Wrocław University of Technology, WPPT 26.10.06

CRYPTOGRAPHY, 2004 Assignments, list # 2

1. Assume that one has implemented CFB encryption mode in such a way that instead of operation $I_{j+1} = \text{shift}(I_j c_j)$ (non-circular shift of the sequence used for encryption) the following formula was used:
$$I_{j+1} = I_j \text{ XOR } c_j$$
(before XOR-ing c_j is appended with zeroes). Find weak point(s) of such a solution.

2. 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 power of differential attack?

3. Construct a table for differential cryptanalysis for an "S-box" which is the following function:
$$i_1, i_2, i_3, i_4, i_5, i_6 \to i_1 + i_2 + i_3, i_4 + i_5 + i_6, i_2 \cdot i_4, \text{MAJORITY}(i_1, i_2, i_3, i_4, i_5, i_6)$$
(there is no magic in the choice of this S-box). You may use a program to compute the results.
Discuss the strength of such an S-box, based on the results obtained.

4. Write down, in a form of pseudocode, algorithm of differential cryptanalysis.

5. Differential cryptanalysis uses pairs of inputs having a given difference. How to proceed, if the attacker cannot determine the inputs to be encrypted?

6. You are given the possibility to read the Hamming weight of each half of the round output of DES. Use this possibility to derive the secret key used for encryption.

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

8. Is saturation attack suitable against DES? Try to perform such an attack against a few rounds.

9. 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 the Rijndael algorithm.

/-/ Mirosław Kutyłowski