MPRI – cours 2.12.2

In order of apparition:

F. Morain, P. Gaudry, B. Smith

morain@lix.polytechnique.fr

`http://www.lix.polytechnique.fr/Labo/...`
`.../Francois.Morain/MPRI/2013`

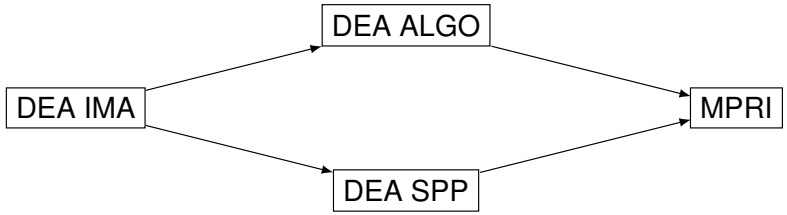
I. Administrative details

Schedule: 16 $\times$ 1.5 hour lectures (1/2)

When	Who	What
23/09	François MORAIN	Groups in crypto (I): Z/NZ, finite fields
30/09	François MORAIN	fast arithmetic, factoring polynomials over finite fields
07/10	François MORAIN	Composition, primality
14/10	François MORAIN	Integer factorization: elementary algorithms
21/10	François MORAIN	Integer factorization: sieves
28/10	Pierrick GAUDRY	discrete logarithms (I)
04/11	Pierrick GAUDRY	discrete logarithms (II)
11/11	–	–
18/11	Pierrick GAUDRY	discrete logarithms (III)
25/11	François MORAIN	lab
02/12	mid-term exam	??? 17:45-19:15

Life after MPRI (2.12.2)

A lot of students attended this course over the years:



A lot did a phD: see next slide.

After their phD + postdoc:

- Academic careers: University, CNRS, INRIA.
- Governemental agencies.
- Other paths.

A short list of recent phD/students

LIX:

- R. Dupont (*Moyenne arithmético-géométrique, suites de Borchardt et applications*, 2006);
- J.-F. Biasse (*Subexponential algorithms for number fields*, defense 20/09/10);
- L. De Feo (*Fast algorithms for towers of finite fields and isogenies*, defense 12/10).

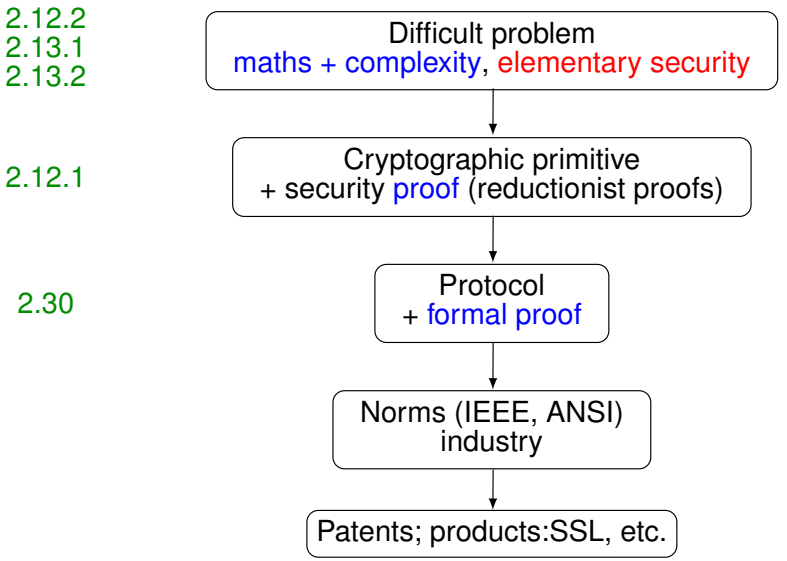
LORIA:

- D. Stehlé (*Algorithmique de la réduction de réseaux et application à la recherche de pires cas pour l'arrondi de fonctions mathématiques*, 2005);
- L. Fousse (*Intégration numérique avec erreur bornée en précision arbitraire*, 2006);
- D. Robert (*Theta functions and applications in cryptography*, defense 21/07/10);
- G. Bisson (*ring of endomorphisms*, defense 2011);
- R. Cosset (*theta functions*, defense 2011).

