Wrocław University of Technology, WPPT 2.01.05

CRYPTOGRAPHY, 2004 Assignments, list # 5

1. Assume that hash values of two blocks can be computed simultaneously. How to use this feature when designing a scheme to hash data of an arbitrary length?

2. 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.

3. Assume that A is a computationally zero-knowledge authentication protocol based on public keys. Does it mean that the protocol is secure?

4. Show that Fiat-Shamir authentication protocol is a zero-knowledge protocol.

5. t persons agree upon a common key with Burmester-Destmedt algorithm, which is a generalization of DH: person i chooses r_i at random, computes $z_i := g^{r_i} \bmod p$ and broadcasts z_i. Then he computes $X_i = (z_{i+1}/z_{i-1})^{r_i} \bmod p$ and broadcasts it. How to computes the common key? What happens if one person sends a wrong message?

6. The following protocol was designed for transporting and confirming a key. This is one of the standard protocols which has been "improved", but these improvements might be wrong. Examine the protocol and propose necessary measure to achieve a secure version out of it.
   A stands for Alice, T for a trusted authority, B for Bob. $E_X(D)$ denotes a ciphertext of D obtained with key X. Let K_{XY} denote a shared key of participants X and Y.

   (a) A chooses r_A at random and sends A, B, r_A to T,

   (b) T replies with $E_{K_{AT}}(r_A, B, k)$,

   (c) A sends $E_{K_{BT}}(k)$ to B,

   (d) B decrypts the ciphertext obtained, chooses r_B at random and sends $E_k(r_B)$ to A,

   (e) A replies with $E_k(r_A)$.

/-/ Mirosław Kutyłowski