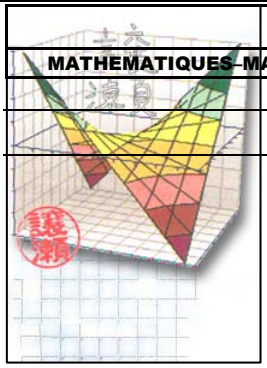


CHIFFREMENT PAR LE SYSTÈME RSA

1. Préambule

Cette méthode a été inventée en 1978 par trois mathématiciens, Rivet, Shamir et Adleman. Ce qui fait son originalité c'est que l'algorithme de chiffrement et la clé sont connus de tous, et cependant une seule personne peut déchiffrer le message. Elle repose sur les résultats d'arithmétique suivants que vous admettrez :

R1

p et q sont deux nombres premiers distincts et n = pq.
e est un entier compris entre 2 et (p – 1)(q – 1) – 1 et premier avec (p – 1)(q – 1)

Alors, il existe un entier d et un seul, 1 < d < (p – 1)(q – 1) tel que ed ≡ 1 [modulo (p – 1)(q – 1)].

R2

Avec les notations précédentes, si $b \equiv a^d$ [modulo pq], alors $a \equiv b^e$ [modulo pq].

Exemple : On choisit p = 3, q = 11, pq = 33, (p – 1)(q – 1) = 20, puis e = 7.
e est premier avec (p – 1)(q – 1) = 20.
• Alors, il existe un nombre d et un seul, entre 1 et 19, tel que ed ≡ 1 [modulo 20].
Ce nombre d est 3, en effet 3 x 7 = 21 et 21 ≡ 1 [mod 20].

Par exemple, il est vrai que $8 \equiv 2^3$ [modulo 33] ; il en résulte que $8^7 \equiv 2$ [modulo 33].
(En effet, 8^7 = 2 097 152 = 33 X 63 550 + 2.)

2. Fonctionnement

ALICE, c'est le nom d'usage, choisit deux nombres premiers p et q, calcule leur produit n = pq, choisit aussi un entier e premier avec (p – 1)(q – 1), et rend publique dans un annuaire l'information (RSA, n, e).
ALICE a choisi p = 13, q = 17, **mais elle ne livre que leur produit 221**.
Remarque : Alice est la seule à connaître p, q et d.

ANNUAIRE			
NOM	**PROCEDE**	**CLE**	**Valeur de e**
Alice	RSA	n = 221	e = 5
José	RSA	n = 19 050 724 489	e = 37
Marie	RSA	n = 437	e = 7

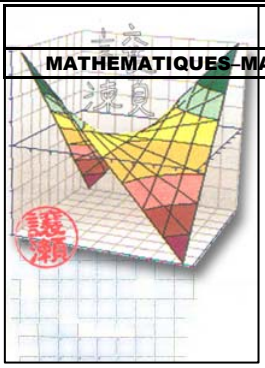
L'information signifie que l'algorithme de chiffrement est :
1/ On élève à la puissance 5 le nombre **b** à chiffrer,
2/ On divise le résultat par n,
3/ On garde le reste **a**.
• Celui ou celle qui veut chiffrer un message destiné à Alice peut donc déterminer le nombre **a** tel que :

$$a \equiv b^e \text{ [modulo n = pq]}$$

et envoyer ce nombre à Alice. **La personne qui chiffre le message pour Alice ne peut pas le déchiffrer**.

• Alice déchiffrera ce nombre **a** en calculant :

$$b \equiv a^d \text{ [modulo n = pq]}.$$



a) Comment BOB envoie-t-il un message à ALICE ?

BOB veut envoyer à ALICE le message "NON".
1] Il l'écrit d'abord sous la forme "14-15-14", en utilisant la position de la lettre de l'alphabet (N est la 14^e lettre, ...).
Le message est donc constitué de trois sous messages de deux chiffres "14-15-14".

