MPRI – cours 2-12

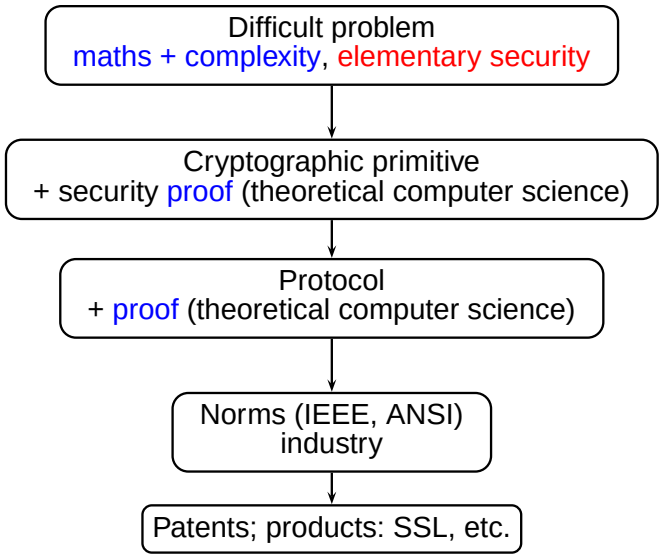
In order of appearence:

F. Morain, P. Gaudry, Phong Nguyen;
David Pointcheval, Louis Granboulan

morain@lix.polytechnique.fr

`http://www.lix.polytechnique.fr/Labo/Francois.Morain/MPRI`

Goals



There is a scientific community looking at any of these problems, in France or abroad.

Schedule (1/2)

When	Who	What
17/09	François Morain	Primality
24/09	François Morain	Elementary factorization
01/10	François Morain	Number fields and factorization
08/10	Pierrick Gaudry	Elliptic curves
15/10	Pierrick Gaudry	Hyperelliptic curves
22/10	Pierrick Gaudry	Pairings
29/10	Phong Nguyen	Euclidean lattices
05/11	Phong Nguyen	Cryptographic applications of lattices
12/11	Partiel	
19/11	Partiel	

Partiel = read and understand a research paper from a given list.

Schedule (2/2)

When	Who	What
26/11	David Pointcheval	Security models
03/12	David Pointcheval	Examples of security proofs
10/12	Louis Granboulan	Stream ciphers
17/12	David Pointcheval	Proofs of knowledge and distributed cryptography
07/01	David Pointcheval	Pairing based cryptography
14/01	Louis Granboulan	Block ciphers
21/01	Louis Granboulan	Operating modes
28/01	Louis Granboulan	Lightweight cryptography
04/02	Exam	

Exam: written exam, with 1 exercise per part.

Format for my part

2 hours lecture + 1 hour exercises.