Technische Hochschule Rosenheim

Computer Science Fundamentals WS 2021/22

Prof. Dr. J. Schmidt; D. Stecher, M.Sc. Exercise 11

Please solve the following exercises at home prior to the tutorial

Exercise 1

Bob sends the message `LOESUNG` to Alice. They have agreed to use the 26 latin letters (A→0, B→1, …) and use a simple substitution cipher for encryption with multiplicative key 7 and additive key 9.

a) What's the encrypted message?
b) How can Alice determine the original text from the encrypted message?

Exercise 2

For the Diffie Hellman key exchange we need two numbers: A prime number p and an integer $g \in \{2, 3, \ldots, p-2\}$.
We choose p = 19 and g = 3.

a) Alice now picks the secret exponent 3, Bob chooses 2.
   - Which number is sent from Alice to Bob?
   - Which number is sent from Bob to Alice?
   - What is the generated key?
b) Show that p is not a safe prime number.
c) Show that g is a primitive root modulo p.
d) The generated key is now used as a one-time pad in binary form. We receive the ciphertext 5 (decimal). What is the plaintext message?

Exercise 3

In RSA, each participant publishes a key (n, c), where n is the product of two large prime numbers p and q, and c is an exponent. Bob chooses the prime numbers $p=3$ and $q=11$.

a) Determine all possible numbers that would be suitable for Bob as public key c.
b) Bob uses the second smallest possible number as his public key. Calculate Bob's secret key d.
c) Alice wants to send the message „EI“ to Bob. Calculate the encrypted message. The numeric encoding of the letters is their position in the alphabet starting with 1 (A=1,…).
d) Bob received the encrypted message „RGAM“ and wants to decrypt it. What calculations does he have to perform?