IAM504 Public Key Cryptography **Spring 2020-2021**
Homework 4 **Due: 05.07.2020**

Question 1

Implement Koblitz Imbedding for the curve

$$y^2 = x^3 + ax + b$$

over $\mathbb{F}_p$ where a, b and p are given in the file `parameters.txt`.

Your program should read an input text from a file `input_text` (take a look at the attached code if you need a refresher), encode it into an integer m and represent it as a point $P = (x, y)$ on the curve using Koblitz Imbedding, then print the point on the console. Take the failure probability as $2^{-\kappa} = 2^{-30}$. Also print out the j value in $x = m\kappa + j$ for the correct x.

Imbed the following three text strings as points on the curve and print the result as above. We don't want a pdf report for this homework so write these values at the beginning of your code as comments.

- Is it imbed or embed?
- Koblitz calls it imbed.
- And a text of your choosing

Question 2

Implement ECDH between two people A and B using the above curve. The generator point G and its order n is also given in `parameters.txt`. Randomly choose a secret key for A and B, find their public keys and the shared secret. Print their private and public keys and the shared secret on the console.

You'll need to implement point addition, point doubling and scalar multiplication. Implement double and add for scalar multiplication.

Guidelines and Implementation Considerations

- You don't have to write a report for this homework.
- You are required to use MPIR library (or GMP). Do not use any other big integer library.
- Your code must be C or C++.
- Write comments in the code if necessary.
- Upload your homework to odtuclass.
- For your codes, only send the .c/.cpp, .h/.hpp. Please don't send the project / solution files, or the executable.
- Include a note about your operating system (win 10, linux distribution etc.) and your IDE (visual studio, devc++, codeblocks...) or your compiler.
- Do not steal your code. You can study other code and give references to them. Copying others code and just changing the variable names is not the purpose of this homework.
- This is not a group homework. You can study with others, but don't copy each others code.