EPREUVE PRATIQUE DE MATHEMATIQUES

CHIFFREMENT PAR LE SYSTEME RSA (spécialité)

1 – ENONCE

ALICE souhaite envoyer un message chiffré à Bob. Elle consulte l'annuaire et trouve les informations : n = 437 et e = 7. Le message à envoyer est "BONJOUR".

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

1/ Après avoir consulté les informations en annexe, déterminer le message chiffré qu'Alice doit envoyer à Bob (vous devrez utiliser le programme **supermod** pour calculer les congruences).

Appeler l'examinateur pour vérifier le chiffrement ou en cas de problème de programmation.

2/ Bob reçoit donc le message d'Alice.
Deux jours plus tard, Alice lui envoie le nouveau message chiffré suivant :

"1 – 124 – 241 – 33 – 75"

Informations confidentielles données par Bob lui-même : Bob a choisi p = 19 et q = 23

a) Vérifier que l'équation diophantienne de Bob est la suivante (consulter l'annexe) :

$$7d - 396k = 1$$

où d est la valeur lui permettant de déchiffrer ses messages.

b) Montrer que la valeur de d acceptable est d = 283

c) Après avoir consulté les informations en annexe, déchiffrer le message d'Alice.

Appeler l'examinateur pour vérifier le déchiffrement.

2- PRODUCTION DEMANDEE

- Saisie et utilisation du programme fourni
- Chiffrement et déchiffrement d'un message

ANNEXE : 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 :

Résultat 1

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 $ed \equiv 1$ [modulo (p – 1)(q – 1)].

Résultat 2

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 $ed \equiv 1$ [modulo 20].
Ce nombre d est 3, en effet 3 x 7 = 21 et $21 \equiv 1$ [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
Marie	RSA	n = 19 050 724 489	e = 37
Bob	RSA	n = 437	e = 7

L'information signifie que l'algorithme de chiffrement est :
1/ On élève le nombre **b** à chiffrer à la puissance e,
2/ On divise le résultat par n,
3/ On garde le reste **a**. **a** est le nombre correspondant au chiffrement de **b**.

• Celui ou celle qui veut chiffrer un message destiné à Alice peut donc déterminer le nombre **a** tel que :

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

et envoyer ce nombre à Alice.
Personne ne peut déchiffrer le message, même pas celle qui a effectué le chiffrement.

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

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

Remarque : Le couple (n,e) d'Alice peut être assimilé à un numéro de téléphone nécessaire pour lui laisser un message sur son répondeur téléphonique.
Alice peut relever les messages de son répondeur en utilisant le couple (n,d), qui peut être assimilé à un code nécessaire pour pouvoir écouter les messages à distance. Alice est la seule à connaître la valeur de d.

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 et O la 15^{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 **1**)
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 diophantienne de la forme ax + by = 1, mais en choisissant d, entre 2 et 192.
1] Alice trouve : d = 77. En effet 5(77) – 2(192) = 1

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 **[**Résultat **2]**. Par exemple, 131^77 ≡ 14 [mod 221]. Finalement elle trouve **"14 – 15 – 14"** c'est-à-dire "NON".

Remarque : 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.

ANNEXE 2 : Programme MMOD

Ce programme permet d'effectuer les calculs de congruences.

Nom du programme : **MMOD**

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).

PROGRAMME (CASIO)

```
"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
```

PROGRAMME (TI 89, 92 TI Voyage 200)

```
mmod()
Prgm
Disp "A^P modulo Q"
Input "Valeur de A : ",a
Input "Valeur de P : ",p
Input "Valeur de Q : ",q
1⟼ b
1⟼ r
While r<p+1
a*b⟼ b
b – q*int(b/q) ⟼ b
r+1 ⟼ r
EndWhile
Disp "A^P est congru à : ",b
EndPrgm
```