PROGRAM ROZWOJOWY
POLITECHNIKI WARSZAWSKIEJ

Propozycja wykładu

Title: **Algorithmic Number Theory**.

ECTS: **4**
JD: **2 (OT, PZ, PZ-O, PZ-ISI)**

Objective: The purpose of this course is to introduce the students to various aspects of algorithmic number theory.

Description: The lecture offers a background to cryptology and its applications in various domains. After having introduced a set of basic notions and subject matter terminology algorithms for proving that an integer is probably a prime number will be discussed. Then, it will be explained how to compute quickly the exponentiation of an element of a group, and how to apply this, say, in the context of a public-key algorithm such as RSA or the key-exchange protocol of Diffie-Hellman. A special slot of the lecture will be devoted to the problems of finite fields, and how to describe them in an efficient way from the computational point of view. Next, the notion of an elliptic curve defined over a field will be introduced and discussed. These curves lead to commutative groups, and we will explain the law group, both from an intuitive point of view, and also with explicit formulas. Then, we will focus on the situation of elliptic curves defined over finite fields, especially Z/pZ, whereas p is a prime number > 3. Some methods for the computation of the number of points of elliptic curves over prime finite fields, culminating with Schoof's polynomial algorithm will be presented, analyzed and evaluated.

The lecture is thoroughly illustrated by a number of “real life” examples, particularly in this part of the lecture that refers to Artificial Intelligence techniques and algorithms. Some examples will require interaction with students.

Duration: 30 hours.

Remarks: This lecture has been delivered to the students of the Luxembourg University as part of the Master in Computer Science and also to the students of Master in Mathematics interested in computer science matters.

The lecture is particularly addressed to the students interested in security and cryptology. It is assumed that the students will have a solid mathematical background and a knack to applied mathematics.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY