Protocole RSA pour envoyer un message crypté :
Une personne « Emetteur » veut transmettre une information secrète à une autre personne « Destinataire ».
(*a*) Création des clefs.
Destinataire construit un quadruplet de nombres (p, q, e, d) tel que p et q sont deux nombres premiers ; on pose $n = p\,q$, e est un entier premier avec le produit $(p-1)(q-1)$; d est un entier positif tel que $e\,d - 1$ est un multiple de $(p-1)(q-1)$, c'est-à-dire tel que $e\,d \equiv 1\ [(p-1)(q-1)]$.
On sait alors d'après l'énoncé du théorème du RSA que, si A est un entier quelconque, alors $A^{e\,d} = A \pmod{n}$, et c'est cette identité qui va tout faire fonctionner.
Le nombre d constitue la clef secrète de Destinataire.
(*b*) Destinataire rend publics n et e, qui constituent la clé publique. Il ne publie surtout pas p, q ou d. Le nombre d constitue la clé secrète du destinataire.
(*c*) Émetteur, qui veut transmettre une information secrète à Destinataire, transforme son information en un nombre entier A, inférieur à n (ou en plusieurs si nécessaire), en utilisant des conventions connues de tous (provenant, par exemple, des codes numériques des caractères typographiques, ou en prenant $a = 01$, $b = 02$, etc.).
(*d*) Emetteur calcule, $B \equiv A^{e}\ [n]$, envoie B à Destinataire par un canal qui n'*a* pas besoin d'être protégé (par exemple, le courrier électronique).
(*e*) Destinataire, pour décoder B, calcule $B^{d} \pmod{n}$, ce qui lui redonne A, car, d'après le théorème du RSA, on a $B^{d} \equiv A^{e\,d} \equiv A \pmod{n}$.

Théorème du RSA :
Soient p et q deux nombres premiers distincts.
On pose $n = p\,q$ et $m = (p-1)(q-1)$.
Si e est un nombre premier avec m alors :
(1) il existe un entier $d > 0$ tel que $e\,d \equiv 1\ [m]$
(2) pour cet entier d et pour tout entier a, on a : $a^{e\,d} \equiv a\ [n]$

Partie théorique :
1. Montrer que si la condition « e et m premiers entre eux » n'est pas remplie, il n'est pas possible de trouver un tel entier d.

2. *a*. Montrer que si p et q sont deux nombres premiers, alors $\begin{cases} a \equiv p & [p] \\ a \equiv p & [q] \end{cases} \Leftrightarrow a \equiv p \quad [p\,q]$.

Cette implication est-elle encore vraie lorsque p ou q n'est pas premier ?

b. Montrer que dans le théorème du RSA, il existe un entier r tel que : $e\,d = (p-1)\,r + 1$
En déduire que $a^{e\,d} \equiv a \quad [p]$
c. Montrer de même que $a^{e\,d} \equiv a \quad [q]$ conclure.

Partie Pratique :
Le couple (n ; e) est la clef publique et le nombre d est la clef caché
On intercepte avec la clef publique (8633 ; 1225) le message : 736 ; 8523 ; 916 ; 6630 ; 279.
Comme le nombre 8633 n'est pas très gros, on peut facilement, à l'aide d'un programme, trouver la clef secrète et décoder le message.
Que dit ce message ?

CORRECTION

Partie théorique :

1. Soit $m = 6$ et $e = 4$, s'il existe un entier $d > 0$ tel que $e\,d \equiv 1\ [m]$ alors $4\,d \equiv 1\ [6]$ donc il existe un entier relatif q tel que $4\,d = 6\,q + 1$
$4\,d$ est un nombre pair, $6\,q + 1$ est un nombre impair donc $4\,d \neq 6\,q + 1$. La propriété (1) n'est pas valide si e et m ne sont pas premiers entre eux.

2. *a*. Si $a \equiv b\ [p]$ et $a \equiv b\ [q]$ alors p divise $a - b$ et q divise $a - b$, p et q sont deux nombres premiers distincts donc sont premiers entre eux donc d'après le théorème de Gauss, $p\,q$ divise $a - b$ donc $a \equiv b\ [p\,q]$.

