

*Introduction to Cryptography
with Coding Theory
Chapter 4: DES/Encryption*

Chapter 4

The Data Encryption Standard

4.1 Introduction

In 1973, the National Bureau of Standards (NBS), later to become the National Institute of Standards and Technology (NIST), issued a public request seeking a cryptographic algorithm to become a national standard. IBM submitted an algorithm called LUCIFER in 1974. The NBS forwarded it to the National Security Agency, which reviewed it and, after some modifications, returned a version that was essentially the Data Encryption Standard (DES) algorithm. In 1975, NBS released DES, as well as a free license for its use, and in 1977 NBS made it the official data encryption standard.

DES has been used extensively in electronic commerce, for example in the banking industry. If two banks want to exchange data, they first use a public key method such as RSA to transmit a key for DES, then they use DES for transmitting the data. It has the advantage of being very fast and reasonably secure.

From 1975 on, there has been controversy surrounding DES. Some regarded the key size as too small. Many were worried about NSA's involvement. For example, had they arranged for it to have a "trapdoor" — in other words, a secret weakness that would allow only them to break the

system? It has also been suggested that NSA modified the design to avoid the possibility that IBM had inserted a trapdoor in LUCIFER. In any case, the design decisions remained a mystery for many years.

In 1990, Eli Biham and Adi Shamir showed how their method of differential cryptanalysis could be used to attack DES. The DES algorithm involves 16 rounds; differential cryptanalysis would be more efficient than exhaustively searching all possible keys if the algorithm used at most 15 rounds. This indicated that perhaps the designers of DES had been aware of this type of attack. A few years later, IBM released some details of the design criteria, which showed that indeed they had constructed the system to be resistant to differential cryptanalysis. This cleared up at least some of the mystery surrounding the algorithm.

The DES has lasted for a long time, but is becoming outdated. Brute force searches (see Section 4.6), though expensive, can now break the system. Therefore, NIST replaced it with a new system in the year 2000. However, it is worth studying DES since it represents a popular class of algorithms and it has been one of the most frequently used cryptographic algorithms in history.

The DES is a block cipher; namely, it breaks the plaintext into blocks of 64 bits, and encrypts each block separately. The actual mechanics of how this is done is often called a Feistel system, after Horst Feistel, who was part of the IBM team that developed LUCIFER. In the next section, we give a simple algorithm that has many of the characteristics of this type of system, but is small enough to use as an example. In Section 4.3, we show how differential cryptanalysis can be used to attack this simple system. We give the DES algorithm in Section 4.4, and describe ways it is implemented in Section 4.5. Finally, in Section 4.6, we describe recent progress in breaking DES.

For an extensive discussion of block ciphers, see [Schneier].