DOCUMENT DE SYNTHÈSE SUR LE SYSTÈME RSA

Introduction :

Le système RSA a été inventé en 1978 par trois mathématiciens, Ronald Rivest, Adi Shamir et Leonard Adleman.
Actuellement, il est le plus sûr car il est basé sur notre incapacité à factoriser un très grand nombre. Par ailleurs, il donne une solution aux anciens systèmes de cryptographie tels que Jules César ou Enigma : la clé reste secrète. Rappelons nous bien que c'est la transmission de la clé qui permettait aux « ennemis » de décrypter les messages.

1. Le petit théorème de Fermat et des conséquences bien pratiques :

Petit théorème de Fermat : Si p est un nombre premier et si a est un nombre entier, on a :

$$a^p \equiv a \; modulo \; p$$

Quelle est l'idée derrière ce théorème ? Voilà. Tu choisis un nombre a quelconque. Ensuite, tu calcules a^p. Pour finir, tu divises le résultat obtenu (a^p) par p. Et qu'obtiens-tu alors ? Le reste de la division euclidienne que tu viens de poser est le nombre a de départ, un peu comme si tu n'avais rien fait !

Ce théorème admet deux conséquences bien pratiques, qui ne seront pas démontrées. Il faut juste que tu en comprennes le principe. Prêt(e) ? Allons-y !

Conséquence 1 : Soit p et q deux nombres premiers et a un nombre entier. Si un nombre entier k vérifie :

$$k \equiv 1 \; modulo \; (p-1) \times (q-1)$$

alors $a^k \equiv a \; modulo \; p \times q$.

Toujours vivant(e) ? Bon, alors il ne faut pas te laisser impressionner par toutes ces écritures. Passons à la conséquence suivante, celle qui sert vraiment en pratique et que nous allons expliquer en détail.

Conséquence 2 : Soit p et q deux nombres premiers. Soit e un nombre premier avec $(p-1) \times (q-1)$. Alors, on peut trouver un et un seul nombre entier d, inférieur à $(p-1) \times (q-1)$ tel que :

$$e \times d \equiv 1 \; modulo \; (p-1) \times (q-1)$$

Donc, d'après la conséquence 1, si a est un nombre entier : $a^{e \times d} \equiv a \; modulo \; p \times q$.

Pas de panique, dans la pratique, ce n'est pas infaisable ! L'idée est un peu la même que pour le petit théorème de Fermat.

Commençons par rappeler qu'un nombre entier premier avec $(p-1) \times (q-1)$ est un nombre qui n'a qu'un seul diviseur commun avec $(p-1) \times (q-1)$, à savoir 1. Cela veut dire que le PGCD de e et de $(p-1) \times (q-1)$ sera 1.

Pour vérifier cela, tu pourras utiliser la fonction *gcd* de MuPad.

À titre d'exemple, prenons $p = 3$ et $q = 11$. Ainsi, $n = p \times q = 33$ et $(p-1) \times (q-1) = 2 \times 10 = 20$.

Vérifie alors que $PGCD(20; 3) = 1$. Nous prendrons alors $e = 3$.

Maintenant, supposons que nous ayons trouvé le nombre d dont parle la conséquence 2 (je te le donne par exemple : ici $d = 7$). Que se passe-t-il alors ?

Choisis alors un nombre a (prends $a = 9$). Calcule a^e (donc 9^3). Calcule le reste de la division euclidienne du résultat par $n = p \times q$ (ici le reste de la division euclidienne de 9^3 par 33). Appelons b ce reste (ici, $b = 3$).

Calcule alors b^d (ici 3^7), puis prends le reste de la division euclidienne de b^d par $n = p \times q$ (ici, le reste de la division de 3^7 par 33).

Quel est alors le reste que tu trouves ? Bonne surprise, c'est le nombre a de départ (ici 9) !

Dernière remarque avant de reprendre l'exemple : nous avons calculé a^e, puis ce nombre là élevé à la puissance d, c'est à dire finalement :

$$(a^e)^d = a^{e \times d}$$

Exemple numérique : $p = 3$; $q = 11$; $n = p \times q = 3 \times 11 = 33$; $(p-1) \times (q-1) = 2 \times 10 = 20$.

