Wrocław University of Technology, WPPT 27.09.11

CRYPTOGRAPHY AND SECURITY, 2011 Assignments, list # 1, modified

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 $k = 40, 56, 90, 128$.

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. Write them down and apply to full reconstruction of LFSR state and connections at the beginning if you are given some sequence of output bits (how long this sequence must be?). Replace XOR by different functions: OR, AND, MAJORITY, and discuss consequences for security of the resulting stream ciphers.

4. Assume that majority rule for A5/1 has been replaced by minority rule:, i.e. only the registers that loose in voting make a shift. Evaluate such a proposal.

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?

6. Assume that you are holding an RC4 encryption device and you can influence it so that an arbitrary number of bytes is initially replaced as you want. Derive the secret key used by the device.

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

8. Discuss what happens if a certain part of CBC ciphertext becomes destroyed or lost. Can we decrypt the rest? Consider all error scenarios.

9. CFB encryption mode is given by the equation: $C_i = E(C_{i-1}, K)$ xor M_i. What is the behavior of CFB in case of transmission errors? What are the advantages and disadvantages of CFB in comparison with ECB and CBC?

10. Derive the decryption algorithm of RC5. Show that RC5 has the Feistel structure.

11. Assume that through a bad hardware implementation it is possible to determine which circular shifts are performed at each round of RC5. Does it leak the secret key?

/-/ Mirosław Kutyłowski