Internships

II. Overview of the lectures

Goals



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.

The difficulty of discrete logarithm computations

Over finite fields:

- $\mathbb{F}_p$:
  - Best algorithm so far: *à la* NFS $O(L_p[1/3, c'])$ (Gordon, Schirokauer).
  - record with $160dd$: T. Kleinjung (2007); 3.3 years of PC 3.2 GHz Xeon64; matrix $2,177,226 \times 2,177,026$ with $289,976,350$ non-zero coefficients, inverted in 14 years CPU.
- $\mathbb{F}_{p^n}$: Adleman-DeMarrais, function field sieve + optimizations.
  - $p = 2$: Coppersmith; $\mathbb{F}_{2^{809}}$: Gaudry *et alii* (2013).
  - record $\mathbb{F}_{36\times 71}$: Hayashi *et al.* (2010).
  - Medium p case: Joux+Lercier; etc.; **lots of results in 2012-2013**; **Barbulescu/Gaudry/Thomé/Joux (2013): doable in quasipolynomial time** $\Rightarrow$ special emphasis on discrete logarithms this year @MPRI.

$$L_N[\alpha, c] = \exp((c + o(1))(\log N)^\alpha (\log\log N)^{1-\alpha}).$$

ECDLP

ECC112b: taken from
`http://lacal.epfl.ch/page81774.html`,
Bos/Kaihara/Kleinjung/Lenstra/Montgomery (EPFL/Alcatel-Lucent Bell Laboratories/MSR)

$p = (2^{128} - 3)/(11 \cdot 6949)$, curve secp112r1

- 3.5 months on 200 PS3; 8.5×10^{16} ec additions ($\approx$ 14 full 56-bit DES key searches); started on January 13, 2009, and finished on July 8, 2009.
- half a billion distinguished points using 0.6 Terabyte of disk space.

As a quick comparison

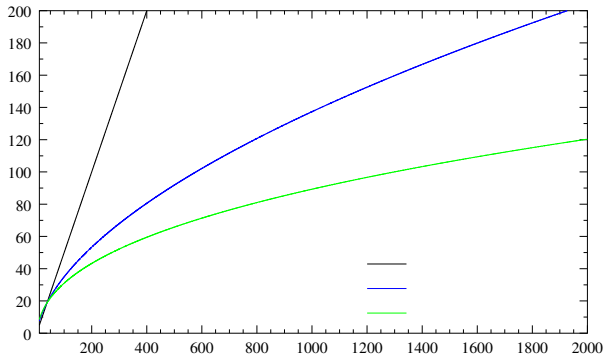


FIG.: (Log of) Security vs. bit size of key (exponential, $L(1/2)$, $L(1/3)$)

$$L_x[\alpha, c] = \exp\left((c + o(1))(\log x)^\alpha (\log\log x)^{1-\alpha}\right).$$

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.

