Wrocław University of Technology, WPPT 29.11.04

Cryptography, 2004 Assignments, list # 3

1. Assume that one has implemented CFB encryption mode in such a way that instead of operation $I_{j+1} = \text{shift}(I_j c_j)$ (noncircular 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. Compression of a file improves its “randomness”, so one may think that it is better to compress file before encryption. But it is recommended to avoid pipelining both procedures. Find the reason for this recommendation.

4. Estimate the effort necessary to perform the attack *meet-in-the-middle* on double-DES.

5. For IDEA encryption: you can influence the choice of the key bits by Alice so that you can determine bits on 64 positions of your choice. Your purpose is to break the ciphertexts created later by Alice. Which positions would to choose and how would you perform the attack?

6. How to apply differential cryptanalysis for DESX?

7. Determine the branch number of MixColumn operation used by Rijndael.

8. 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).

9. Consider Twofish algorithm: find a class of inputs so that after as many rounds as possible we have certain saturation properties.

/-/ Mirosław Kutyłowski