PWr, Inf. algo. CRYPTOGRAPHY, 2022 assignments list # 11, password authentication

1. Let us recall the original protocol SPEKE by D.Jablon mentioned during the lecture. Let π be the shared password, let f be a function that maps passwords to a group G where DDH problem is hard.

   1a) Alice chooses x_A at random and sends $X_A := (f(\pi))^{x_A}$ to Bob,

   1b) Bob chooses x_B at random and sends $X_B := (f(\pi))^{x_B}$ to Alice,

   2a) Alice computes $K = \text{Hash}(X_B^{x_A})$

   2b) Bob computes $K = \text{Hash}(X_A^{x_B})$

   ..... K is a shared master key .....

   3) Alice chooses C_A at random and sends $E_1 := \text{Enc}_K(C_A)$ to Bob,

   4)) Bob decrypts E_1, chooses C_B at random and sends $E_2 := \text{Enc}_K(C_B, C_A)$ to Alice,

   5) Alice decrypts E_2, checks if C_A is in the plaintext, computes $E_3 := \text{Enc}(C_B)$ and sends it to Bob,

   6) Bob decrypts E_3, and compares the plaintext obtained with C_B

   I. Analyze the protocol and check that:

   (a) an observer that can see all messages cannot find π (even if he has a small dictionary of all passwords that can be used by Alice and Bob),

   (b) a man-in-the-middle attack fails against SPEKE,

   (c) a replay attack fails against SPEKE.

   II. What is the motivation for steps 3-6? What could happen in case that these steps are eliminated from the protocol?

/-/ Mirosław Kutyłowski