Le commerce électronique en danger ?

G. Guillerm[*], J. Marchand[†], F. Morain[‡], P. Zimmermann[§]

26 août 1999

Les codes secrets ont toujours fasciné le grand public. Décrypter les dépêches ennemies a très souvent joué un rôle dans l'Histoire, dans la diplomatie, pendant les conflits. De nos jours, les systèmes de chiffrement sont employés dans les transactions numériques (commerce électronique) et plus près de nous dans nos portefeuilles (cartes à puce pour le paiement, pour la santé). Le record décrit ici montre que ces systèmes sont en danger.

Casser les codes de protection se ramène très fréquemment au problème suivant : étant donné un nombre, comment le brise-t-on (on dit encore qu'on le factorise) en ses parties élémentaires, les nombres premiers ? Par exemple, on peut écrire 6 sous la forme 2×3 et on ne peut aller plus loin, 2 et 3 sont premiers. Les nombres considérés dans le cadre des systèmes de chiffrement modernes (comme le célèbre RSA, du nom de ses inventeurs Rivest, Shamir et Adleman en 1976) sont bien sûr plus grands que 6, ils s'écrivent avec 100 à 200 chiffres, et pour les implantations les plus courantes, avec 155 chiffres ou encore 512 chiffres binaires (bits). Factoriser ces nombres est un problème ardu sur lequel les mathématiciens se cassent les dents depuis des millénaires. À l'époque où RSA a été inventé, factoriser des nombres de 512 bits relevait de la Science-Fiction. Vingt-cinq années ont passé et cette barrière psychologique vient d'être franchie, l'inconcevable est devenu réalité.

Les meilleures méthodes de factorisation connues à ce jour sont très sophistiquées et difficiles à mettre en œuvre. Les temps de calcul mis en jeu sont colossaux : plusieurs dizaines d'années de temps d'ordinateur... Pour les atteindre en quelques mois de temps humain, on répartit les tâches entre plusieurs centaines de machines, généralement des stations de travail ou des ordinateurs personnels (PC).

Pour être à même de mesurer les progrès établis dans le domaine de la factorisation, la firme américaine RSA, Inc. (du nom du cryptosystème) parraine un concours de factorisation de nombres. Des listes sont disponibles sur leur site Web[1] et des prix sont accordés chaque trimestre. Dans cette liste, on trouve ainsi le nombre appelé RSA155, qui matérialise cette barrière psychologique des 512 bits.

S'attaquer à RSA155 nécessite d'utiliser la meilleure méthode de factorisation connue, qu'on appelle le crible algébrique, inventé par J. Pollard en 1988. Cet algorithme présente

[*]École polytechnique, SITX
[†]École polytechnique, UMS MEDICIS
[‡]DGA/École polytechnique, UMR LIX, **morain@lix.polytechnique.fr**
[§]INRIA Lorraine, UMR LORIA, **Paul.Zimmermann@loria.fr**
[1]`http ://www.rsa.com/`

deux phases. Dans la première, la plus gourmande en temps, des milliards de données sont calculées pour préparer la deuxième phase qui aboutira à la découverte des facteurs du nombre. Les meilleurs spécialistes du domaine, A. K. Lenstra et P. L. Montgomery se sont attelés à l'écriture des programmes nécessaires, et les calculs ont été répartis entre 300 ordinateurs de 11 équipes triées sur le volet, représentant 6 pays (Pays-Bas, USA, Canada, Australie, Royaume Uni, France), sous la coordination de H. te Riele au CWI (Amsterdam). On y trouve ainsi trois laboratoires français : deux à l'École polytechnique (Laboratoire d'Informatique – LIX[2], F. Morain, avec l'aide de G. Guillerm du SITX ; l'UMS Medicis[3], J. Marchand), et le Centre Charles Hermite[4] (P. Zimmermann à Nancy). Nos trois équipes ont fourni un tiers de l'effort nécesaire. Ce n'est pas une surprise, car ces trois laboratoires disposent de fortes compétences reconnues internationalement en calcul formel, théorie des nombres et cryptographie, alliées à de puissants moyens de calcul.

Donnons quelques détails sur le record. Les calculs ont commencé le 27 avril 1999 et la première phase s'est terminée le 13 juillet. La seconde s'est achevée le 22 août, par la découverte des deux facteurs premiers du nombre :

```
RSA155 =
1094173864157052742180970732204035761200373294544920599091384213147634\
9984288934784717997257891267332497625752899781833797076537244027146743\
531593354333897
=
102639592829741105772054196573991675900716567808038066803341933521790711307779
*
106603488380168454820927220360012878679207958575989291522270608237193062808643
```

La première phase a nécessité environ 8000 années de MIPS[5], la seconde 224 heures sur le Cray-C916 du SARA à Amsterdam.

Un pas important a été franchi. Utiliser RSA (et plus généralement tout système dont la sécurité repose sur la factorisation des entiers) avec des clefs de 512 bits assure une protection qui n'est plus inviolable mais limitée dans le temps. Il n'a fallu que quelques mois et finalement assez peu de ressources pour casser cette clef. 300 PC sont faciles à rassembler (1 PC coutant 5 kF, l'attaque revient tout compris à environ 2 MF), même si la phase finale des calculs demande à l'heure actuelle un super-ordinateur et une grande mémoire centrale.

Dans le combat éternel entre l'épée et le bouclier, celle-là vient de reprendre un peu d'avance sur celui-ci. Aujourd'hui, les systèmes utilisant des clefs de 768 ou 1024 bits restent hors d'atteinte. Pour combien de temps ?

[2]http ://www.lix.polytechnique.fr

[3]http ://www.medicis.polytechnique.fr

[4]http ://cch.loria.fr

[5]Le MIPS est l'acronyme de "Million Instructions Per Second", correspondant à la puissance d'un VAX 780, exécutant 1 million d'opérations à la seconde. Même si une telle machine n'existe plus, la dénomination a perduré. On peut traduire en disant que 8000 années de MIPS correspondent à 32 années d'un processeur à 250 MHz.