MT10 - Algèbre, Calcul Formel, Arithmétique

Vincent Robin

UTC - GI/LMAC

Printemps 2012

Intervenants :

- Dominique Fontaine : TD (jusqu'au 12 mai)
- Vincent Robin : cours (jusqu'au 12 mai) et TP (jusqu'à la fin)
- Walter Schön : cours + TD (en fin de semestre)

Chapitre 0 - Introduction à partir de RSA

de gauche à droite, SRA :

Adi Shamir, Ronald L. Rivest, Leonard Adleman

source : page web de Adleman.

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.
Rivest, Shamir, Adleman. (1978)
à lire absolument !

... et quelques 30 ans plus tard :

Annoncé le 7 janvier 2010 sur `http://www.mersenneforum.org/` :

We are pleased to announce the factorization of RSA768, the following
768-bit, 232-digit number from RSA's challenge list : (tronqué !)
1230186684530117755130494958384962720772853569595334792197322452150726365751874520219978646938995647494277406384592519255732630345376507917026122142913461670429214311602221240479274737794080665351419
6902143413.
The factorization, found using the Number Field Sieve (NFS), is :
3347807169895689878604416984821269081770479498371376856891
2431388982883793878002287614711652531743087737814467999489 *
3674604366679959042824463379962795263227915816434308764267
6032283815739666511279233373417143396810270092798736308917
Both factors have 384 bits and 116 digits.

Cryptosystème : vocabulaire (anglais)

- message clair alphabétique (plaintext)
- message clair numérique (plaintext ?)
- message crypté (ciphertext)
- coder, numériser (to encode)
- crypter, chiffrer (to encrypt, to encipher)
- décrypter, déchiffrer (to decrypt, to decipher)
- alphabétiser ? (to decode)

Lire : `http://fr.wikipedia.org/wiki/Chiffrement`
Faire un schéma !
Autres : confidentialité (privacy), intégrité, signature, ...

cryptosystème RSA : description du cœur

fonctionne avec 3 paramètres : N, e, d

- Clé publique : (N, e)
  $N = pq$, où p et q sont 2 (grands) nombres premiers (secrets !)
  e entier premier avec $\phi(N) = (p-1)(q-1)$
- Clé privée : d
  d est l'inverse de e modulo $\phi(N)$
- crypter : une exponentiation modulaire

$$\begin{array}{rcl} RSA_{(N,e)} : \mathbb{Z}/N\mathbb{Z} & \longrightarrow & \mathbb{Z}/N\mathbb{Z} \\ x & \longmapsto & x^e \end{array}$$

- décrypter : encore une exponentiation modulaire

$$\begin{array}{rcl} RSA_{(N,d)} : \mathbb{Z}/N\mathbb{Z} & \longrightarrow & \mathbb{Z}/N\mathbb{Z} \\ x & \longmapsto & x^d \end{array}$$

cryptosystème RSA : comment ça marche ?

Théorème (petit théorème de Fermat)

Soit p un nombre premier. Alors on a : $(\forall x \in \mathbb{Z}) \qquad p | x^p - x$,
et si, de plus, $x \wedge p = 1$, *alors* $p | x^{p-1} - 1$.

<u>Démonstration</u> : élémentaire, par récurrence sur x, ... $\square$

Preuve de RSA

1. Il s'agit de vérifier que $(\forall x \in \mathbb{Z}/N\mathbb{Z}) \qquad x^{ed} = x$.
2. Par hypothèses sur e et d, on obtient (avec Bézout) l'existence de $k \in \mathbb{N}$ tel que $ed = k(p-1)(q-1) + 1$.
3. On conclut avec le petit théorème de Fermat.

RSA : d'autres questions ...

- Comprendre les détails de ce qui précède
  ($\mathbb{Z}/N\mathbb{Z}$, ses inversibles, ϕ, ...)
- Générations des clés ?
  (grands nombres premiers, tests de primalité, résistance aux attaques, ...)
- Sécurité de RSA ?
  (quelles attaques, factorisation des entiers ...)
- Effectivité de RSA ?
  (calcul avec de grands entiers, calcul rapide de $x^n \quad [N]$ ...)

... et la suite de MT10

- Cours, TD et TP complémentaires !
- Travail personnel important (2 sens !)
- Plan approximatif du cours :
  1. Entiers - Structures - Morphismes ...
  2. Groupes
  3. Anneaux et corps
  4. Corps finis
  5. Cryptographie (avec W. S. : AES, courbes elliptiques, ...)
- Evaluation : médian, TP, final.

$$\boxed{\text{score final} = 0.3TP + 0.35M + 0.35F}$$

avec :

- M = note à l'examen médian
- F = note à l'examen final
- T = moyenne des notes de TP (en (groupes de) binômes)