Devoir en temps libre, à rendre le vendredi 30 avril 2010.

Cryptographie : le système RSA

1. Lire la description du système de cryptographie RSA qui est donnée sur le site internet de Didier Müller à l'adresse :

   http ://www.apprendre-en-ligne.net/crypto/rsa/index.html

   On peut la trouver aussi à partir de la table des matières : chapitre XV paragraphe 5. (On ne demande pas de faire l'exercice ni le travail de programmation)

   Dans la suite de ce devoir, nous allons démontrer que l'on peut bien déchiffrer le message de Bob grâce à la méthode donnée. On appliquera aussi la méthode de chiffrage et de déchiffrage en prend comme exemple $p = 7$ et $q = 23$.

2. Donner dans ce cas la valeur du produit $p\,q$. Vérifier que 5 convient pour le nombre e.
   Ces deux nombres sont rendus publics.

Chiffrement

On ne s'intéresse pas à l'étape de "découpage en blocs de même longueur" décrite sur le site internet. On chiffrera les messages en remplaçant chaque lettre par son rang dans l'alphabet (A =1, B=2, etc.) sans faire de regroupement. On aura donc à chiffrer uniquement des nombres de 1 à 26.

3. En détaillant les calculs, chiffre les 5 premières lettres de ton prénom en utilisant les clés publiques de la question précédente.
4. De même, chiffre la lettre Z. Que remarques-tu ?

Déchiffrement

5. (a) Justifier l'existence d'entiers x et y tels que $e\,x + (p-1)(q-1)\ y = 1$.
   (b) Soit $(x_0; y_0)$ une solution particulière de l'équation précédente.
   Démontrer qu'alors il existe $k \in \mathbb{Z}$ tel que $x = x_0 + k\,(p-1)(q-1)$.
   (c) En déduire qu'il existe un unique entier d tel que

   $$1 < d < (p-1)(q-1) \quad \text{et} \quad e\,d \equiv 1 \text{ (modulo } (p-1)(q-1)).$$

   (d) Déterminer cet entier d pour notre exemple.
6. Soit a un un nombre entier premier avec p et q.
   (a) Justifier qu'il existe un entier k tel que $a^{(p-1)(q-1)} = 1 + kp$.
   (b) Justifier de même qu'il existe un entier k' tel que $a^{(p-1)(q-1)} = 1 + k'q$.
   (c) Démontrer que k est un multiple de q et en déduire, avec les hypothèses ci-dessus que $a^{(p-1)(q-1)} \equiv 1\ (pq)$.
   (d) Démontrer que, pour tout entier a, si $k \equiv 1\ ((p-1)(q-1))$ alors $a^k \equiv a\ (p\,q)$.
7. Déduire de tout ce qui précède que, quels que soient les entiers naturels b et c, si $c \equiv b^e\ (p\,q)$, alors $c^d \equiv b\ (p\,q)$.
8. Vérifier que l'on retrouve bien le mot initial en effectuant le déchiffrement du mot codé trouvé à la question 3 (détaille les calculs).

Éléments de correction

1.

2. $pq = 7 \times 23 = 161$
   $(p-1)(q-1) = 6 \times 22 = 132$ et 5 est bien premier avec 132. C'est d'ailleur le plus petit entier naturel possible.

3.

lettre	b	b^5	$b^5 \mod (161)$
a	1	1	1
b	2	32	32
c	3	243	82
d	4	1 024	58
e	5	3 125	66
f	6	7 776	48
g	7	16 807	63
h	8	32 768	85
i	9	59 049	123
j	10	100 000	19
k	11	161 051	51
l	12	248 832	87
m	13	371 293	27
n	14	537 824	84
o	15	759 375	99
p	16	1 048 576	144
q	17	1 419 857	159
r	18	1 889 568	72
s	19	2 476 099	80
t	20	3 200 000	125
u	21	4 084 101	14
v	22	5 153 632	22
w	23	6 436 343	46
x	24	7 962 624	47
y	25	9 765 625	9
z	26	11 881 376	59

4. On remarque que la lettre Z est chiffrée par un nombre supérieur à 26.
   Effectivement, le résultat du codage peut être un nombre entre 0 et $(pq-1)$ soit ici entre 0 et 160. On peut donc chiffrer un alphabet composé de 161 signes.

