Wrocław University of Technology, WPPT 23.10.07

CRYPTOGRAPHY AND SECURITY, 2007 Assignments, list # 3

1. Some DES keys are called weak. One of the reasons could be that the subkeys generated are the same, or there are just a few different subkeys. Does it potentially weaken the encryption? Find all keys of this type.

2. Prove that
$$\mathrm{DES}_{\overline{K}}(\overline{X}) = \overline{\mathrm{DES}_K(X)}$$
for each X and K, where $\overline{Y}$ denotes Y after flipping its each bit.

3. 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 complexity of differential attack?

4. Differential cryptanalysis of DES starts with a table of values for a single S-Box. Which values of this table would be the best for constructing characteristics?

5. Assume taht you can read the Hamming weight of each half of the round output of DES. Use this possibility to derive the secret key used for encryption.

6. Build any linear approximation of a circuit adding a 6-bit key to a 6-bit input.

7. Let us change a single bit of the input to RC5. Estimate roughly the average number of rounds after which every bit may get influenced by the change. Consider 32-bit words (i.e. 64-bit blocks). Solve the same problem for AES.

/-/ Mirosław Kutyłowski