Wrocław University of Technology, WPPT 3.11.09

CRYPTOGRAPHY AND SECURITY, 2009 Assignments, list # 4

1. Suppose that one has changed the subkey schedule of DES so that the subkeys are generated in some very hard way and the subkey bits are no longer the bits of the original key. How does it influence the strength of the algorithm against differential attack?

2. Assume that you can read the Hamming weight of each half of the round output of DES. Use this feature to derive the secret key used for encryption.

3. Look for linear approximation of a circuit adding a 6-bit key to a 6-bit input modulo 2^7.

4. Look for linear approximations of the Sbox considered on the previous list.

5. Assume that you can generate faults only during the first round of DES. Propose some reasonable scenarios for using it for attack against DES.

/-/ Mirosław Kutyłowski and Filip Zagórski