Wrocław University of Technology, WPPT 20.10.09

CRYPTOGRAPHY AND SECURITY, 2009 Assignments, list # 2

1. Try to define one-way functions in a formal way. It should not only be formally correct, but also should catch correctly the practical meaning of impossibility to invert.

2. Show that if a hash function H is not a one-way function, then H is not collision-free. (One-way means that it is impossible to invert it. H is collision-free if it is impossible to find any collision, $H(x) = H(x')$.)

3. Design a mutual authentication protocol between Alice and Bob sharing a secret key k. Minimize the number of messages exchanged between them. If possible, show that it cannot be reduced.

4. Design a scheme based on onion routing so that a connection is established and the packets are encrypted and decrypted with symmetric methods only. (In fact, this is a question how the protocols like TOR can be designed)

5. Assume that you are holding an RC4 encryption device and you can influence it so that an arbitrary number of bytes is initially replaced as you want.

   Derive the secret key used by the device.

6. Design an encryption method for file systems such that

   - without an encryption key one cannot determine if two blocks of plaintext are identical,
   - it is possible to replace each single block of plaintext by replacing a single block of the ciphertext.

7. Assume that an adversary can determine the IV used in CBC encryption. Is it dangerous?

8. Discuss what happens if a certain part of CBC ciphertext becomes destroyed or lost. Can we decrypt the rest? Consider all error scenarios.

9. CFB encryption mode is given by the equation: $C_i = E(C_{i-1}, K)$ xor M_i. What is the behavior of CFB in case of transmission errors? What are the advantages and disadvantages of CFB in comparison with ECB and CBC?

/-/ Mirosław Kutyłowski and Filip Zagórski