CORR 2001-17

A Tutorial on Linear and Differential Cryptanalysis

Howard M. Heys*

Abstract In this paper, we present a detailed tutorial on linear cryptanalysis and differential cryptanalysis, the two most significant attacks applicable to symmetric-key block ciphers. The intent of the paper is to present a lucid explanation of the attacks, detailing the practical application of the attacks to a cipher in a simple, conceptually revealing manner for the novice cryptanalyst. The tutorial is based on the analysis of a simple, yet realistically structured, basic Substitution-Permutation network cipher. Understanding the attacks as they apply to this structure is useful, as the Rijndael cipher, recently selected for the Advanced Encryption Standard (AES), has been derived from the basic SPN architecture. As well, experimental data from the attacks is presented as confirmation of the applicability of the concepts as outlined.