2] Il élève alors chaque sous message à la puissance e = 5 et il en cherche le reste dans la division par n = 221, en utilisant les congruences (utilisez le programme sur la calculatrice).

Vérifiez que $145 \equiv 131$ [mod 221] et que $155 \equiv 19$ [mod 221].
BOB obtient "131-19-131", message qu'il transmet à ALICE.

b) Comment ALICE déchiffre-t-elle le message de BOB ?

ALICE, qui est la seule à connaître p et q, doit calculer d'abord le nombre d.
$0 < d < 192$, tel que $ed \equiv 1$ [mod $(p-1)(q-1)$] ; c'est-à-dire que $5d \equiv 1$ [mod 192]. (Voir le résultat **R1**)

Cela signifie que 5d - 1 est un multiple de 192, c'est-à-dire que 5d- 1 = 192q, ou encore

5d+ 192(-q) = - 1.

ALICE doit donc résoudre cette équation de la forme ax + by = 1, mais en choisissant d, entre 2 et 192.
1] Vérifiez que d = 77.

2] ALICE élève alors chaque sous message reçu à la puissance d = 77, elle en prend le reste modulo 221, et reconstitue ainsi le message de BOB, grâce à **[R2]**.

3] Retrouvez ainsi le message "NON" transmis par BOB.

c) Le message "131-19-131" ne peut-il être déchiffré que par ALICE ?

Tout le monde peut connaître n = 221 et e = 5 , en consultant l'annuaire public, donc tout le monde peut connaître p et q, puisque n = pq, et donc d, puisque $ed \equiv 1$ [modulo n], et donc tout le monde, en théorie, peut décrypter.

Avec 221, c'est possible, évidemment. Mais si l'on choisit des nombres premiers p et q de façon que leur produit s'écrive **avec 200 chiffres**, par exemple, l'ordinateur le plus puissant ne peut pas décomposer n en produit pq en un **temps raisonnable**.
Le record actuel de factorisation est de 120 chiffres, encore faut-il, pour obtenir ce résultat, faire travailler un ordinateur puissant pendant un mois et utiliser un algorithme très complexe.
Ainsi RSA est-il considéré comme un « système de sécurité absolue » dès qu'on utilise des grands nombres premiers.

d) Comment ALICE peut-elle envoyer un message à BOB ?

Par exemple encore, le message "NON".
1] Elle l'écrit comme plus haut, "14-15-14" puis elle élève chaque sous message à la puissance d = 77 et elle en prend le reste modulo 221.

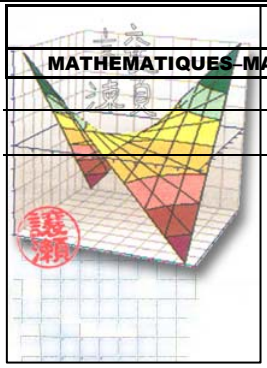
2] Complétez les congruences suivantes en mettant à droite un nombre compris entre 0 et 220
$(14)^{77} \equiv$ ….. [mod 221], $(15)^{77} \equiv$ ….. [mod 221] et écrivez le chiffrement obtenu par ALICE.

3] BOB recevant le message d'ALICE, élève chaque sous message à la puissance e = 5 et prend le reste modulo 221, et retrouve ainsi le message "NON".

e) Mais quelle différence y a-t-il avec le paragraphe b) ?

Au paragraphe b), tout le monde pouvait écrire à ALICE de façon chiffrée mais seule ALICE pouvait déchiffrer le message.
Dans ce paragraphe, tout le monde peut déchiffrer le message d'ALICE mais seule ALICE peut le chiffrer.

