Wrocław University of Technology, WPPT 15.10.06

CRYPTOGRAPHY, 2004 Assignments, list # 1

1. We have to find a key that has been used to obtain a ciphertext C from a plaintext T. We assume that there exists only 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 the key by brute force.

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

2. For one-time-pad the length of a key and the plaintext are the same. 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 cihertext).

   Propose an alternative definition: *perfect security means that for each cihertext is equally probable for a given plaintext.* Are both definitions equivalent?

3. Estimate power of frequency analysis for an encryption scheme using blocks consisting of 3 ASCII numbers.

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

5. 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.

6. Design an encryption method for file systems such that

   - without a encryption key one cannot determine if two blocks of plaintext are identical,
   - it is possible to change each single block of plaintext and then a single block of ciphertext.

7. Discuss what happens if 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.

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

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

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

/-/ Mirosław Kutyłowski