MPRI – cours 2.12.2

In order of apparition:

F. Morain, E. Thomé, B. Smith

morain@lix.polytechnique.fr

```
http://www.lix.polytechnique.fr/Labo/...
        .../Francois.Morain/MPRI/2011
```

I. Administrative details

Schedule: 16 × 1.5 hour lectures (1/2)

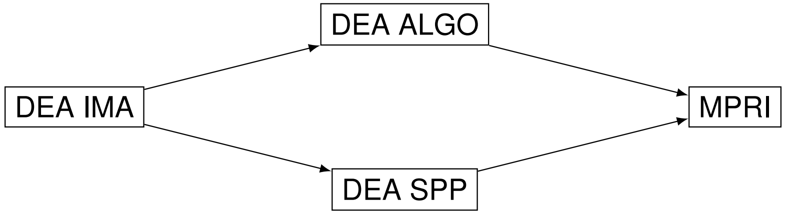
When	Who	What
13/09	François Morain	Groups in crypto (I): Z/NZ, finite fields
20/09	François Morain	Groups in crypto (II): elliptic curves
27/09	François Morain	Composition, primality
04/10	François Morain	Integer factorization: elementary algorithms
11/10	François Morain	Discrete logarithm
18/10	François Morain	TD
25/10	Emmanuel Thomé	Factorization (II)
08/11	Emmanuel Thomé	Factorization (III)
15/11	Emmanuel Thomé	Sparse linear algebra
22/11	Emmanuel Thomé	TD
29/11	mid-term exam	**??? 14:00-15:30**

Schedule: 16 × 1.5 hour lectures (2/2)

When	Who	What
29/11	mid-term exam	**??? 14:00-15:30**
06/12	Emmanuel Thomé	Number field sieve (I)
13/12	Emmanuel Thomé	Number field sieve (II)
03/01	Ben Smith	Elliptic curves (I)
10/01	Ben Smith	Elliptic curves (II)
17/01	Ben Smith	Hyperelliptic curves (I)
24/01	Ben Smith	Hyperelliptic curves (II)
31/01	Ben Smith	Pairings (I)
07/02	Ben Smith	Pairings (II)
14/02	Ben Smith	TD
21/02	Final exam	**??? 13:45-15:45**

Life after MPRI (2.12.2)

A lot of students attended this course over the years:



DEA IMA

DEA ALGO

DEA SPP

MPRI

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).

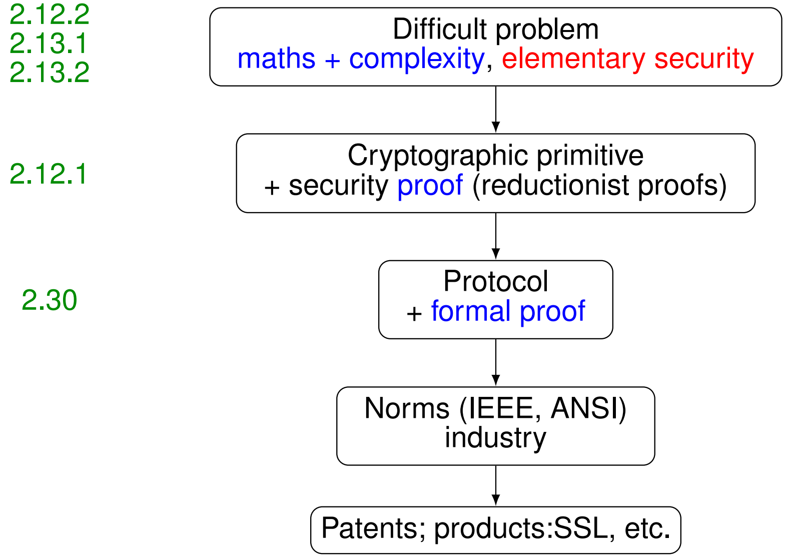
LORIA:

- 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



2.12.2
2.13.1
2.13.2

Difficult problem
maths + complexity, elementary security

2.12.1

Cryptographic primitive
+ security proof (reductionist proofs)

2.30

Protocol
+ formal proof

Norms (IEEE, ANSI)
industry

Patents; products:SSL, etc.

