Wrocław University of Technology, WPPT 1.10.02

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. For one-time-pad the length of key and the plaintext are the same. 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).

   Propose an alternative definition: *perfect security means that for each cihertext is equally probable for a given plaintext.* Are bothe definitions equivalent?

3. A digital signature of Alice provides a proof that Alice has signed a document. In practice (in a bank or so) we often are asked to sign the same document for the second time in the purpose for better authentication.

   Digital signatures are sometimes deterministic procedures. How to implement „signing for the second time“ in this case?

4. 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.

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

6. A bit commitment protocol is executed as follows

   - Alicja chooses a bit b, encodes it as $m = f(b)$ and shows m to Bob
   - Bob cannot retrieve from m whether $b = 0$,
   - at a later moment Alicja *reveals* b and convinces Bob that $m = f(b)$

   How to implement such a protocol so that Alicja cannot cheat about the value chosen?
   Solve this question if Alicja and Bob have
   (a) only asymetric encryption algorithm,
   (b) only a good hash function.

7. How two persons communicating by phone could flip the coin (the result determines who will wash dishes)?

/-/ Mirosław Kutyłowski