MPRI – cours 2.12.2

In order of apparition:

F. Morain, B. Smith, R. J. Barbulescu

morain@lix.polytechnique.fr

`http://www.lix.polytechnique.fr/Labo/...`
`.../Francois.Morain/MPRI/2014`

I. Administrative details

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

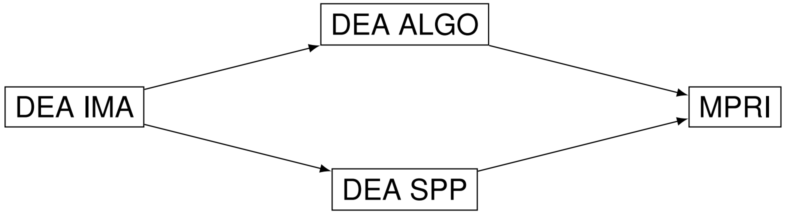
When	Who	What
15/09	François MORAIN	Groups in crypto (I): Z/NZ, finite fields
22/09	François MORAIN	fast arithmetic, factoring polynomials over finite fields
29/09	François MORAIN	Composition, primality
06/10	François MORAIN	Integer factorization: elementary algorithms
13/10	Ben SMITH	Elliptic curves (I)
20/10	Ben SMITH	Elliptic curves (II)
27/10	Ben SMITH	Elliptic curves (III)
03/11	Ben SMITH	Elliptic curves (IV)
10/11	–	–
17/11		TD
24/11		mid-term exam ?
01/12		mid-term exam ?

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

When	Who	What
08/12	Ben SMITH	Hyperelliptic curves (I)
15/12	Ben SMITH	Hyperelliptic curves (II)
05/01	Ben SMITH	Pairings (I)
12/01	Ben SMITH	Pairings (II)
19/01	Ben SMITH	TD
26/01	Razvan J. BARBULESCU	Sieves
02/02	Razvan J. BARBULESCU	NFS
09/02	Razvan J. BARBULESCU	Discrete Logarithms (I)
16/02	Razvan J. BARBULESCU	Discrete Logarithms (II)
23/02	Razvan J. BARBULESCU	TD
02/03		final exam ??
09/03		final exam ??

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:

- 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:

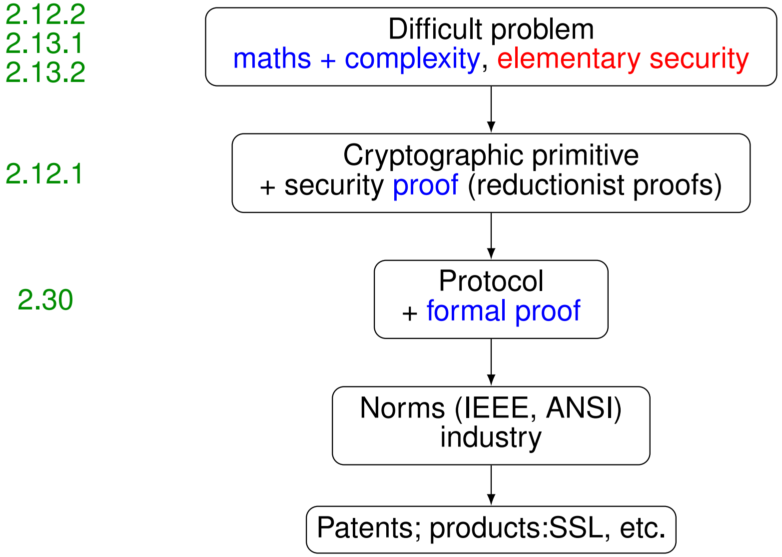
- L. Fousse (*Intégration numérique avec erreur bornée en précision arbitraire*, 2006);
- D. Robert (*Theta functions and applications in cryptography*, defense 21/07/10);
- G. Bisson (*ring of endomorphisms*, defense 2011);
- R. Cosset (*theta functions*, defense 2011).
- R. J. Barbulescu (*discrete logarithms*, defense 2013).

Internships

- F. MORAIN: primality proving with polynomials (AKS, Jacobi Sums, etc.);
- B. SMITH: algebraic curves, point counting algorithms.

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:

$$A \overset{g^a \bmod p}{\longrightarrow} B$$

$$A \overset{g^b \bmod p}{\longleftarrow} B$$

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

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

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 $180dd$ (2014): Bouvier/Gaudry/Imbert/Jeljeli/Thomé (CADO-NFS), matrix $7.28 \cdot 10^6$ rows and columns.
- $\mathbb{F}_{p^n}$: Adleman-DeMarrais, function field sieve + optimizations.
  - $p = 2$: Coppersmith; $\mathbb{F}_{2^{809}}$: Gaudry *et alii* (2013).
  - record $\mathbb{F}_{3^{6 \times 71}}$: 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** $\Rightarrow$ see end of the course.
  - $\mathbb{F}_{p^k}$, k small: Barbulescu/Gaudry/Guillevic/M. (2014)

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

ECDLP

ECC2K-108: (Harley *et al.*, taken from `http://cristal.inria.fr/~harley/`)

- 1300 individuals, 9500 machines, dec 1999 until april 2000.
- 200,000 days on a 450 MHz PC with MMX, i.e. more than 500 years. For comparison, cracking a 56-bit DES key by exhaustive search would take about 110,000 days.
- 2.8×10^{15} elliptic-curve operations of which 2.3×10^{15} led to distinguished points recorded at INRIA; 2.05 million distinguished points in 1.3 Gigabytes of email.

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.

