5 Une nouvelle ère avec l'asymétrie : le système RSA

OBJECTIF Étudier le principe du système RSA. On admettra le petit théorème de Fermat.

Point info

De la symétrie …

Pendant des siècles, et encore pendant la majeure partie du XX^{e} siècle, les procédés de chiffrement étaient symétriques : l'émetteur et le récepteur d'un message s'entendaient sur une information partagée, la clé secrète qui permettait de chiffrer mais aussi d'en déduire le déchiffrement. Les chiffrements affines, chiffrements de Vigenère ou de Hill étudiés précédemment sont de ce type.

Les mécanismes de chiffrement symétrique sont mathématiquement sûrs et avantageux dans les cas où le nombre d'interlocuteurs potentiels est réduit. Le problème de distribution des clés se posent cependant.

« Dans les années 1970, les banques employaient des coursiers qui sillonnaient le monde munis de mallettes cadenassées contenant les précieux codes pour les messages de la semaine suivante. Les soucis logistiques et le coût d'une telle distribution devenaient problématiques. »[1].

Un autre problème consiste en le nombre de clés nécessaires pour un nombre important d'interlocuteurs.

…à l'asymétrie

Une nouvelle ère s'ouvre à partir de 1976 avec l'invention, par les Américains Diffi et Hellman (voir TP 6 page 100), de la cryptographie asymétrique : une clé publique sert à chiffrer les messages tandis que la clé de déchiffrement reste secrète et connue uniquement du destinataire des messages.

L'idée générale consiste à utiliser une « opération » pour le chiffrement qu'on ne puisse pas réaliser facilement en sens inverse. L'exemple le plus connu est celui du système RSA, mis au point en 1977 par trois mathématiciens, Ronald Rivest, Adi Shamir et Leonard Adleman (photo ci-dessus). L'opération choisie est une simple multiplication, l'opération inverse consistant en la factorisation d'un entier pouvant être particulièrement difficile… (voir point info page 99).

Aujourd'hui ce système reste l'un des plus utilisés au monde, aussi bien pour la sécurité des cartes bancaires que pour la confidentialité des échanges sur Internet…

1. La recherche, n° 46 HS

A Le principe sur un exemple

Nous prendrons dans cet exemple $p = 5$, $q = 19$ et $c = 61$.

1. Vérifier que c est premier avec $n = (p - 1)(q - 1)$.

2. Prenons $a = 3$.
Calculer le reste b dans la division de a^c par pq.

3. a. Résoudre l'équation $61x - ny = 1$.

b. En déduire la valeur de d tel que $61\,d \equiv 1\ (n)$ et $0 \leqslant d < n$.

c. Calculer le reste dans la division de b^d par pq.
Retrouve-t-on bien a ?

Dans la pratique le produit pq est public ainsi que l'entier c mais les entiers p et q sont gardés secrets.
Si l'on ne peut pas factoriser pq, on ne peut pas calculer $n = (p - 1)(q - 1)$ et il est impossible de déchiffrer !
La sécurité du RSA repose donc sur la difficulté à factoriser l'entier pq (voir point info page 99)

Le principe du RSA

1. La clé publique consiste en la donnée du produit pq de deux nombres premiers et d'un exposant c entier naturel premier avec $n = (p - 1)(q - 1)$.

2. Le chiffrement : un entier a est chiffré en un entier b tel que $b \equiv a^c\ (\text{mod } pq)$, avec $0 \leqslant b < pq$.

3. Le déchiffrement : l'entier b est déchiffré en $a \equiv b^d\ (\text{mod } pq)$ où d est l'entier tel que $cd \equiv 1\ (\text{mod } n)$ avec $0 \leqslant d < n$.

B Une justification

On considère deux entiers p et q premiers, un entier naturel c premier avec $n = (p-1)(q-1)$.
Pour a entier naturel, on pose $b \equiv a^c \pmod{pq}$.

1. a. Montrer que l'équation $cx - ny = 1$ aux inconnues entières x et y admet des solutions et que si $(x_0 ; y_0)$ est l'une d'elles, les autres sont $(x_0 + kn ; y_0 + kc)$, $k \in \mathbb{Z}$.

b. En déduire qu'il existe un unique entier d tel que $0 \leqslant d < n$ et $cd \equiv 1 \pmod{n}$.

