Asymmetric Cryptography with Colors

Justus Rotermund, Jens Lechtenbörger

September 2017

1 Preparation

Each student is supposed to bring along pens or text markers in different colors and receives white sheets of paper and envelopes.

1. Form groups with three students each such that every student has a pen in a different color. Every player needs to know the colors of the other group members to identify communication partners. Intuitively, your personal color represents your asymmetric key pair.

2. To allow other students to send encrypted messages to you, mark some envelopes with the pen of your color (a clearly visible, colored part is enough) and distribute those colored envelopes among the other players of your group.

2 Rules

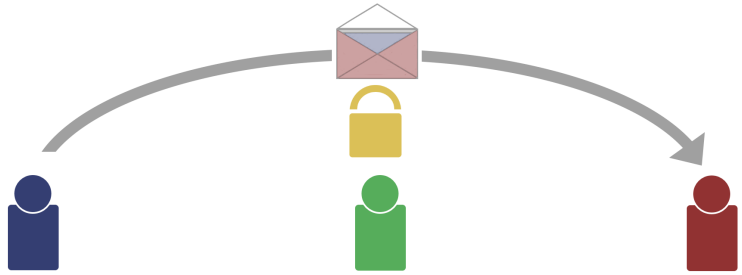
A message placed into a colored envelope is considered to be encrypted with the corresponding public key. Only the player with the proper private key, the pen of the matching color, is allowed to retrieve the message from a colored envelope. To sign a message, either mark the sheet of paper or write the message in your personal color.

The exercise proceeds as follows: Communicate with each other with the means of public key cryptography. Forward differently colored (including white) messages contained in differently colored (including white) envelopes from sender to recipient via the third student. Experiment with possibilities not explained explicitly and try to find loopholes within this style of communication.

3 Self-Test Questions

- What does a white paper in a white envelope represent?
- What does a red paper in a white envelope represent?
- What does a red paper in a blue envelope represent?
- What does a blue paper in a blue envelope represent?
- Which security goals are protected how and when?

- And in our own interest: How can we improve this exercise to make the concept of public key encryption understandable?



4 Acknowledgment

This game is based on the Security Protocol Game by Len Hamey.

License Information