Cryptography, exercise sheet 1 for 03 Sep 2024

These are the exercises for the instruction session. These are not for homework.

In particular for the first few exercises you should work in a small team of 2 people, 3 can work as well. For the other exercises go for your preferred group size.
Your TA will explain the perfect-code system in the first 5 - 10 min, for the rest of the time you can work on your own and call your TA over when you have a question or to check your solution.

1. Exercises regarding the perfect-code system and general understanding of the concepts

   (a) Find a partner and execute the system so that each of you generates a keypair, gives the public key to the other person, encrypts a number to the other person's key, and finally decrypts their received message.

   Note: Keep the numbers small to avoid making mistakes. Eight nodes is enough, but you can make this harder for yourself.

   (b) Show that the public key is indeed a perfect code, i.e., show that there exists a selection of nodes so that each node is in the neighborhood of exactly one selected node (a selected node is in its own neighborhood.

   (c) Show why this system works, i.e., why the decryption returns the plaintext.

   (d) Break the examples, e.g. get a ciphertext and public key from some other group. Can you scale your attack to work for graphs with 1000 nodes?

   Note: There are different notions of breaking – complete breaks recover the private key from the public key, but a system is also broken if you can recover messages from ciphertexts.

2. Exercises regarding clock Diffie-Hellman

   (a) $(2, -2)$ is a point on the clock modulo 7. Compute $5(2, -2)$. Remember the double-and-add method and also what you know about orders of points.

   (b) Prove that for (x_1, y_1) and (x_2, y_2) on the circle $x^2 + y^2 = 1$ also their sum $(x_1, y_1) + (x_2, y_2) = (x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$ is on the circle.

   (c) Doubling is a special case of addition. Squarings are typically faster than multiplications. Show how to compute $2((x_1, y_1)$ using only squarings (next to additions and subtractions).

   (d) The clock addition formula $(x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$ can be computed in 4 multiplication. Figure out how to do it with 3.