PWr, Inf. algo. CRYPTOGRAPHY, 2022 assignments list # 1, 2.3.2022

1. One can try to defend against frequency analysis by first compressing the file to be encrypted. Note that a compression algorithm attempts to encode the information so that each byte in the compressed file is (almost) 1 information byte. So it looks promising – there are no "frequent symbols"

   However, it is not recommended to do it in this way. What could be the reason? Maybe you will have to look to some details of the compression schemes.

2. An alternative definition for perfect security for symmetric encryption schemes has been proposed: *perfect security B* means that *each ciphertext is equally probable for a given plaintext and key chosen at random*. Are the notions of *perfect security* and *perfect security B* equivalent?

3. Find an example of an encryption scheme with perfect security that is different from 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)?

   What is the maximal length of the encryption keys so that no two keys would yield always the same results?

4. Recall the definition of *semantic security*.

   - show that *perfect security* implies *semantic security*.
   - does *semantic security* imply *perfect security*? Find a convincing argument or an example.
   - Semantic security may be formulated in terms of 4 plaintexts: Alice chooses m_1, m_2, m_3, m_4, encrypts m_b and Bob has to guess b. Is this notion stronger?

5. [homework] 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 e.g. on your laptop, estimate the energy cost (assume you have to pay 1PLN/kWh) according to the nominal (real, if you can) power consumption.

6. How to play Monopoly using only email for communication? (Of course, everybody can cheat)

/-/ Mirosław Kutyłowski