Wrocław University of Technology, WPPT 11.10.05

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.

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

2. How to make DH key exchange immune to the man-in-the-middle attack? One of the ideas is to send halves of ciphertexts at each round of communication – this should make recoding impossible.

3. Lamport signature scheme is the following procedure: We choose $y_{i,0}, y_{i,1}$ at random from a set Y for $i \leq m$. We compute $z_{i,j} = f(y_{i,j})$ dla $i \leq m, j = 0, 1$, where f is a cryptographically good hash function. The numbers $z_{i,j}$ are published, the numbers $y_{i,j}$ are kept secret.
   A signature for $x_1, \ldots, x_m$ equals $y_{1,x_1}, \ldots, y_{m,x_m}$.

   Discuss security and efficiency of this solution. Propose ways to improve it.

4. How to construct a hashing function provided that we have a strong encryption algorithm?

   asymetric encryption algorithm,
   (b) only a good hash function.

5. How to design a bit commitment algorithm given no hash function and

   - only a digital signature algorithm?
   - only a good hash function.

6. How to play pocker through Internet?

/-/ Mirosław Kutyłowski