Problem 1. (20 points)
Assume the following one-way function for messages m of length n. z is the product of two primes.

1. $h_0 = 0$
2. Calculate $h_i = 2^{(h_{i-1}+m_i)} \pmod{z}$ for $i \in 1, ..., n$
3. $h(m) = h_n$

(a) Calculate the hash value for the message $m = (3, 33, 13, 14)$ with the given function using $z = 55$.

(b) The hash function is used for signing a message. Construct a signature scheme for the hash value that is based on the Rabin cipher with primes p and q. Consider only the case that the hash value is a quadratic residue with respect to the system parameters p and q.

(c) Sign the message from part a) with the new signature scheme. Use $p = 19$ and $q = 31$.

Problem 2. (10 points)
In Lamport's protocol, a one-way function is used by A to authenticate to B. In order to make the protocol robust against packet loss and reordering, B accepts not only the next password w_i, but any password in an interval of ± 10 surrounding the last received password, i.e. any w_j is accepted for $j \in \{i-10, ..., i-1, i+1, ..., i+10\}$.

(a) How can an attacker exploit the change of the protocol to authenticate himself to B? How often can the attacker authenticate himself?

(b) Propose an enhancement of the protocol and describe its benefits and disadvantages.

To make the authentication secure, challenge-response protocols should be used.

(c) Describe two protocols from the lecture that allow for secure mutual authentication and describe at least one advantage for each.

Problem 3. (8 points)
Consider a secure coin-flipping protocol over the telephone.

(a) On which problem is the coin-flipping protocol known from the lecture based?

(b) How can a fair coin flipping be conducted by help of a hash function? Describe the steps of the protocol.

(c) How can such a protocol be executed using a block cipher?

Problem 4. (22 points)
Consider the elliptic curve

$$E : y^2 = x^3 + 3x + 5.$$

The curve is defined over $\mathbb{F}_{11}$.

(a) Calculate all points of the curve. How many points are in $E(\mathbb{F}_{11})$?

(b) Identify the inverses $-P$ for all points $P \in E(\mathbb{F}_{11})$.

Now the Diffie-Hellman key exchange is performed on $E(\mathbb{F}_{11})$ with the generator $P = (0, 7)$. Alice chooses the secret $x = 5$ and Bob chooses $y = 3$.

(c) Calculate Bob's message to Alice.

For the given curve, the cardinality is easily found by counting the points. When using secure curves, this does not hold. However, an estimation of the number of points is necessary for rating the security of the curve.

(d) Give a sensible upper and lower bound for the cardinality of the curve $E(\mathbb{F}_{11^4})$.