Wrocław University of Technology, WPPT 5.01.06

CRYPTOGRAPHY, 2005 Assignments, list # 4

1. TESLA is a communication protocol such that each packet is authenticated by the previous one: message i contains $H(r)$, message $i+1$ contains r, where r is random, and H is a hash function. Modify the protocol so that the connection does not break down when some number of packets is lost.

2. How to design a good hashing function from a good symmetric encryption algorithm? Propose a procedure and list all necessary properties of the encryption algorithm in order to get a sound solution.

3. Good hashing functions provide outputs that are quite long. Assume that you need short fingerprints, say of 2 bytes, as error detection codes. How to design them?

4. Hashing based on discrete logarithm problem can be based on three numbers instead of two:

$$H(x,y,z) := \alpha^x \cdot \beta^y \cdot \gamma^z \bmod p$$

   Is this solution secure?

5. Let us generate a pseudorandom sequence in the following way:
   $x_0 = s^2 \bmod n$,
   $x_{i+1} = x_i^2 \bmod n$.
   The output of the genarator is $z_1, z_2, \ldots$, where z_i is the second half of x_i. (So it is a faster version of BBS algorithm).
   Is it secure?

6. LFSR are cryptographically weak. So the XOR operation has been replaced by AND operation (which is nonlinear one) in the hope that it will be impossible to recover the internal state of the registers via linear equations. Is it a sound solution?
   A similar investigation should be performed for OR and majority function.

7. Show that not every hypothetical state of the registers of A5/1 at step t there are predecessor states at time steps $t-1, t-2, \ldots$ that agree with an available output sequence. estimate probability that a random hypothetical state has such a predecessor at step $t-1$.

/-/ Mirosław Kutyłowski