CRYPTOGRAPHY, 2004   Assignments, list # 3

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. Try to implement the CFB encryption in the situation that we have no block encryption but only a good hash function.

3. 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.

4. 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?

5. 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.

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

7. Is it possible to saturate any part of the output of the first round of DES algorithm?

/-/ Mirosław Kutyłowski