Secure and Dependable Systems Module: CO-566
Constructor University Date: 2023-04-21
Dr. Jürgen Schönwälder **Due: 2023-04-28**

Problem Sheet #10

Problem 10.1: *points of an elliptic curve and orders of cyclic subgroups* (1+2 = 3 points)

Consider the elliptic curve $E(Z_{11}) = \{\, (x, y) \in Z_{11} \times Z_{11} \,|\, y^2 = x^3 + 1 \,\}$.

a) Determine the set of points of the elliptic curve $E(Z_{11})$.

b) For each point $P \in E(Z_{11})$, which is not infinity, determine its cyclic subgroup and the order of the subgroup. The cyclic subgroup of P is obtained by computing the set $C_p = \{\, n{\cdot}P \,|\, n \geq 0 \,\}$. The order of $|C_p|$ is the number of elements of C_p.

Problem 10.2: *elliptic curve diffie hellman key exchange* (1+1+1 = 3 points)

Alice and Bob execute a Diffie-Hellman key exchange. They agree on using the point $P = (24, 80)$ on the elliptic curve $E(Z_{191}) = \{\, (x, y) \in Z_{191} \times Z_{191} \,|\, y^2 = x^3 + x + 1 \,\}$.

a) Alice randomly chooses $a = 12$. Which point does Alice send to Bob?

b) Bob randomly chooses $b = 7$. Which point does Bob send to Alice?

c) What is the shared secrect that Alice and Bob calculate?

Problem 10.3: *elliptic curve digital signatures* (1+1+1+1 = 4 points)

Let $E(Z_p)$ be an elliptic curve and $G \in E(Z_p)$ a point on the curve defining a group over $E(Z_p)$ with the order n. The sender chooses a private key $k \in Z_p$ and determines the corresponding public key $K = k \cdot G$. The algorithm to create signatures works as follows:

S1 Using the hash function H, create a hash $h = H(m)$ of the document m to be signed.

S2 Select a fresh random number e in the range $[1, n-1]$ (or instead derive e from a hash calculated over h and k).

S3 Calculate $P = e \cdot G$ and then let $r = P.x$ where $P.x$ refers to the x-coordinate of the point P. If $r = 0$, repeat with a different random number e.

S4 Calculate $s = e^{-1} \cdot (h + r \cdot k) \pmod n$ where e^{-1} is the modular inverse of e, such that $e \cdot e^{-1} \equiv 1 \pmod n$. If $s = 0$, repeat with a different random number e.

S5 The signature of m is the tuple (r, s).

The algorithm to verify signatures works as follows:

V1 Using the hash function H, create a hash $h' = H(m')$ of the received document m'.

V2 Calculate the modular inverse s^{-1} of s, such that $s \cdot s^{-1} \equiv 1 \pmod n$.

V3 Calculate $P' = (h' \cdot s^{-1}) \cdot G + (r \cdot s^{-1}) \cdot K$ and then let $r' = P'.x$.

V4 Test whether $r = r'$ holds.

Alice signs a message she is sending to Bob. Alice and Bob agree on using the elliptic curve $E(Z_{193}) = \{\, (x, y) \in Z_{193} \times Z_{193} \,|\, y^2 = x^3 + x + 1 \,\}$ and the point $G = (28, 65)$. The order of the subgroup is $n = 67$.

a) Alice chooses the private key $k = 37$. Calculate the corresponding public key K.

b) Alice picks the fresh random value $e = 21$. Calculate P and r.

c) The hash of the document m is the number $h = 123$. Calculate the signature (r, s) that Alice is going to send with the document m to Bob.

d) Bob obtains the document m' the signature (r, s) and he calculates the same hash number $h' = 123$. Show how Bob calculates the value of r' and determine whether Bob accepts the signature.