ECDLP – cont'd

ECC2K-113: *Solving the discrete logarithm of a 113-bit Koblitz curve with an FPGA cluster*, E. Wenger & P. Wolfger, 2014.

24 days on an 18-core Virtex-6 FPGA cluster.

Hardware is fun:

- 165 MHz instead of maximum 275 MHz.
- (more or less related) one ECC-breaker per FPGA.

As a quick comparison

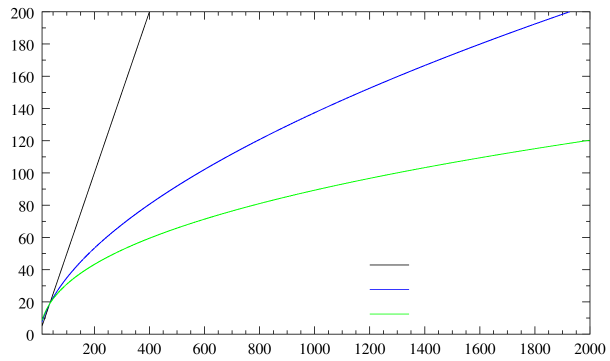


Figure : (Log of) Security vs. bit size of key (exponential, $L(1/2)$, $L(1/3)$)

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

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.

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

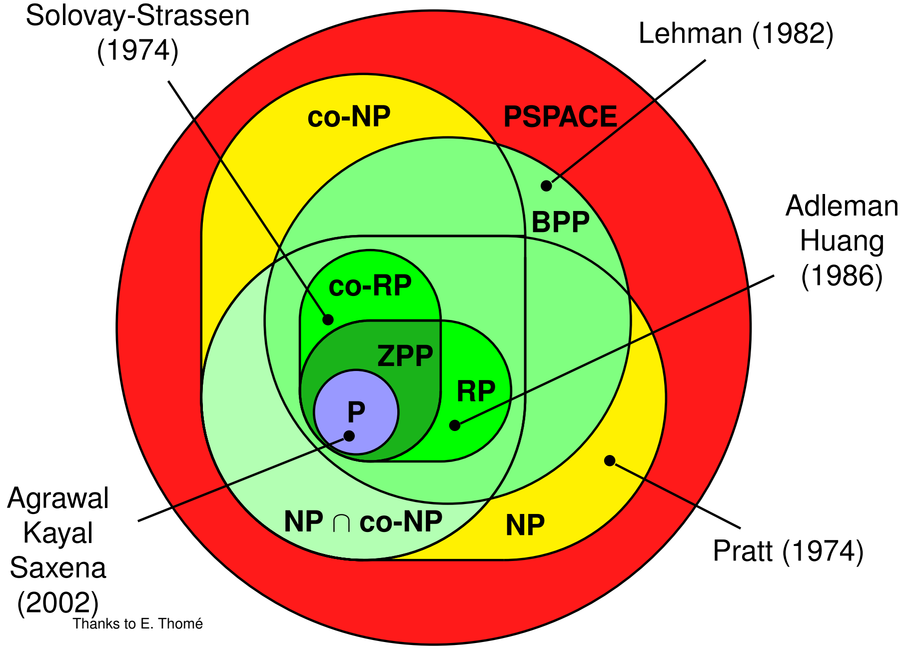
Rules of the game

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

- 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?

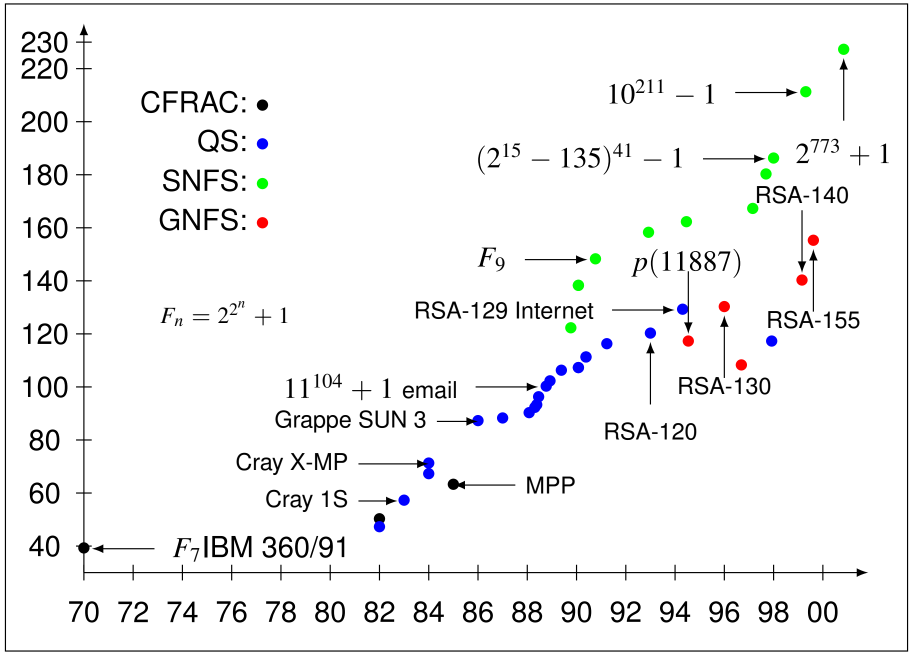
Best : **P** (e.g., integer multiplication).
At least : **RP**.
And: what about a proof?

Complexity classes



Thanks to E. Thomé

How difficult is factoring?



Et aussi: 03/1991: 2,463+ (c101) sur un Cray Y-MP4/464; 04/1992: RSA-110 sur une MasPar (16K nœuds).

The cluster era