le cnam

Algèbre de Boole, probabilités et arithmétique

Cours 8 Code de Rivest, Shamir et Adleman

- Quelques mots de cryptographie

Le mot "cryptographie" a une double racine grecque : *kruptôs* : caché, dissimulé et *graphein* : écrire, dessiner. C'est l'art de transformer un texte afin qu'il ne soit pas compris par quelqu'un qui réussit à l'intercepter.

Chiffre de Cesar (Caius Julius Caesar, 100 avant J.C. − 44 avant J.C.)
Il s'agit d'un décalage constant des lettres de l'alphabet. On code d'abord les 26 lettres de l'alphabet avec des nombres de 0 à 25 avec la convention $a = 0$:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Le chiffre de Cesar consiste à ajouter +3 à chaque nombre, en calculant *modulo* 26 ; Ainsi a $\longmapsto$ d, b $\longmapsto$ e, *etc*. Enfin y $\longmapsto$ b, z $\longmapsto$ c. Par exemple la célèbre phrase *alea jacta est* devient "dohd mdfwd hvw", qui n'est pas facile à comprendre ! Si on connaît la clef de codage, c'est à dire la valeur $c = +3$ du décalage, il suffit de la retrancher à chaque lettre du texte crypté pour retrouver le message initial.
Le chiffre de Cesar est un chiffrage faible. En effet, la clef de cryptage, le nombre c du décalage, parcourt l'ensemble $\{0, 1, ..., 25\}$. Il suffit de tester les 26 clefs possibles devant un message crypté pour récupérer à coup sûr le message initial. La clef de cryptage appartient à un ensemble trop petit.

Analyse statistique d'une langue
La réponse naturelle à la critique précédente est de choisir une permutation quelconque σ de l'ensemble $\{0, 1, ..., 25\}$ dans lui-même. Le nombre de clefs est alors le nombre de permutations d'un ensemble de 26 éléments, soit $26! \simeq 4,03 \times 10^{26} \simeq 2^{88}$. Mais une attaque statistique rend alors ce choix essentiellement obsolète. En effet, dans une langue vivante, certaines lettres apparaissent statistiquement plus de d'autres. Pour la langue Française par exemple, la lettre "e" est présente pour 14,8% des lettres d'un texte, la lettre "s" pour 7,9%, le "a" dans 7,6% des cas, *etc*. Il est alors possible de proche en proche de mettre en évidence les éléments caractéristiques de la permutation σ et finir par déchiffrer le message.

Chiffre de Vigenère (Blaise de Vigenère, 1523-1596)
C'est un chiffre de Cesar dynamique où la clef change à chaque lettre du texte à crypter. On découpe le texte en blocs et on le code avec une clef de cryptage qui est lui même un mot ou un texte court. Dans l'exemple proposé par "Wikipedia", la phrase *j'adore ecouter la radio* est codée avec la clef "musique", qui est un mot de sept lettres. Cette clef secrète "musique" est

partagée uniquement par l'émetteur et le récepteur du message. On met ensuite en regard le texte en clair décomposé en blocs de sept lettres et la clef de cryptage, dupliquée autant que nécessaire :

j a d o r e e c o u t e r l a r a d i o
m u s i q u e m u s i q u e m u s i q u

Au dessous de chaque lettre du texte initial, on lit alors la clef de cryptage d'un code de Cesar. Ainsi pour les trois premières colonnes, avec la convention a $\longrightarrow$ 0, b $\longrightarrow$ 1, *etc.*, on a
j & m $\longmapsto$ 9 + 12 = 21 $\longmapsto$ v, a & u $\longmapsto$ 0 + 20 = 20 $\longmapsto$ u et d & s $\longmapsto$ 3 + 18 = 21 $\longmapsto$ v.
Le texte crypté devient "vuvwhyioimbulpmlslyi" si on enlève toute trace de ponctuation et d'*a priori* sur la longueur de la clef. En particulier, la double lettre "e" est codée avec des symboles différents.

Cryptage symétrique à clef secrète

Le chiffre de Vigenère a bien sûr été amélioré. Mais il contient toutes les caractéristiques du cryptage symétrique à clef secrète, qui doit être partagée à la fois par celui qui émet le message et celui qui reçoit le message crypté. Une clef privée est d'autant plus efficace qu'elle est longue et sert peu souvent.

Le principe de Kerckhoffs (Auguste Kerckhoffs, 1835 - 1903) énonce que la sécurité ne doit pas reposer sur l'algorithme de cryptage mais sur le secret de la clef privée. Le système de chiffrement peut rester public et il importe d'avoir un espace de clef de cryptage suffisamment grand pour résister à une attaque systématique.

Le "Data Encryption Standard" est un cryptage symétrique à clef secrète qui fait suite à un appel d'offres du National Bureau of Standards américain en 1973. Il a été opérationnel de 1977 à 2001. Mais la clef de cryptage comporte au maximum "seulement" 56 bits utiles (et 8 bits de parité, voir le cours "Codes et Automates"), soit $2^{56} \simeq 7,2 \times 10^{16}$ choix possibles. Une attaque systématique de ce code "DES" est aujourd'hui considérée comme facile.