Réciproquement : si $a \equiv b\ [p\,q]$, il existe un entier relatif n tel que $a - b = n\,p\,q$.
$n\,q$ est un entier relatif donc p divise $a - b$ donc $a \equiv b\ [p]$
$n\,p$ est un entier relatif donc q divise $a - b$ donc $a \equiv b\ [q]$
donc si $a \equiv b\ [p\,q]$ alors $a \equiv b\ [p]$ et $a \equiv b\ [q]$ d'où l'équivalence : $\begin{cases} a \equiv b & [p] \\ a \equiv b & [q] \end{cases} \Leftrightarrow a \equiv b \quad [p\,q]$

Soit $p = 3$ et $q = 6$:
Soit $a = 6$, $b = 12$ alors $a - b = 6$ donc $a \equiv b\ [3]$ et $a \equiv b\ [6]$
$a - b = 6$ et $p\,q = 18$ donc $p\,q > a - b$ donc $p\,q$ ne divise $a - b$, on n'a pas $a \equiv b\ [p\,q]$.
La propriété ne s'applique pas si p ou q n'est pas premier.

b. Dans le théorème du RSA, $e\,d \equiv 1\,[m]$ donc il existe un entier k tel que $e\,d = (p-1)(q-1)k+1$
soit $r = (q-1)k$ alors r est un entier et $e\,d = (p-1)r+1$

$a^{e\,d} = a^{(p-1)r+1} = a^{(p-1)r} \times a$.
si a n'est pas divisible par p, p est un nombre premier donc, d'après le petit théorème de Fermat : $a^{p-1} \equiv 1\,[p]$
donc $a^{(p-1)r} \equiv 1\,[p]$
donc $a^{(p-1)r} \times a \equiv 1\,[p]$ soit $a^{e\,d} \equiv a\,[p]$

Si a est divisible par p, alors $a \equiv 0\,[p]$ donc $a^{e\,d} \equiv 0\,[p]$ donc $a^{e\,d} \equiv a\,[p]$
dans tous les cas $a^{e\,d} \equiv a\,[p]$.

c. Dans le théorème du RSA, $e\,d \equiv 1\,[m]$ donc il existe un entier k tel que $e\,d = (p-1)(q-1)k+1$
soit $r' = (p-1)k$ alors r' est un entier et $e\,d = (q-1)r'+1$

$a^{e\,d} = a^{(q-1)r'+1} = a^{(q-1)r'} \times a$.
si a n'est pas divisible par q, q est un nombre premier donc, d'après le petit théorème de Fermat : $a^{q-1} \equiv 1\,[q]$
donc $a^{(q-1)r'} \equiv 1\,[q]$
donc $a^{(q-1)r'} \times a \equiv 1\,[q]$ soit $a^{e\,d} \equiv a\,[q]$

Si a est divisible par q, alors $a \equiv 0\,[q]$ donc $a^{e\,d} \equiv 0\,[q]$ donc $a^{e\,d} \equiv a\,[q]$
dans tous les cas $a^{e\,d} \equiv a\,[q]$.

$a^{e\,d} \equiv a\,[p]$ et $a^{e\,d} \equiv a\,[q]$
p et q sont deux nombres premiers distincts donc d'après la propriété démontrée à la question 2. *a*., $a^{e\,d} \equiv a\,[p\,q]$ soit $a^{e\,d} \equiv a\,[n]$

Partie Pratique :
$n = 8633$ et $e = 1225$, déterminons s'il existe p et q deux nombres premiers tels que $n = p\,q$ et $m = (p-1)(q-1)$.
$8633 = 89 \times 97$,
89 et 97 sont deux nombres premiers donc $m = 88 \times 96 = 2^8 \times 3 \times 11 = 8448$
$e = 5^2 \times 7^2$ donc e est un nombre premier avec m.
$e\,d \equiv 1\,[m] \Leftrightarrow 1225 \times d \equiv 1\,[8448]$ donc $d = 3193$.