Cryptography, winter 2014/2015

Priv.-Doz. Dr. Adrian Spalka, Dr. Daniel Loebenberger

12. Exercise sheet
This sheet will not be graded

Exercise 12.1 (Did you get it?). *Answer the following questions on topics covered in the course:*

(i) *What is computer security all about?*

(ii) *What is cryptography all about?*

(iii) *What is the difference between computer security and cryptography?*

(iv) *How do you securely exchange a key? Which computational tools do you need for that?*

(v) *Once having a shared secret, how do you communicate now encrypted? Which algorithm do you employ? Give a concrete example and explain how is it designed.*

(vi) *How do you make sure that no one alters on the way your message? Which tools do you use here?*

(vii) *If you talk over the line to someone else, how do you make sure that the person you talk to is actually the person you want to talk to? Which methods do you employ?*

(viii) *When do you consider a cryptographic system to be secure?*

(ix) *Specifically for hash functions: Which security definitions do we have? Do these also apply to the Merkle-Damgård construction? How?*

(x) *Which hash functions would you employ in practice?*

(xi) *Is 0 a random bit? Is 1? Elaborate on this question.*

(xii) *How do you generate a 2048bit RSA key pair? Give a detailed answer.*

Exercise 12.2 (Teach!). *Consider the material covered this winter term. Invent some detailed questions you would ask in a written exam. Note: The type of above questions is* not *suitable for exam questions, since they are stated far to general.*

Exercise 12.3 (Working in elliptic curves). (0 points)

Consider the example $E = \{(u,v) \in \mathbb{F}_7^2 : v^2 = u^3 + u\} \cup \{\mathcal{O}\}$ for an elliptic curve over $\mathbb{F}_7$ (see Figure 12.1).

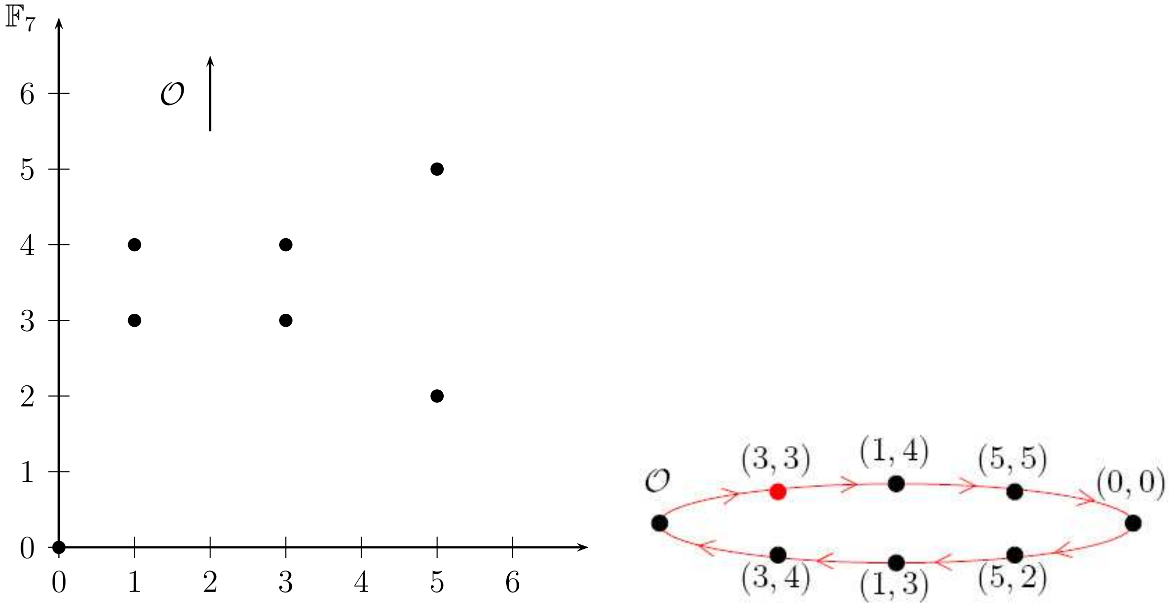

Figure 12.1: Graph and diagram for the group structure of E generated by the point $(3,3)$.

(i) Let $P = (5,5)$. Determine $S = 2 \cdot P$ and $T = 5 \cdot P$ from the diagram on the right of Figure 12.1.

The addition of two distinct points corresponds to a secant of the graph. The doubling of a point corresponds to a tangent to the graph.

(ii) Draw the tangent corresponding to $S = 2 \cdot P$ into the graph on the left of Figure 12.1.

(iii) Determine $S + T$ from the graph on the left and check your result by doing the same computation in the diagram on the right.

Alice and Bob heard about the cryptographic applications of elliptic curves. They want to perform a Diffie-Hellman key exchange using the elliptic curve E.

(iv) List all possible generators for the cyclic group E.

ALICE and BOB publicly agree on the generator P from above. The secret key of ALICE is 3 and the secret key of BOB is 4.

(i) Which messages are exchanged over the insecure channel and what is ALICE's and BOB's common secret key?