Some Regular Properties of the DES

Donald W. Davies
National Physical Laboratory

A cipher function should appear to be a random function of both the key and the plaintext. Any regular behaviour is of interest. In the extreme case it might point to a weakness of the cipher but in any case it is possible that precautions are needed in the use of a cipher that has regular features. This paper describes five regular properties of the DES, two of which have been described many times but are included for completeness: the complementation property, the weak keys, the semi-weak keys, further keys to be avoided, and the permutations P and E in relation to the S boxes.

In this paper we have described four functional regularities of the DES algorithm and one regularity in its structure. The regularities of function could be avoided by a change in the key generation part of the algorithm. The regularity of the structure of permutations could have been a design feature intended to spread any single bit change as quickly as possible.

There is no evidence that any of these regularities results in a weakness of the algorithm. The weak keys can be avoided in practice (if they are thought to matter) and are therefore just a nuisance. The design of the algorithm could have avoided these features. It is also probable that a less regular set of permutations with the same 'spreading properties would have produced as good a cipher algorithm.