Wrocław University of Technology, WPPT 5.10.11

CRYPTOGRAPHY AND SECURITY, 2011 Assignments, list # 2

1. Design an encryption method for file systems such that

   - without an encryption key one cannot determine if two blocks of plaintext are identical,
   - it is possible to replace each single block of plaintext by replacing a single block of the ciphertext.

   Note that neither ECB nor CBC fulfils these requirements.

2. 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. Find some keys of this type. See `http://www.itl.nist.gov/fipspubs/fip46-2.htm` for a detailed description of key schedule for DES.

3. 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.

4. Consider the S-box S_5 of DES. (For the specification of Sboxes see the NIST publication: `http://www.itl.nist.gov/fipspubs/fip46-2.htm`.)

   For $x = 011011$ and each $y \in \{0,1\}^4$ compute the probability that
   $$S_5(z) \text{ XOR } S_5(z \text{ XOR } x) = y$$
   for a random $z \in \{0,1\}^6$.

5. 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?

6. (to be solved if there is enough time left)
   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.

/-/ Mirosław Kutyłowski