PWr, Inf. algo. CRYPTOGRAPHY, 2022 assignments list # 8, hash functions

1. Bit commitment scheme is to

   (a) Alice creates a commitment $c$ for a a value $d$,

   (b) Alice presents $c$ to Bob,

   (c) some other steps of Alice and Bob ...

   (d) Alice "opens" $c$ by showing $d$ and proving that she has created $c$ from $d$

   Explore possibilities to construct a commitment scheme based on:

   (a) a hash function,

   (b) asymmetric encryption,

   (c) symmetric encryption.

   In each case formulate necessary properties of the underlying scheme.

2. AES can be used to create a hash function. (One of the advantages is that in case of a weak embedded device one can implement the code of AES instead of, say, AES and SHA-3.This reduces the code size.) The algorithm is as follows:

   - apply padding: add zeroes so that we have an odd number of blocks of length 128, add the length of the original file in the next block of length 128,
   - put $H_0 = 2^{256} - 1$ (string of 256 ones),
   - $H_i = \text{Enc}_{x_i}(H_{i-1}) \oplus H_{i-1}$, where $x_i$ is the $i$th block after padding,
   - output the last computed $H_i$

   Discuss (informally), why this construction should have the properties required from a cryptographic hash function.

3. In the previous problem, replace the previous formula by $H_i = \text{Enc}_{x_i}(H_{i-1})$. What are the problems for the resulting hashing scheme?

4. (a) Create a hash value of your name using AES Hash, MD4, MD5, SHA-1, SHA-256, SHA-512.

   (b) Install BLAKE2 (`https://github.com/BLAKE2/`) on your computer. You might be asked to hash something with BLAKE2.

   (Note that BLAKE was one of the finalists of the NIST competition).

5. Urzedowe Poświadczenie Odbioru (UPO) for your electronic tax declaration (assuming you submit your declaration online) contains "skrót dokumentu" and "skrót podpisanego dokumentu".

   - if you have the xml file for the UPO, browse through this file and find the meaning of these fields,
   - if you have not declared your income online, then compare the proof value of the UPO for tax declaration and a seal of the tax authority on the paper copy of a tax declaration.

/-/ Mirosław Kutyłowski