En résumé : La **clé publique d'Alice** (RSA, n, **e**) permet aux expéditeurs de chiffrer les messages destinés à Alice. Cette clé permet également de **déchiffrer les messages provenant d'Alice** (seule Alice peut chiffrer les messages qu'elle envoie). Ceci permet aux destinataires d'être sûr que c'est bien Alice qui a envoyé le message.
Alice, grâce à sa **clé privée** (RSA, n, **d**) **est la seule** à pouvoir chiffrer un message qu'elle envoie ou à pouvoir déchiffrer un message qu'elle reçoit.



CHIFFREMENT PAR LE SYSTÈME RSA

ANNUAIRE			
NOM	**PROCEDE**	**CLE**	**Valeur de e**
Alice	RSA	n = 221	e = 5
José	RSA	n = 19 050 724 489	e = 37
Marie	RSA	n = 437	e = 7

PARTIE A

A l'aide des exemples du TD "Le Système RSA", répondez aux questions supplémentaires suivantes :

1/ Alice souhaite écrire "**MOI AIMER TOI**" à Bob. Quel message crypté (chiffré) recevra Bob ?

2/ Bob lui envoie en retour le message crypté suivant :
"13-19-42 131-19-131 152-207-21-15"

Alice vous demande de déchiffrer pour elle le message de Bob.

PARTIE B

Marie souhaite s'inscrire dans l'annuaire et elle communique les informations n = 437 et e = 7.
Remarque importante *: Ici nous prenons* ***de petites valeurs de p et de q*** *pour que les calculs soient réalisables sans devoir utiliser un ordinateur. Pour de grandes valeurs de p et de q le principe reste le même et il est extrêmement difficile de déterminer p et q à partir du produit n = pq. RSA est considéré comme un système de sécurité absolue dès qu'on utilise de grands nombres premiers. Autrement dit vous ne pouvez pas déterminer p et q (sans l'aide de Marie !).*

Vous êtes son ami(e) et elle vous demande de l'aider à vérifier si son choix de n et de e est valide.
Pour cela elle vous communique les valeurs de p et de q (**valeurs confidentielles qu'elle devrait garder pour elle seule ...** mais vous êtes son ami(e)).

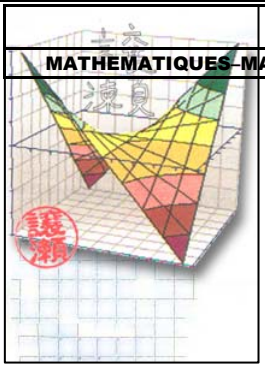
p = 19 et q = 23.

1/ Le choix de e est-il correct ? Justifiez
2/ Déterminez la valeur de **d** que Marie doit utiliser (détaillez les calculs).

3/ Marie souhaite écrire "**MOI AIMER TOI**" à Bob. Quel message crypté (chiffré) recevra Bob ?

4/ Bob lui envoie en retour le message crypté suivant :
"1-430-4-2-339 256-339-124-124-339 124-241-4 "

Marie vous demande de déchiffrer pour elle le message de Bob.



ANNEXE : Programme SUPERMODULO
Ce programme vous fera gagner du temps pour le calcul des congruences.

Nom du programme : SUPERMODULO
Description : Ce programme permet de calculer le reste de la division euclidienne de a^p par q

On peut écrire également : $a^p \equiv r\,[\text{modulo } q]$ avec $0 \leq r < q$

Remarques :
Ce programme est **indispensable**. Vérifiez qu'il est très difficile (pour les calculatrices CASIO) de trouver le résultat suivant par un autre moyen : $131^{77} \equiv 14\,[\text{mod } 221]$

Le tableur Excel ne pourra pas vous aider non plus, la fonction **mod(131^77 ;221)** retourne une erreur (dépassement de capacité).
Vous comprenez mieux le nom de ce programme …

PROGRAMME

```
"A^P MOD Q, A=":?→A
"P=":?→P
"Q=":?→Q
1→B
1→R
While R<P+1
AxB→B
B – Qx Int(B/Q)→B
R+1→R
WhileEnd
"A^P CONGRU  " :B
```