5. (a) Comme e et $(p-1)(q-1)$ sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers x et y tels que $e\,x + (p-1)(q-1)\,y = 1$.

   (b) $e\,x+(p-1)(q-1)\,y = e\,x_0+(p-1)(q-1)\,y_0$ donc $e\,(x-x_0) = (p-1)(q-1)\,(y_0-y)$
   Donc $(p-1)(q-1)$ divise $e\,(x-x_0)$ et comme e est premier avec $(p-1)(q-1)$, d'après le théorème de Gauss, $(p-1)(q-1)$ divise $(x-x_0)$.
   Donc il existe $k \in \mathbb{Z}$ tel que $x - x_0 = k\,(p-1)(q-1)$ soit $x = x_0+k\,(p-1)(q-1)$.

   (c) On démontre la réciproque. S'il existe $k \in \mathbb{Z}$ tel que $x - x_0 = k\,(p-1)(q-1)$, alors $ex = ex_0 + ek(p-1)(q-1)$. Or $ex_0 = 1-(p-1)(q-1)y_0$ donc $ex = 1-(p-1)(q-1)y_0 + ek(p-1)(q-1)$ donc $ex \equiv 1 \pmod{(p-1)(q-1)}$.
   Parmis tous les nombres de la forme $x = x_0+k\,(p-1)(q-1)$ avec $k \in \mathbb{Z}$, il en existe un unique compris entre 1 et $(p-1)(q-1)$. (x est non nul).

   Pour l'expliciter, on peut faire la division euclidienne de $(p-1)(q-1)-x_0$ par $(p-1)(q-1)$
   Afin de simplifier les notations, on pose $a = (p-1)(q-1)$. Il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que $a - x_0 = q \times a + r$ avec $0 < r < a$. ($r \neq 0$ car ...) On a donc $x_0 + q \times a = a - r$. Comme $r > 0$, $a - r < a$ et comme $r < a$, $0 < a - r$.

   (d) Grâce à l'algorithme d'Euclide (ou en voyant une solution "évidente"), on trouve une solution particulière à l'équation $5\,x + 132\,y = 1$. Par exemple $x_0 = -79$ et $y = 3$.
   On trouve alors la valeur $d = -79 + 132 = 53$ comprise entre 1 et 132. On vérifie que $5 \times 53 \equiv 265 \equiv 1 \pmod{132}$.

6. (a) p est un nombre premier et a un nombre premier avec p donc d'après le petit théorème de Fermat, $a^{p-1} \equiv 1 \pmod{p}$ donc $a^{(p-1)(q-1)} \equiv 1^{(q-1)} \equiv 1 \pmod{p}$ donc il existe $k \in \mathbb{Z}$ tel que $a^{(p-1)(q-1)} = 1 + kp$.

(b) De même en remplaçant p par q, on obtient qu'il existe $k' \in \mathbb{Z}$ tel que $a^{(p-1)(q-1)} = 1 + k'q$.

(c) $1 + kp = 1 + k'q$ donc $kp = k'q$. Comme p et q sont premiers entre eux (deux nombres premiers distincts), et que q divise kp, alors d'après le théorème de Gauss, q divise k. Donc il existe $k'' \in \mathbb{Z}$ tel que $k = qk''$ et donc $a^{(p-1)(q-1)} = 1 + qpk''$ ce qui prouve que $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

