Cryptography for Computer Scientists 2018/19 Nov 7, 2018

Exercises 6

Stefan Dziembowski MIM UW

Exercise 1: Key exchange from PKE

Given a public-key encryption scheme construct a key exchange protocol.

Exercise 2: Key agreement from padlocks

Suppose Alice and Bob have access to physical padlocks P_A and P_B (respectively) that can be locked and open with keys K_A and K_B (respectively). Moreover, Alice has a physical box that can be locked using the padlocks P_A and P_B, and that can contain documents with bit strings written on them. They also have a courier that is "honest but curious", that it is will deliver messages between them, but will try to read their secrets (for example: he will read the documents in the box if the box is not locked). Show how Alice and Bob can agree on a secret key in this settings.

Can you implement your protocol in the digital way by replacing the physical box and padlocks with symmetric encryption?

Exercise 3: Authenticated key exchange

Some implementations use *authenticated key exchange* constructed as follows. The parties Alice and Bob share a key K, and use a standard key exchange protocol authenticating (by message authentication codes) every message with this key. What is the advantage of this approach over a simpler method where Alice selects a random key X and sends it to Bob using authenticated encryption (with key K)?

Exercise 4: Security of Feistel networks

Let f be a pseudorandom function.

1. Let g be a keyed function that results from using f in a 2-round Feistel network. Show that g is not a pseudorandom function.

2. Let h be a keyed function that results from using f in a 3-round Feistel network. Show that g is not a strong pseudorandom function.