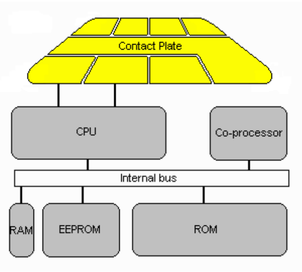
Factorisation et Cartes Bancaires

> *Tout nombre entier se décompose de manière unique, à l'ordre des facteurs près, en un produit de nombres premiers.*
>
> Les Éléments, Euclide, Livre VII, -300 avjc.

Cette affirmation vieille de plus de 23 siècles soulève deux interrogations. Comment décider si un nombre est premier ? Comment trouver un facteur d'un nombre composé ? Les deux questions sont de complexité très différentes. D'un côté, l'algorithme de Rabin-Miller permet de tester rapidement la primalité d'un nombre de plusieurs centaines de chiffres décimaux. D'un autre côté, les logiciens n'ont pas de certitude sur la difficulté intrinsèque du problème de la factorisation des entiers. Le temps de calcul du meilleur algorithme (NFS) pour factoriser un entier n est de l'ordre de :

$$e^{1.902\sqrt[3]{\log n(\log\log n)^2}}$$



La carte à puce est une petite merveille technologique. Elle intègre des ressources matérielles et logicielles : microprocesseurs, port de communication, mémoires et système de fichiers. Un ordinateur capable de traiter des applications d'origines diverses. Le code PIN est la partie visible des mesures de sécurité qui peuvent être implantées sur une carte à puce : DES, RSA, ECDSA, AES. Dans le contexte des transactions bancaires, un serveur authentifie une carte au moyen d'un système de chiffrement à clef publique : RSA.

En 1976, Rivest, Shamir et Adleman ont proposé un cryptosystème à clé publique (RSA) qui s'appuie sur l'apparente difficulté du problème de factorisation. Il s'agit d'une utilisation habile d'un petit théorème d'Euler à propos du groupe des inversibles modulo n, le module RSA. L'élégance et la simplicité du protocole expliquent la popularité du système RSA même si sa fiabilité n'est pas prouvée. La sérénité du système est assurée par RSA-LABS qui organise un concours de factorisation de grand nombre, dans le tableau ci-contre RSA-xyz désigne un module de xyz chiffres.

Number	Prize
RSA-129	factored !
RSA-130	factored !
RSA-140	factored !
RSA-155	factored !
RSA-174	$10,000
RSA-193	$20,000
RSA-212	$30,000
RSA-232	$50,000
RSA-270	$75,000
RSA-369	$100,000
RSA-463	$150,000
RSA-617	$200,000

Dans le contexte des transactions bancaires, un serveur authentifie une carte par le système de chiffrement RSA. Tout le secret repose donc sur l'entier de 768 bits (232 chiffres décimaux) ci-contre en bleu à droite. La factorisation constitue une attaque majeure susceptible de créer de sérieuses difficultés au GIE «cartes bancaires». D'après Lenstra et Verheul, un million de pentium 450Mhz seraient nécessaires pour factoriser un entier de cette taille en moins d'une année, soit un budget de 10 millions de dollars. D'après Morain, les progrés algorithmiques et technologiques permettront de factoriser les entiers de 1024 bits dans une dizaine d'années.

1550880802
7837692984239
2150075130787847
1020215206711102793
1119903875394553459999
757630467173585609159
753897974089381733440
4347047809863900699066
790967289330814050449
35969514508676239949
3440750589270015
7399623745293
63251827

Authentification

Le module RSA n du GIE est égal au produit de deux nombres premiers secrets p et q. Un entier s tel que $3s$ soit congru à 1 modulo $(p-1)(q-1)$ est calculé. Ce dernier reste secret et sera utilisé pour «marquer» toute carte émise par le GIE. Lors de la fabrication d'une carte, l'identité du titulaire est formatée en un entier z suivant un codage bien établi. Le résultat v du calcul z^s modulo n est chargé dans la puce, c'est la «valeur de signature» du titulaire. Lors d'une transaction, le serveur authentifie la carte en vérifiant que v^3 est bien égal à z modulo n (Th. Euler). Pour fabriquer une fausse carte, il est indispensable de connaître s ce qui revient à factoriser n.

1952 Apparition des cartes de crédits : Dinner's Club, American Express.
1971 Appatition des cartes à piste magnétique.
1972 R. Moreno fonde INNOVATRON.
1974 IBM et la NSA proposent le DES : Data Encryption Standard, système à clé secrète. Diffie et Hellman inventent le concept de cryptographie à clef publique (asymétrique).
1975 R. Moreno : brevet de la carte à mémoire. Morrison et Brillart factorisent F_7, un entier 39 chiffres, 128 bits.
1976 Les chercheurs Rivest, Shamir et Adleman publient le cryptosystème RSA.
1977 M. Ugon (BULL) dépose le brevet de la carte à microprocesseur.
1978 BULL produit des cartes à mémoire de 1Ko.
1980 Production des cartes BULL CP8, micro–processeur MOTOROLA. Onze banques forment le GIE «cartes bancaires».
1984 Le GIE adopte la carte CP8. Factorisation du nombre de Fermat F_9, par le crible quadratique de Pomerance.
1987 Norme iso7816 carte à puce : caractéristiques physiques, rôle et positions des contacts, protocole d'échange et jeu de commande.
1992 La puce équipe toutes les cartes bancaires.
1994 Factorisation de RSA-129 par la méthode du crible quadratique, 1600 machines.
1996 Factorisation de RSA-130 par la méthode du crible algébrique de Pollard.
1998 Affaire Humpich. Modification de la carte bancaire.
1999 NFS factorise le challenge rsa-155 (512 bits) en 8 mois, 292 machines.
2001 Publication sur internet d'un programme pour fabriquer la «Yescard».

Groupe de Recherche en Informatique et Mathématiques
Université de Toulon et du Var
http://www.univ-tln.fr/~grim/