MPRI – cours 2-12-2

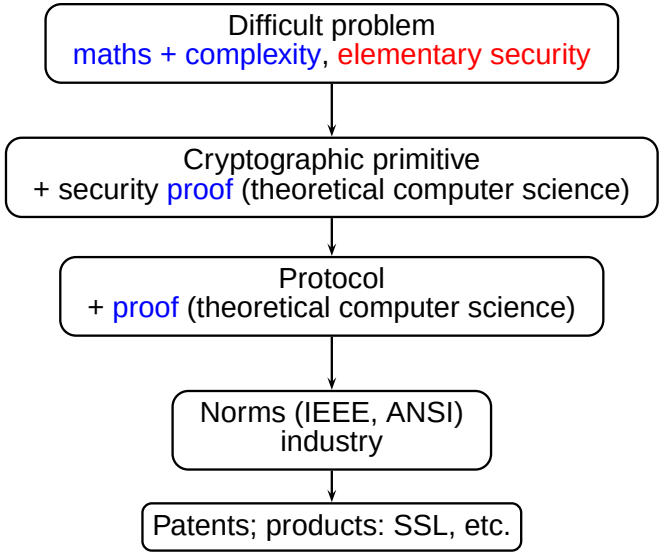
In order of appearence:

F. Morain, E. Thomé, B. Smith

morain@lix.polytechnique.fr

`http://www.lix.polytechnique.fr/Labo/...`
`.../Francois.Morain/MPRI/2009`

Goals



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

Schedule

When	Who	What
23/11	François Morain	Introduction; Primality
30/11	François Morain	Generic groups; Elementary factorization
07/12	Emmanuel Thomé	Integer Factorization (I)
14/12	Emmanuel Thomé	Integer Factorization (II); sparse linear algebra
04/01	Emmanuel Thomé	Number Field Sieve
11/01	Ben Smith	Elliptic curves
18/01	Ben Smith	Hyperelliptic curves
25/01	Ben Smith	Pairings
01/02		Written exam

Format for my part: 2 hour lecture + 1 hour exercises.

Cryptographic motivations: two algorithms

A) Diffie-Hellman

Public parameters: p prime number, g generator of $\mathbb{F}_p^*$.
Protocol:

$$A \xrightarrow{g^a \bmod p} B$$

$$A \xleftarrow{g^b \bmod p} B$$

$$A : K_{AB} = (g^b)^a \equiv g^{ab} \bmod p$$

$$B : K_{BA} = (g^a)^b \equiv g^{ab} \bmod p$$

DH problem: given (p, g, g^a, g^b), compute g^{ab}.

DL problem: given (p, g, g^a), find a.

Thm. DL $\Rightarrow$ DH; converse true for a large class of groups (Maurer & Wolf).

$\Rightarrow$ **Goal for us:** find a good resistant group.

B) RSA

Key generation: Alice chooses two primes p and q, $p \neq q$, $N = pq$, e s.t. $\gcd(e, \lambda(N)) = 1$, $d \equiv 1/e \bmod \lambda(N)$.

Public key: (N, e).

Private key: d (or (p, q)).

Encryption: Bob recovers the authenticated public key of Alice; sends $y = x^e \bmod N$.

Decryption: Alice computes $y^d \bmod N \equiv x \bmod N$.

Rem. of course, in real life, more has to be done, but this has already been told somewhere else.

$\Rightarrow$ **Goal for us:** what size should N have, in order not to be factored?