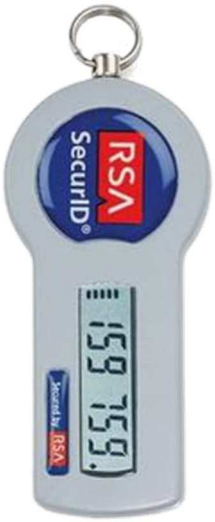
PRINCIPE DU SYSTEME RSA

Niveau : Terminale, Mathématiques Expertes.
Lien avec le programme : nombres premiers, petit théorème de Fermat. Déterminer un inverse de a modulo n lorsque a et n n'ont pas de diviseur en commun autre que 1. Étude du système cryptographique RSA.
Lien avec Les maths au quotidien : Codage.



Le système RSA est un système assez récent (1977) de cryptographie dissymétrique à clé publique, très fiable. La puissance du système RSA repose sur l'idée que l'on peut forcer n'importe quel système de cryptographie, mais on peut rendre le temps de « cassage » suffisamment long pour obtenir une sécurité suffisante. Il est fondé sur le fait qu'on ne connaît pas d'algorithme, exécutable en un temps raisonnablement court, capable de décomposer de très grands nombres (ayant plus de cent chiffres) en produit de facteurs premiers. Ainsi si quelqu'un calcule le produit de deux nombres premiers de plus de 100 chiffres chacun, personne ne peut décomposer le nombre obtenu rapidement sauf celui qui a fait le produit.

I. Propriété fondamentale :

PROPRIETE : soient deux nombres premiers p et q, et n leur produit.
Soient e et d deux entiers naturels tels que $ed \equiv 1 \pmod{(p-1)(q-1)}$.
Pour tous M et C entiers, si $C \equiv M^e \pmod{n}$ alors $C^d \equiv M \pmod{n}$, ou encore $M^{ed} \equiv M \pmod{n}$.

Démonstration : $C^d \equiv (M^e)^d \equiv M^{ed} \pmod{n}$.
Or $ed \equiv 1((p-1)(q-1))$: il existe un entier k tel que $ed = 1 + k(p-1)(q-1)$.
Donc, si M n'est pas multiple de p : $M^{ed} \equiv M^{1+k(p-1)(q-1)} \equiv M\,(M^{(p-1)})^{k(q-1)} \equiv M \pmod{p}$ car d'après le petit théorème de Fermat $M^{(p-1)} \equiv 1 \pmod{p}$. On obtient $\boldsymbol{M^{ed} \equiv M \pmod{p}}$.
De même, si M n'est pas multiple de q : $\boldsymbol{M^{ed} \equiv M \pmod{q}}$.
Les deux congruences mises en évidence en « gras » sont en fait réalisées pour n'importe quel entier M, car si M est un multiple de p, M et toutes ses puissances non nulles sont congrues à 0 modulo p. De même pour q.
L'entier $M^{ed} - M$ est donc un multiple de p et de q, qui sont premiers distincts : $M^{ed} - M = pa = qb$, avec a et b entiers. p divise qb et p ne divise pas q donc p divise b par le lemme d'Euclide : $b = pc$ avec c entier.
Donc $M^{ed} - M = qb = qpc$ avec c entier. Par conséquent $M^{ed} - M$ est divisible par pq.

II. Utilisation

Tous les éléments du message à crypter sont transformés en nombres (par exemple en utilisant le code ASCII) et le message est transformé en blocs de nombres (inférieurs à n).
M est un bloc numérique à coder. p et q sont deux nombres premiers distincts, très grands et $n = pq$.

On choisit e entier qui n'a pas de diviseur commun avec $(p-1)(q-1)$ autre que 1. On verra dans le chapitre « PGCD… » que dans ce cas, il existe toujours un entier d tel que $ed \equiv 1 \pmod{(p-1)(q-1)}$.

Le couple $(n ; e)$ est **la clé publique du codage**, elle est connue de tous et répertoriée dans des annuaires.
d est un entier naturel tel que $ed = k(p-1)(q-1) + 1$ (k entier naturel). **d est la clé privée du codage**.
Pour coder M, on calcule $C \equiv M^e\ (n)$. C est le bloc codé. Pour décoder, on calcule $C^d \equiv M\ (n)$. M est le bloc initial.