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

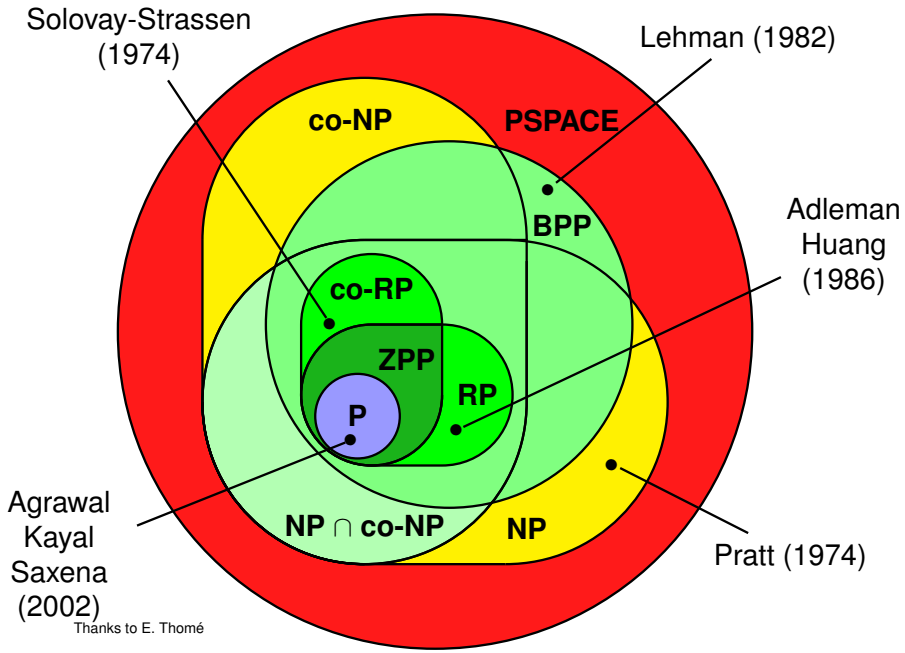
Rules of the game

$$N = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

- What do we do in practice? Which size is doable?
  Factorization : number field sieve
  $O(\exp(c(\log N)^{1/3}(\log\log N)^{2/3}))$; 768 bits (a lot of people, 2010).
  Primality: hopefully without too much factoring, past some easy trial division; 25,000 decimal digits.
- Complexity question: to which class does **isPrime?** belong?

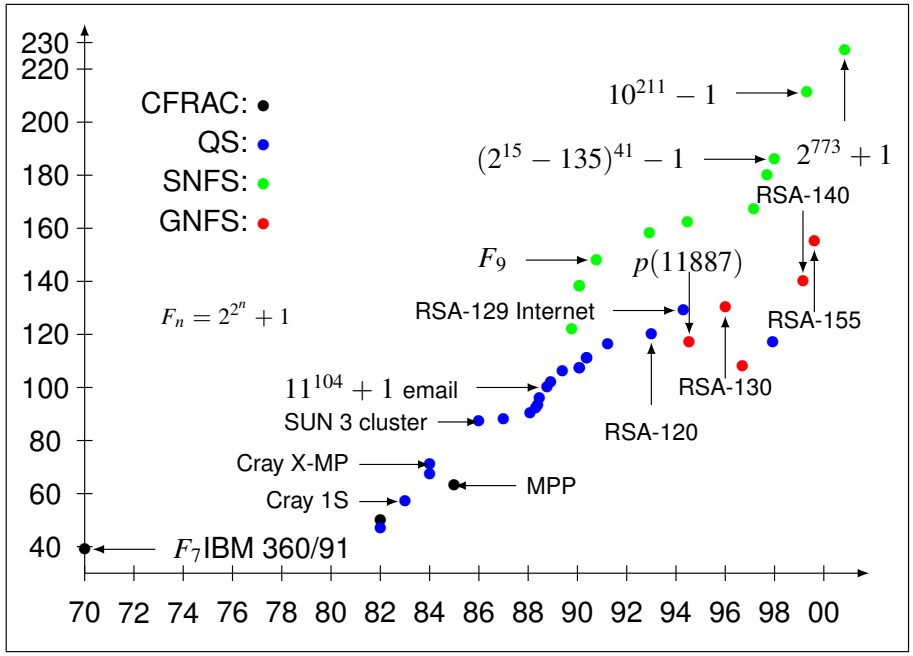
Best : **P** (e.g., integer multiplication).
At least : **RP**.
And: what about a proof?

Complexity classes



Thanks to E. Thomé

How difficult is factoring?



Also: 03/1991: 2,463+ (c101) on a Cray Y-MP4/464; 04/1992: RSA-110 on a MasPar (16K nodes).

The cluster era