"Begin at the beginning," the King said gravely,
"and go on till you come to the end: then stop."

— Lewis Carroll, Alice in Wonderland

# Project and Training 2
# Mathematics Part

## BSc in Computer Science
## Autumn Semester 2020

### Structure

The Mathematics part is divided into two independent sections - the first topic is **Linear Algebra** and the second is the **RSA-Algorithm**.

The **RSA-tasks** build upon the topics **Number Theory and Cryptography**, covered in *Discrete Mathematics I* last year. In order to complete them you will also need the two pairs of primes, the three messages and a public key that will be sent to you personally by email.

### Deliverables

**Linear Algebra:** A single pdf-file of your solutions. Solutions written in a suitable word processing system such as LaTeX are preferred, but you may also write your solutions by hand. In the latter case, provide a proper scan of your solutions. The pdf-file containing your solutions should be uploaded into the corresponding tool in moodle.

**RSA-Algorithm:** Please submit your code and answers electronically via moodle.

### Evaluation

The following criteria are important for the evaluation

1. Correctness of both the results and your derivations
2. Completeness of your arguments
3. Mathematical style and readability

Each of the four exercises in Linear Algebra exercises is dotted with 2 points. The RSA-exercise can help you attain 4 points. To successfully accomplish the Mathematics part of P&T 2 a minimum of 9 out of 12 points is required.

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

**Exercise 1** The following three points are given $A(1,1)$, $B(2,3)$, $C(3,7)$. All the calculations are to be carried out by hand.

a) Determine the quadratic polynomial

$$p_2(x) = ax^2 + bx + c \ ,$$

whose graph passes through these three points.

b) Determine all cubic polynomials

$$p_3(x) = ax^3 + bx^2 + cx + d \ ,$$

whose graph passes through the three points.

**Exercise 2** In a car model, power steering S and air conditioning K are optional extras. For a particular delivery $100'000$ vehicals were produced. In these vehicals, S was installed $65'100$ times and K was installed $12'600$ times. All the calculations are to be carried out by hand.

a) Set up the system of linear equations.

b) Solve the system of linear equations and give all ***meaningful*** solutions.

c) What is the minimum number of vehicles that had no special equipment?

**Exercise 3** As a result of several mergers and acquisitions, stock in four companies has been distributed among the companies. Each row of the following table gives the percentage of stock in the four companies that a particular company owns and the annual net income of each company (in millions of swiss francs):

| Firma | A | B | C | D | Profit (in Million CHF) |
|---|---|---|---|---|---|
| A | 71% | 8% | 3% | 7 % | 3.2 |
| B | 12% | 81% | 11% | 13% | 2.6 |
| C | 11% | 9% | 72 % | 8 % | 3.8 |
| D | 6% | 2% | 14 % | 72 % | 4.4 |

So company A holds 71% of its own stock, 8% of the stock in company B, 3% of the stock in company C, etc. For the purpose of assessing a state tax on corporate income, the taxable income of each company is defined to be its share of its own annual net income plus its share of the taxable income of each of the other companies, as determined by the percentages in the table. What is the taxable income of each company?

a) Set up the system of linear equations by hand.

b) Use a calculator or computer to solve the system of linear equations and include the final answer in the file with your results.

**Exercise 4** If $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the eigenvalues of a $n \times n$ matrix $A$, prove the following:

a) $A^T$ has the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$.

b) If $A$ is upper triangular, then its eigenvalues are exactly the main diagonal entries.

c) The inverse matrix $A^{-1}$ has eigenvalues $\frac{1}{\lambda_1}, \frac{1}{\lambda_2}, \ldots, \frac{1}{\lambda_n}$.

d) If $k \in \mathbb{R}$ then the matrix $A - k \cdot \mathbb{I}$ has eigenvalues $\lambda_1 - k, \lambda_2 - k, \ldots, \lambda_n - k$.

e) If $k \in \mathbb{N}$ then the matrix $A^k$ has eigenvalues $\lambda_1^k, \lambda_2^k, \ldots, \lambda_n^k$.

**Exercise 5** Using Java or Kotlin, implement the RSA algorithm for encrypting and decrypting so that the following tasks can be completed.

a) First convert your first message into ASCII and then encrypt it using the RSA algorithm using your first pair of primes. List the code with **annotations**, **describing** the main steps of the algorithm as well as the output it generated when you encoded your first message.

b) Next, explain the purpose of hashing a message in $1-3$ sentences and explain algorithmically (in words), how you would implement it.

c) Next decrypt your encoded message using the second pair of primes and convert it back from ASCII. List the code with **annotations describing** the main steps of the algorithm, and the output it generated when you decoded your second message.

d) You suspect that the public key that the encrypted third message was written in, was poorly chosen, in that the two primes used to generate it were very close together. Write the code to crack the key and decode the message. Use the method, discussed in the *Discrete Mathematics I* script and notes.

e) RSA is not widely used in the industry anymore. Write a brief paragraph ($< 300$ words) describing where RSA is still used, why it is not used as widely as before, what are some of the popular encryption methods today and what their advantages over RSA are.