Wrocław University of Technology, WPPT 6.10.09

CRYPTOGRAPHY AND SECURITY, 2009 Assignments, list # 1

1. We have to find a key K that has been used to obtain a ciphertext C from a plaintext T. We assume that there exists exactly one such a key and that the key length equals k. Assume that encryption rate is 10^6 ciphertexts/second. Estimate the effort required for finding key K by a brute force attack, that is, checking all possible keys.

   Answer this question for $k = 40$, $k = 56$, $k = 90$, $k = 128$.

2. Recall that one-time pad is a scheme where for an n bits plaintext $t_1 t_2 \dots t_n$ and a key $k_1 \dots k_n$ the ciphertext $c_1 \dots c_n$ is obtained by equality: $c_i = t_i \text{XOR} k_i$ for $i \leq n$.

   This scheme achieves *perfect security*, i.e., for a given ciphertext each plaintext is equally probable.

   1. Show that *perfect security* cannot be achieved when the key length is smaller than the length of the ciphertext (perfect security means that for each plaintext is equally probable for a given ciphertext).
   2. Is this true that one-time pad is the only algorithm with perfect security property?
   3. Propose an alternative definition: *perfect security means that for each ciphertext is equally probable for a given plaintext*. Are both definitions equivalent?

3. 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 the LFSR generator. Replace XOR by different functions: OR, AND, MAJORITY, and discuss consequences for security of the resulting stream ciphers.

4. How to attack A5/1 when the majority rule is disabled, i.e. all three registers make a shift at each step.

5. 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?
   Could you break a version A5/1 which uses LFSR registers of length 11, 12 and 1 with a standard computer? Make the attack as efficient as possible.

/-/ Mirosław Kutyłowski and Anna Lauks-Dutka