Wrocław University of Technology, WPPT 30.09.13

CRYPTOGRAPHY, 2013 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 each key consists of k bits. Assume that encryption rate is 10^6 ciphertexts/second. Estimate the time effort required for finding key K by a brute force attack, that is, checking the possible keys one by one Answer this question for $k = 40, 56, 90, 128, 256$.

   Check encryption speed of AES (google for the most efficient hardware), estimate the energy cost (assume you have to pay 0.2PLN/kWh).

2. One-time pad is a scheme where for an n-bit 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: $c_i = t_i \,\mathrm{XOR}\, k_i$ for $i \leq n$.

   This scheme achieves *perfect security*, i.e., for a given ciphertext each plaintext is equally probable, if the encryption key is chosen at random.

   1. Show that *perfect security* cannot be achieved when the key length is smaller than the length of the ciphertext.
   2. Find an example of an encryption scheme with perfect security that is different form one-time pad. Can it happen that the key length is higher than the length of the ciphertext (we mean schemes where all bits of the key have influence on the encryption outcome)?
   3. Propose an alternative definition: *perfect security means that for each ciphertext is equally probable for a given plaintext.* Are both definitions equivalent?

3. For encryption of plaintexts longer than n bits and the key of length n one can use one-time pad in the following way: $c_i := t_i \,\mathrm{XOR}\, k_{i \bmod n}$. Describe a procedure of an attack against such a scheme when encryption is applied to a program in a high level programming language.

4. An encryption scheme is *semantically secure* if given a ciphertext it is infeasible to derive any information about the plaintext.

   - show that *perfect security* implies *semantical security*.
   - is it true vice-versa?
   - try to define more precisely the notion *it is infeasible to derive* <u>*any*</u> *information about the plaintext.*

5. There are many situations for cryptanalytic attacks. For instance *ciphertext-only* is based on knowledge of the ciphertext only (like before World War 2, listening to enemy's radio traffic without knowing the side information). On the other hand, there is a *chosen-plaintext attack*, where the attacker has a tamper-proof encryption device, he can encrypt an arbitrary plaintext, but aims to derive the encryption key stored inside the device.

   - try to categorize all practical attacks scenarios,
   - check whether one-time pad is secure against these attacks.

/-/ Mirosław Kutyłowski and Maciej Gebala