Wrocław University of Technology, WPPT 10.10.07

CRYPTOGRAPHY AND SECURITY, 2007 Assignments, list # 2

1. Consider an LFSR random number generator. Since XOR is equivalent to addition operation in field $\{0, 1\}$, it leads to systems of linear equations describing LFSR generator. Replace XOR by different functions: OR, AND, MAJORITY, and discuss consequences for security of resulting stream ciphers.

2. Consider a version of A5/1 which uses LFSR registers of length 11, 12 and 13. Could you break such a scheme with a standard computer? Make the attack as efficient as possible.

3. One of the major properties of A5/1 is that it is hard to reconstruct its previous state. Estimate the number of possible previous states one step before the observed internal state of an LFSR. How does this influence a "brute force" attack on GSM use of A5/1?

4. 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.

5. Discuss what happens if a certain part of CBC ciphertext becomes destroyed. Can we decrypt the rest? What happens if some number of bits is missing?

   Answer the same question for CFB encryption mode.

6. Assume that an adversary can determine the IV used in CBC encryption. Is it dangerous?

7. Generalize attack on double-encryption to triple-encryption scheme. Estimate complexity of this attack.

8. Generalize Feistel method to scheme using 4 blocks instead of 2. Which method seems to be most reasonable?

9. How to design permutations used in DES so that avalanche effect is strong? Estimate the number of rounds necessary for dissemination of changes.

/-/ Mirosław Kutyłowski