Wrocław University of Technology, WPPT 20.12.04

CRYPTOGRAPHY, 2004 Assignments, list # 4

1. Is it possible to saturate any part of the output of the first round of the IDEA algorithm?
2. Build any linear approximation of a circuit adding a 6-bit key to a 6-bit input.
3. You are given possibility to flip k bits during symmetric encryption in a circuit. Which bits would you flip in order to perform an attack deriving the secret key used for encryption?
   Consider this question for the symmetric encryption schemes presented during the lecture on cryptanalysis.
4. Differential cryptanalysis of DES starts with a table of values for a single S-Box. Which contents of this table would be the best for you, if you are trying to construct characteristics?
5. You are given the possibility to read the Hamming weight of each half of the round output of DES. Use this possibility to derive a secret key used for encryption.

/-/ Mirosław Kutyłowski