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; record with $\mathbb{F}_{2^{613}}$: Joux/Lercier (2005).
  - record $\mathbb{F}_{3^{6\times 71}}$: Hayashi *et al.* (2010), `http://eprint.iacr.org/2010/090`.
  - Medium p case: Joux+Lercier.

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

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

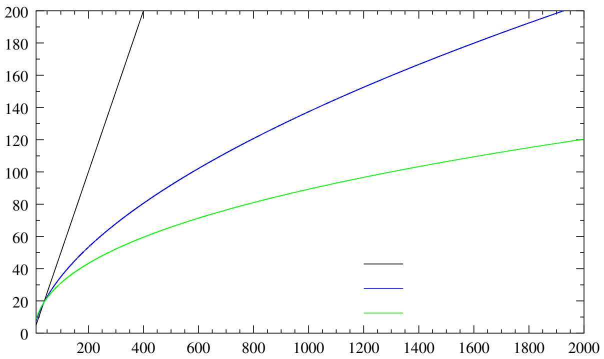


FIG.: (Log of) Security vs. bit size of key (exponential, $L(1/2)$, $L(1/3)$)

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

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?

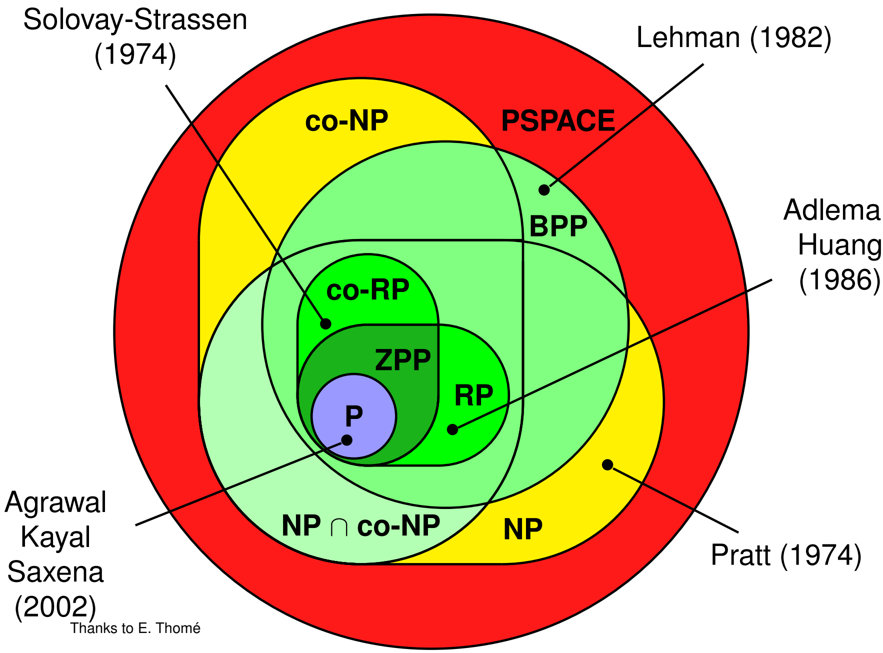
Rules of the game

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

- 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?

