Wrocław University of Technology, WPPT 15.10.13

CRYPTOGRAPHY, 2013 Assignments, list # 3

1. DES encrypts blocks of length 64, but it is said that the key length is too short – one can perform a brute force attack. Is it also necessary to extend the length of the block as well? Say, is it possible to design a good block cipher that takes blocks of length 64 and long keys immune against brute force?

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. Change one bit of a plaintext for AES. Specify which bytes during the AES computation cannot be affected by this change. Consider round 1 and round 2.

   Perform the same analysis for DES.

4. Derive the decryption procedure for AES from its encryption specification.

5. 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 $z \in \{0,1\}^6$.

   Compute a few other entries in the table of differentials for this S-box.

6. We have considered fault generation combined with differential cryptanalysis for DES. How to apply this technique for AES?

   Recall that the last round of AES is: SubBytes, ShiftRows, AddRoundKey

7. 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?

8. Assume that we have a characteristic for differential cryptanalysis that holds with probability 2^{-43}. Assume that a characteristic delivers 20 candidates for the round key from the last round, out of 2^{48} possible round keys.

   How many encryptions we need to do in order to fish out the round key from the last round? (of course the algorithm is probabilistic, so present the number such that with probability ... (e.g. 0.9) we succeed).

/-/ Mirosław Kutyłowski and Maciej Gebala