(d) Soit k un entier tel que $k \equiv 1\ ((p-1)(q-1))$ donc il existe $l \in \mathbb{Z}$ tel que $k = 1+l(p-1)(q-1)$.
1er cas : a est premier avec p et q. D'après les questions précédentes, $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$ donc $a^k \equiv a^{1+l(p-1)(q-1)} \equiv a \times \left(a^{(p-1)(q-1)}\right)^l \equiv a \times 1^l \equiv a \pmod{pq}$.
2ème cas : si p divise a. Alors $a \equiv 0\ (p)$ donc $a^k \equiv 0 \equiv a\ (p)$. De même si q divise a , sinon, d'après le petit théorème de Fermat, $a^{(q-1)} \equiv 1 \quad (q)$ donc $a^{(q-1)(p-1)} \equiv 1^{p-1} \equiv 1 \quad (q)$ donc $a^{(q-1)(p-1)l} \equiv 1 \quad (q)$ donc $a^{(q-1)(p-1)l-1} \equiv a \quad (q)$ donc $a^k \equiv a\ (q)$.
Comme q et p sont premiers entre eux et que p divise $a^k - a$ et que q divise $a^k - a$, alors $p\,q$ divise $a^k - a$ donc $a^k \equiv a\ (pq)$.

7. Supposons que $c \equiv b^e\ (p\,q)$. Alors $c^d \equiv b^{e\,d}\ (p\,q)$. Or, $e\,d \equiv 1 \pmod{(p-1)(q-1)}$. Donc d'après la question précédente, $b^{e\,d} \equiv b\ (p\,q)$ donc $c^d \equiv b\ (p\,q)$.

8. Pour les calculs pratiques, on doit calculer c^{53} pour des valeurs de c pouvant aller de 0 à 161. Si on essaye de calculer directement c^{53}, on dépasse très rapidement la précision des calculatrices ou des tableurs. On doit donc décomposer 53 et faire les calculs comme on le ferait "à la main". Exemple :
$53 = 5 \times 5 \times 2 + 3$ donc $32^{53} = \left((32^5)^5\right)^2 \times 32^3$
$32^5 \equiv 33\ 554\ 432 \equiv 100 \quad (161)$ puis on recommence :
$32^{25} \equiv 100^5 \equiv 39 \quad (161)$
$32^{50} \equiv 39^2 \equiv 1524 \equiv 72 \quad (161)$
$32^3 \equiv 32\ 768 \equiv 85 \quad (161)$
$32^{53} = 32^{50} \times 32^3 \equiv 72 \times 85 \equiv 6\ 120 \equiv 2 \quad (161)$

lettre	c	c^5	c^5 mod (161)	c^{25} mod (161)	c^{50} mod (161)	c^3 mod (161)	c^{53} mod (161)
a	1	1	1	1	1	1	1
b	32	33 554 432	100	39	72	85	2
c	82	3 707 398 432	73	12	144	104	3
d	58	656 356 768	18	72	32	141	4
e	66	1 252 332 576	33	157	16	111	5
f	48	254 803 968	55	146	64	146	6
g	63	992 436 543	21	14	35	14	7
h	85	4 437 053 125	29	71	50	71	8
i	123	28 153 056 843	16	144	128	29	9
j	19	2 476 099	80	5	25	97	10
k	51	345 025 251	158	79	123	148	11
l	87	4 984 209 207	26	59	100	13	12
m	27	14 348 907	104	41	71	41	13
n	84	4 182 119 424	7	63	105	63	14
o	99	9 509 900 499	155	113	50	113	15
p	144	61 917 364 224	2	32	58	78	16
q	159	101 621 504 799	129	61	18	153	17
r	72	1 934 917 632	151	142	39	50	18
s	80	3 276 800 000	5	66	9	20	19
t	125	30 517 578 125	111	34	29	34	20
u	14	537 824	84	7	49	7	21
v	22	5 153 632	22	22	1	22	22
w	46	205 962 976	23	46	23	92	23
x	47	229 345 007	24	47	116	139	24
y	9	59 049	123	16	95	85	25
z	59	714 924 299	96	150	121	104	26