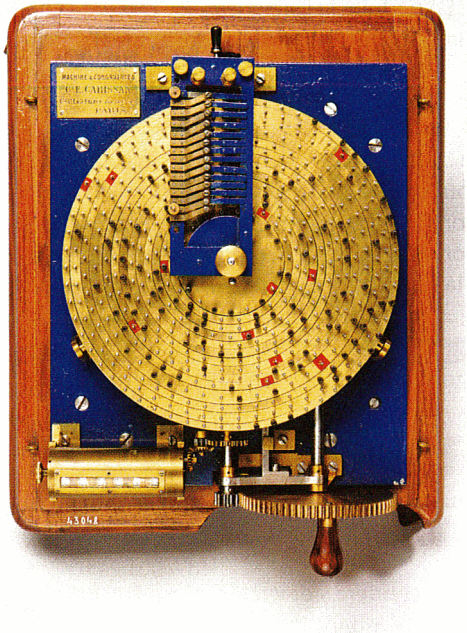
2. On suppose que a n'est divisible ni par p ni par q et on admet que $a^{p-1} \equiv 1\ (p)$ et $a^{q-1} \equiv 1\ (q)$ (Petit théorème de Fermat : voir exercice 103 page 111).
Montrer que $a^{(p-1)(q-1)} \equiv 1 \pmod{p}$ et $a^{(p-1)(q-1)} \equiv 1 \pmod{q}$. En déduire que $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

b. En déduire que pour tout entier $k = 1 + mn$, $a^k \equiv a \pmod{pq}$.

3. Des questions 1.b. et 2.b. déduire que $a \equiv b^d \pmod{pq}$.

Point info

Des tests de primalité (voir chapitre 2) permettent de savoir qu'un entier n'est pas premier, mais de là à savoir le factoriser …



La machine de Carissan

Pierre et Eugène Carissan s'intéressent à la fabrication d'une telle machine. En 1919 Eugène achève la construction d'une machine dite **machine à congruences** (photo ci-contre). Cette machine permet de factoriser des nombres de treize chiffres en moins de 18 minutes, alors que les calculs à la main demanderaient plusieurs jours de travail. Elle permettra la résolution de plusieurs problèmes de théorie des nombres. Un exemplaire de la machine se trouve au Conservatoire National des Arts et Métiers à Paris et fonctionne toujours !

La sécurité du RSA aujourd'hui …

Si la recherche pour trouver des algorithmes de factorisation est très active, les meilleures méthodes actuelles de factorisations sont très sophistiquées, difficiles à mettre en œuvre et surtout très coûteuses en temps !
En 1978, on estimait par exemple le temps nécessaire pour factoriser un nombre de 100 chiffres à 74 années ! Autant dire que lors de l'invention du système de cryptographie RSA (en 1976), utiliser des nombres entre 100 et 200 chiffres paraissait une garantie suffisante de sécurité…
Aujourd'hui, la factorisation des nombres à 100 chiffres est facilement accomplie avec le matériel et les algorithmes dont on dispose mais les nombres de plus de 200 chiffres résistent encore en général.
Dans le cadre du système RSA, la dernière factorisation concerne le nombre RSA768 bits de 232 chiffres, réalisée en 2010, sous la forme d'un produit de 2 nombres premiers ayant chacun 116 chiffres.
RSA768 = 33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489 ×
367460436667995904282446337996279526322791581643430876426760322838157396665112792333734171433968102700927987363089 17
Le RSA792 utilise un produit pq qui s'écrit avec 239 chiffres et le RSA1024 un produit de 309 chiffres !
Le « nombre monstre » RSA2048 a encore de beaux jours devant lui, enfin peut-être…

La menace de l'ordinateur quantique

Les systèmes asymétriques actuels sont potentiellement sensibles à une future attaque à l'aide d'un ordinateur quantique lorsque celui-ci sera opérationnel. Des systèmes « post quantiques » sont actuellement mis au point et la recherche est particulièrement active dans ce domaine.