Technische Hochschule Rosenheim

Computer Science Fundamentals WS 2021/22

Prof. Dr. J. Schmidt; D. Stecher, M.Sc. Exercise 12

Please solve the following exercises at home prior to the tutorial

Exercise 1

An RSA-Participant sent a single encrypted symbol of numerical value 128. Their public key is (187, 7). Break the encryption by calculating the private key. What character was transmitted assuming a numbered alphabet starting with A=1?

For the next two exercises we'll be looking at the following elliptic curve over the finite field with 11 elements: $y^2 = x^3 + 2x + 10$

Exercise 2

a) Does the above equation satisfy the conditions for an elliptic curve?

b) Determine all points (x, y) on this curve
(Hint: There's a total of 7 points, not counting the neutral element).

Exercise 3

Calculate a Diffie-Hellman key exchange using the above curve.

a) Which of the following points can in principle be used as a public element g? Which one is secure, i.e., which one is a primitive element?
(1, 2), (7, 2), (9, 3)

b) The public generator is $g = (4, 7)$. Alice chooses the secret number $x_A = 3$, Bob chooses $x_B = 6$. Determine the shared key by performing the calculations for both sides (Alice und Bob).