES) was developed by IBM in the early 70's, and adopted as a FIPS standard in 1977. Both the block size and, in particular, the key size of the DES have become too small for todays' applications. It has been shown that at the cost of about one million US$ it is possible to construct a dedicated dardware device, capable of performing an exhaustive search of a DES key in expected time only 3.5 hours. Also, recently it was deomstrated that even in software a 56-bit key does not provide sufficient protection, when a DES key was found by exhaustive search using implementations distributed on the Internet. Moreover, the relatively small block size of the DES becomes a problem when one key is used for many encryptions.

To account for these weaknesses the American National Standards Institute (ANSI) is working on adopting a suite of modes for triple-DES. Also, the National Institute of Standards and Technology (NIST) recently announced that they intend to standardize a new encryptio algorithm, the Advanced Encryption Standard (AES), as a replacement for the DES. NIST realises that it will be several years before the AES will be ready and that they intend to recognize the triple-DES once it is approved as an ANSI standard, which makes the ANSI initiative even more important.

In this talk we discuss the security of block ciphers in general focusing on the DES and the triple-DES variants. We propose a new variant of triple-DES, which we believe is better than existing proposals, and discuss the requirements for the AES.