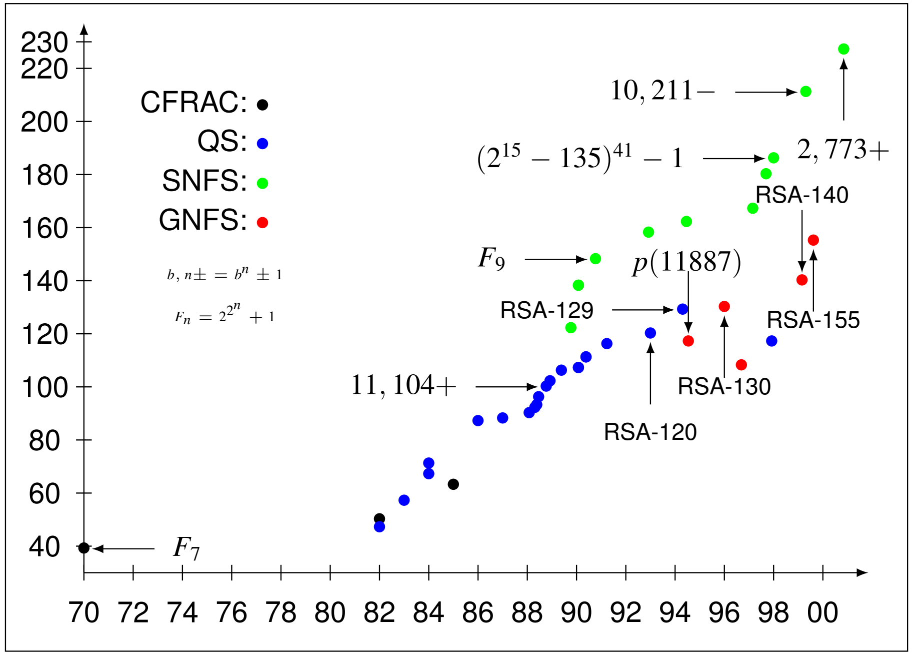
Best : **P** (e.g., integer multiplication).
At least : **RP**.
And: what about a proof?

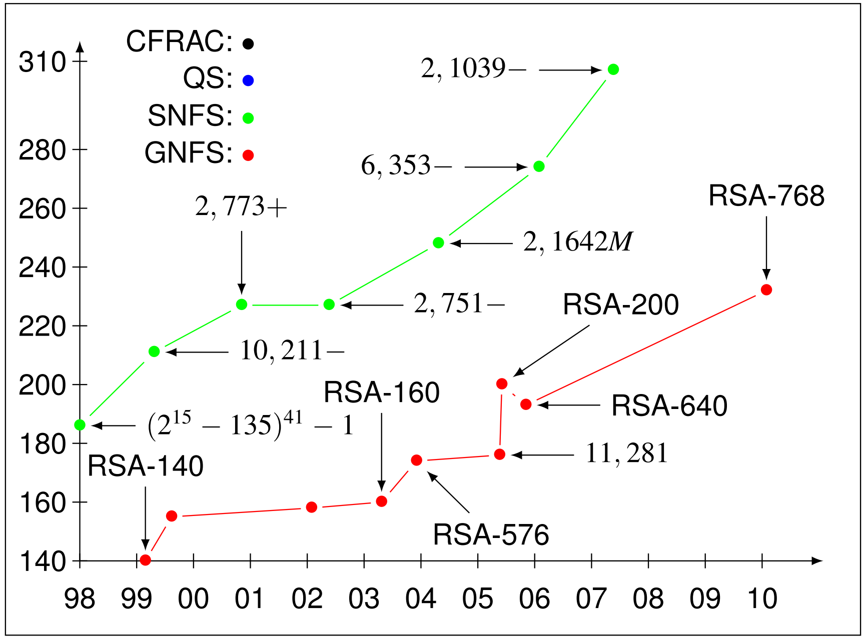
Complexity classes



Thanks to E. Thomé

How difficult is factoring?


CFRAC: ●
QS: ●
SNFS: ●
GNFS: ●
$b, n\pm = b^n \pm 1$
$F_n = 2^{2^n} + 1$
$(2^{15} - 135)^{41} - 1$
RSA-140
F_9
$p(11887)$
RSA-129
RSA-155
RSA-130
RSA-120
F_7


CFRAC: ●
QS: ●
SNFS: ●
GNFS: ●
RSA-768
2, 1642M
RSA-200
RSA-160
RSA-640
$(2^{15} - 135)^{41} - 1$
RSA-140
RSA-576