2ndeMPS SEANCE CRYPTOGRAPHIE : LE CRYPTAGE PAR CODE RSA

Ou Codage à Clé asymétrique.

Recherches :

**- Informations générales :**

1. Que signifie le code RSA ?
2. Qui sont les inventeurs ? Quels sont leurs profils professionnels  (étude/ profession)
3. En quelle année a –t-il été inventé ?
4. A quoi sert-il principalement ?

* **La part de mathématiques dans le code RSA :**

1) Qu’est-ce qu’un nombre premier ?

2) Qu’est-ce que le crible d’Ératosthène ? A quoi sert-il ?

Servez-vous de la méthode pour donner les nombres premiers compris entre 1 et 100.

4) Les nombres suivants sont-ils premiers ?

Si non donner un produit de nombres premiers égal à ce nombre. (On dit qu’on décompose le nombre en produit de facteurs premier. )

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 159 | 223 | 231 | 551 | 127 | 543 | 1001 | 1777 |
|  |  |  |  |  |  |  |  |

1. Décomposer en produit de facteurs premiers :
2. Qu’est-ce que la division euclidienne ?

Que représente R et Q  dans A = B x Q + R avec R < B

1. Modulo et reste de la division euclidienne :

Compléter ce tableau :

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17 | modulo | 5 | Est égale à | 2 | car | 17 = 3 x 5 + 2 | On note | 17 ≡ 2 [5] |
| 29 |  | 4 |  |  |  |  |  |  |
| 30 |  | 3 |  |  |  |  |  |  |
| 54 |  | 5 |  |  |  |  |  |  |
| 100 |  | 7 |  |  |  |  |  |  |
| 45 |  | 2 |  |  |  |  |  |  |
| 986 |  | 2 |  |  |  |  |  |  |
| 1003 |  | 9 |  |  |  |  |  |  |

Construire un tableau dans Excel :

Dans la première colonne les nombres entiers, dans la seconde colonne l ‘entier modulo et dans la troisième le résultat.

Qu’elles sont les fonctions prédéfinies utilisées ?

**-Petite explication :**

La personne 1 qui veut recevoir un message “privé”, génère quatre nombres de la façon suivante :

- deux nombres p et q premiers et distincts

- deux nombres c et d tels que cd ≡ 1 [(p − 1)(q − 1)]

- On caclule alors le nombre n = p q.

Le couple (n, c) constitue la clé publique. La personne 1 la diffuse publiquement a toute personne qui souhaite communiquer avec lui.

Une fois son message numérisé, sous la forme d’un entier M, elle calcule et envoie :

E = Mc [n]

La personne 1 reçoit E etpeut alors le déchiffré en calculant grâce à sa clé

privée: M’ = Ed [n]

La personne 1 a alors le message M’ = Ed = Mcd ≡ M [n].  
  
La sécurité de ce système repose sur le fait que connaissant la clé publique (n, c), il est très difficile de déterminer le nombre d, nécessaire au décryptage.

Il faudrait par exemple factoriser n pour trouver p et q, ce qui est encore impossible à réaliser de nos jours lorsque p et q sont de très grands nombres, de l’ordre de 100 chiffres (on ne sait pas factoriser aujourd’hui des entiers de plus de 120 chiffres… et encore cela prend du temps.).

En résumé, tout le monde connaît la clé publique, donc tout le monde peut chiffrer un message, mais seuls ceux connaissant la clé privée peuvent déchiffrer.