Wrocław University of Technology, WPPT 3.10.07

CRYPTOGRAPHY AND SECURITY, 2007 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. 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 cihertext).
   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 cihertext is equally probable for a given plaintext*. Are both definitions equivalent?

3. Bit commitment is a scheme in which Alice commits to a bit and cannot change her decision. However the choice of Alice cannot be determined until Alice explicitely reveals it.

   1. Design a bit commitment scheme based on one-way, collision-free hash functions.
   2. Design a scheme of choosing a random string together by two parties.

4. Show that if a hash function H is not a one-way function, then H is not collision-free.

5. Is it possible to design mutual authentication between Alice and Bob sharing a secret key k so that only two messages are exchanged?

6. Design a scheme based on onion routing so that a connection is established and the packets are encrypted and decrypted with symmetric methods only.

/-/ Mirosław Kutyłowski