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/2010

I. Administrative details

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

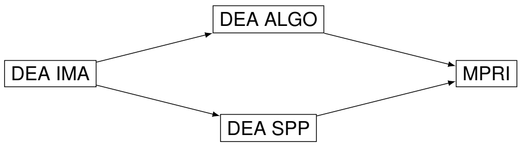
When	Who	What
14/09	François Morain	Primality and complexity
21/09	François Morain	Generic groups
28/09	François Morain	Smooth numbers and applications
05/10	François Morain	Computing discrete logarithms
12/10	Emmanuel Thomé	Factorization (I)
19/10		no lecture (ECC2010)
26/10	François Morain	TD
02/11	Emmanuel Thomé	Factorization (II)
09/11	Emmanuel Thomé	Factorization (III)
16/11	Emmanuel Thomé	Sparse linear algebra
23/11	Emmanuel Thomé	TD
30/11	mid term exam ?	?

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

When	Who	What
30/11	mid term exam ?	?
07/12	Emmanuel Thomé	Number field sieve (I)
14/12	Emmanuel Thomé	Number field sieve (II)
04/01	Ben Smith	Elliptic curves (I)
11/01	Ben Smith	Elliptic curves (II)
18/01	Ben Smith	Hyperelliptic curves (I)
25/01	Ben Smith	Hyperelliptic curves (II)
01/02	Ben Smith	Pairings (I)
08/02	Ben Smith	Pairings (II)
15/02	Ben Smith	TD
22/02	Exam	**Salle U/V, 12:45-15:45**

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).

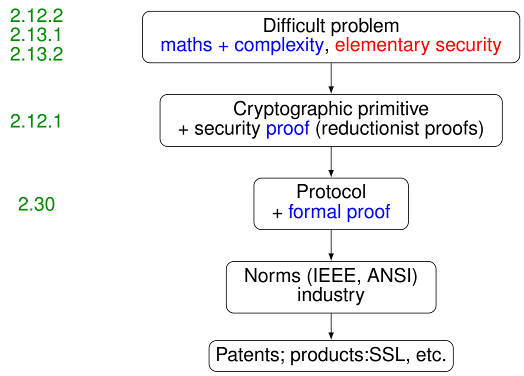
LORIA:

- 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.

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?

C) 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) $p = (2^{128} - 3)/(11 * 6949)$, 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

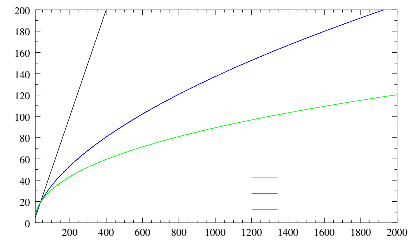
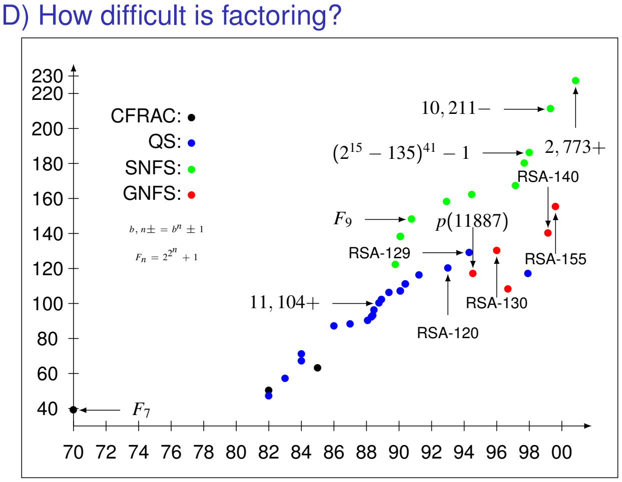
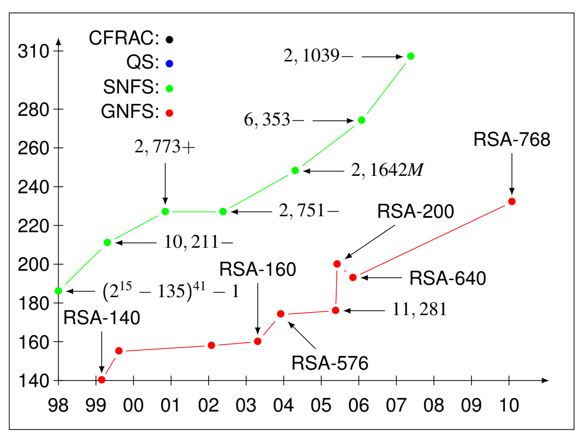


FIG.: (Log of) Security vs. bit size of key (exponential, $L(1/2)$, $L(1/3)$)

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

D) How difficult is factoring?





Primality is easier

See forthcoming lecture!