Exemple : les lettres de l'alphabet sont chiffrées par :

A	B	C	D	E	...	X	Y	Z
01	02	03	04	05		24	25	26

Le président Emmanuel Macron souhaite envoyer un message codé à Joe Baden avec le système RSA : Joe, …
Pour cela, il va utiliser la clé publique de Joe.
Joe choisit deux nombres premiers très grands : pour la simplicité des calculs et puisque seul le principe nous intéresse, il prend ici $p = 3$ et $q = 13$, petits. Alors n = …….. = …….. . Il calcule $(p-1)(q-1)$ = ……

Joe veut choisir $e = 29$ (qui n'a pas de diviseur commun avec 24 autre que 1). (39 ; 29) sera la **clé publique**.

EXERCICE 1 : à l'aide d'un outil numérique, fournir **une clé privée** à Joe.

Emmanuel, comme tous ceux qui veulent envoyer un message à Joe, a pour clé publique (39 ; 29).
Emmanuel code son message avec la clé publique : Joe est chiffré en clair par 10 15 05.

EXERCICE 2 : compléter par des entiers naturels inférieurs à 39 : $10^{29} \equiv$ …… (39), $15^{29} \equiv$ …… (39), $5^{29} \equiv$ ……. (39).

Emmanuel envoie le message suivant : 04 06 05, ….
Pour le décrypter, Joe utilise sa clé privée : ….., et les congruences.
La fin du message est : 04 01 10 06 18 05 12 05 28 13 01 11 08 28.

EXERCICE 3 : aider Joe à décrypter la fin du message d'Emmanuel : …….

Le système RSA assure la confidentialité et l'intégrité de la correspondance, il permet de plus d'en établir l'authenticité. En effet, Emmanuel peut aussi utiliser un système RSA et cela va permettre d'authentifier son message. Emmanuel va ajouter à son message sa signature, codée avec sa propre clé privée. Joe, à la fin du décodage du message avec sa clé privée, utilisera la clé publique d'Emmanuel pour décoder la signature d'Emmanuel. Le message sera authentifié car seul Emmanuel est capable de coder sa propre signature :

Signature d' Emmanuel	→	Emmanuel crypte sa signature avec sa clé privée	→	Emmanuel crypte le message avec la clé publique de Joe	→	Joe décrypte le message avec sa clé privée	→	Joe décrypte la signature avec la clé publique d'Emmanuel

RSA Data Security est devenu le standard de référence des échanges sécurisés à travers le monde. RSA est utilisé par des logiciels comme Netscape Navigator ou encore par Microsoft Windows et des centaines d'autres produits informatiques. RSA fait partie des standards proposés pour internet et le World Wide Web, mais aussi pour les réseaux de commerce électronique et les réseaux financiers.

Authentification de carte bancaire lors d'un paiement

Sur une carte bancaire sont inscrites certaines informations (nom du propriétaire, numéro de carte, date de validité...), et une valeur de signature VS. La VS est calculée lors de la fabrication de la CB.
D'autre part, on associe à l'ensemble des informations écrites sur la carte, que l'on notera I, un nombre Y qui représente ces informations. On dit que l'on utilise une fonction de hachage et que le nombre Y est le haché des informations I. On écrit $Y = h(I)$, où h est la fonction de hachage. La VS est alors calculée confidentiellement en utilisant la clé secrète du groupement des cartes bancaires, le GIE Carte Bancaire : $VS = f(Y)$.
Lorsque la carte est introduite dans le terminal de paiement, celui-ci lit les informations portées par la carte, et la valeur de signature VS. Il calcule alors $Y = h(I)$, et aussi un nombre Y' à partir de la VS grâce à la clé publique du GIE : $Y' = g(VS)$.
Or $g(VS) = g(f(Y))$. La carte est valide si et seulement si $Y = Y'$.
Ces fonctions à clé secrète et à clé publique sont basées sur le RSA.
Le nombre n est en France un nombre connu entre 768 et 1 024 bits.
L'exposant e qui compose la clé publique vaut 3.

Identifier un ordinateur distant

Un certificat d'authentification permet une protection sur le courrier électronique, garantit votre identité auprès d'un ordi-nateur distant, garantit l'identité d'un ordinateur distant, etc. Il s'agit ci-contre d'un certificat sur serveur sécurisé où apparaît le nombre n de la clé publique écrit en système hexadécimal (base 16) ainsi que l'identificateur de la clé de l'autorité qui a établi le certificat (en dessous).