Public-Key Cryptology

Course title:

Public-Key Cryptology

Course timing:	**May 18 & 19 2017**
Mode of study:	**Lectures: 10 hours**

Prerequisites for entering the course:

Students should be able to think in abstract terms, and have followed basic courses in mathematics.

Course summary& organization:

The main challenges of cryptology will be outlined. A description of the principles of public-key cryptology and digital signatures will be provided from a historical point of view. An overview of complexity, prime number generation, public-key algorithms will be provided as well. The main problems underlying the security of public-key algorithms will be addressed. Should time allow, one of the problems of the millennium will be described, as far as it is linked to objects used in cryptology. The course itself will be organized around conferences and lectures. Conferences will provide a general overview, whereas Lectures will go deeper into the material.

Teacher:

Prof. Dr. Franck Leprévost (University of Luxembourg – UL) is the founder of the Laboratory of Algorithmic, Cryptology and Security, and was the vice-president of the University of Luxembourg during 10 years. Launched in 2003, the UL is nowadays among the top 200 universities in the world. His research includes algorithmic number theory & cryptology. He is member of the board of Luxtrust SA, of UNICA, senior advisor to the leadership of universities throughout the world. He spent the most part of 2016 at the Peter the Great St Petersburg Polytechnic University. In his free time, he is an art collector & dramatist. His last play – "La chambre des larmes" in French – will soon be available electronically (ebook) in Russian speaking countries under the title "Комната слез".

Conferences & Lectures outline (subject to changes):

Title	Duration
James Bond's most secret weapon	1:30 hours
Complexity: How big is big? How fast is fast?	1:30 hours
The elementary particles of the integers	2 hours
Cryptology principles from Cesar to Luxtrust	2 hours
Public-key algorithms and John Cage's approach (in more than 4'33") to heavy problems	1:30 hours
Malevich's painted squares and the Birch and Swinnerton-Dyer conjecture	1:30 hours