Nous avons vu que nous pouvons prendre $e = 3$. Le nombre d qui correspond est alors 7 (vérifie que 3×7 est congru à 1 modulo 20).

Choisissons par exemple $a = 7$.

Calcule $a^e = \ldots$

Calcule le résultat modulo n : ... $\qquad\qquad$ $b = \ldots$

Calcule alors $b^d = \ldots$

Calcule ce dernier résultat modulo n : $b^d\,(a^e)^d \equiv \ldots\ldots$ *modulo* $p \times q$

2. La cryptographie et le système RSA :

Quel rapport y a-t-il entre tout ceci et la cryptographie. Voyons cela tout de suite !

Admettons que tu veux transmettre le message composé de la lettre I à ton correspondant. Dans l'ordre de l'alphabet, la lettre I correspond au nombre 9. Tu codes donc la lettre I par le nombre 9.

Ensuite, tu calcule 9^3 *modulo* 33, ce qui te donne 3. 3 correspond à la lettre C dans l'ordre alphabétique. Tu envoies donc la lettre codée C à ton correspondant. Tu viens de coder ton message !

Celui-ci reçoit ton message : C. Il transforme cette lettre en le nombre 3, calcule 3^7 *modulo* 33 et tombe sur le nombre 9, qu'il transforme en la lettre I. Il vient de décoder ton message !

Bien sûr, si ton message comporte plusieurs lettres, tu codes chaque lettre de cette manière.

Les annuaires :

Si tu veux recevoir des messages codés, tu vas publier tes ≪coordonnées cryptographiques ≫ dans un annuaire qui ressemble à ceci :

NOM :	**PROCÉDÉ**	**CLÉ**	
Docteur X	RSA	$n = 33$	$e = 3$

Si ton correspondant veut te transmettre un message, il regarde dans l'annuaire, trouve ton nom et ta clé de, puis effectue les calculs décrits précédemment, en codant chaque lettre, que tu vas ensuite décoder.

Mais pourquoi ce procédé est-il sûr ? As-tu remarqué que, dans l'annuaire, tu n'as publié que le nombre e et le produit des deux nombres premiers que tu as choisis. À aucun moment, tu n'as divulgué le nombre d qui permet de décoder ton message.
Cela veut dire que ton correspondant, celui qui t'a envoyé le message codé ne connaît pas le nombre d qui permet de décoder le message, ce qui signifie que même lui ne peut pas décoder son propre message codé !

Comment est-ce possible ? Imagine que ton correpondant veuille décoder le message. Il lui font donc calculer le nombre d. Mais non avons vu dans la conséquence 2 que pour le calculer, il y a un moment où il faut faire une congruence modulo $(p-1)\times(q-1)$, c'est à dire qu'il faut connaître les deux nombres premiers choisi au départ. Et ceux-là, il ne les connaît pas, il ne connait que leur produit n que tu as publié !

Bien sûr, avec $n = 33$, il est très facile de retrouver que les nombres premiers sont 3 et 11 $33 = 3 \times 11$. Mais maintenant, essaie de retrouver les deux nombres premiers dont le produit est :

$$122454544546711314571941571$$

Difficile hein ? Voilà, c'est le principe. À l'heure actuelle, avec toutes nos connaissances mathématiques et les plus gros ordinateurs, si les nombres premiers choisis sont assez grands, on ne sait pas factoriser leur produit.

Le système RSA a donc résolu le problème de la transmission de la clé dont nous avons parlé : elle reste confidentielle et le système est sûr !

3. À toi de jouer :

3.1 Le même message pour tous :

Avec ton binôme, en utilisant MuPad, code puis décode le message suivant :

Lettre	G	A	R	E	A	U	G	O	R	I	L	L	E
a													

Cryptage : $c =$ reste la division euclidienne de a^3 par 33.

c													
Lettre													

Déryptage : $m =$ reste la division euclidienne de c^7 par 33.

m													
Lettre													

3.2 Un message original :

Écris un nouveau message, code le et donne le codé à un autre groupe, qui devra le décoder (pas la peine maintenant de repasser par le codage de la lettre intermédiaire, donne directement les nombres !).