L'"Advanced Encryption Standard" est une extension du protocole DES afin de permettre des clefs secrètes de plus grande longueur qui comportent classiquement 128, 192 ou 256 bits. La question est ensuite de pouvoir s'échanger des clefs secrètes. On utilise pour cela un système de cryptographie asymétrique, plus lent à mettre en œuvre, mais qui résout cette difficulté.

Cryptage asymétrique

L'autorité qui lit les message émet une "clef publique" à toute entité qui souhaite crypter une information relativement courte comme une clef de cryptage symétrique ou des coordonnées bancaires typiquement. Le message crypté est envoyé à cette autorité qui, seule dispose d'une "clef privée" qui lui permet de décoder le message.

Dans les applicatons informatiques, un "certificat" est émis, qui contient divers paramètres comme l'identification de l'interlocuteur et un processur de signature électronique. Le protocole de communication 'Transport Security Layers" contient une suite de de "Secure Sockets Layers". Dans un chiffrement asymétrique, la clef publique est sur le site web et la clef privée est cachée dans les profondeurs internes du serveur informatique. On passe alors du protocope "http" au protocole "http avec ssl", soit "https". Deux algorithmes mathématiques de cryptage peuvent être utilisés : le codage "RSA" décrit plus loin dans cette leçon ou la cryptographie

fondée sur les courbes elliptiques (Elliptic Curve Cryptography) qui demande des connaissances mathématiques plus élaborées que les fondements de l'arithmétique qui suffisent à comprendre le code RSA. Notons que la cryptographie sur les courbes elliptiques permet des clefs beaucoup plus courtes que les clefs nécessaires au codage RSA.

- Rappels d'arithmétique

Au cours des deux cours précédents, nous avons d'abord étudié la division euclidienne : pour tout $a \in \mathbb{Z}$ et tout entier $b \geq 1$, il existe un unique couple d'entiers $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tel que $0 \leq r \leq b-1$ de sorte que $a = bq + r$.

Puis nous avons introduit la notion de plus grand commun diviseur. Le "pgcd" des entiers a et b, noté pgcd (a, b) ou $a \wedge b$ se calcule avec une suite de divisions euclidiennes puisqu'on a la propriété fondamentale pgcd (a, b) = pgcd (b, r). Si pgcd (a, b) =1, on dit que les entiers a et b sont premiers entre eux : $a \wedge b = 1$.

Quand on suit pas à pas l'algorithme d'Euclide pour le calcul du plus grand commun diviseur, on aboutit à la caractérisation de nombres premiers entre eux à l'aide de l'identité de Bézout. Les entiers a et b sont premiers entre eux si et seulement si il existe deux entiers u et v de sorte que $au + bv = 1$.

Le lemme de Gauss exprime que si un entier a divise le produit bc et si $a \wedge b = 1$, alors a divise c. C'est une conséquence directe de l'identité de Bézout.

Il est utile ensuite d'introduire le vocabulaire des congruences : deux entiers x et y sont congrus *modulo* n si et seulement si $x - y$ est un multiple de n. On le note $x \equiv y \pmod{n}$.

L'entier a compris entre 1 et $n-1$ est inversible *modulo* n si et seulement si il existe un entier b compris entre 1 et $n-1$ de sorte que $ab \equiv 1 \pmod{n}$. L'identité de Bézout permet d'établir que a est inversible *modulo* n si et seulement s'il est premier à n, c'est à dire $a \wedge n = 1$.

Un nombre premier a exactement deux diviseurs : 1 et lui-même. Le petit théorème de Fermat exprime que si p est un nombre premier, alors pour tout $x \in \mathbb{Z}$, $x^p \equiv x \pmod{p}$. Une autre formulation consiste à dire que si x et p sont premiers entre eux, c'est à dire $x \wedge p = 1$, alors $x^{p-1} \equiv 1 \pmod{p}$.

Nous avons vu également une généralisation du petit théorème de Fermat à un entier n produit de deux nombres premiers distints p et q: $n = pq$. Si x et n sont premiers entre eux, alors $x^{(p-1)(q-1)} \equiv 1 \pmod{n}$. On pose aussi $\varphi(n) = (p-1)(q-1)$ si $n = pq$.

- Crible d'Ératosthène

On se propose dans ce paragraphe de mettre en œuvre le crible d'Ératosthène de Cyène (276 avant J.C. - 198 avant J.C.) afin de trouver tous les nombres premiers inférieurs strictement à 100. Rappelons qu'un nombre premier a un ensemble de diviseurs constitué d'une paire. Donc 0 (qui a tous les nombres entiers comme diviseurs) et 1 (qui a comme seul diviseur lui-même) ne sont pas premiers. On commence par écrire tous les nombres entiers positifs et le premier "nombre premier" qui apparaît est le nombre 2, comme illustré à la figure de gauche ci-dessous.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	

	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99

On enlève tous les nombres pairs (multiples de 2) et le nombre suivant dans la liste est le nombre 3 (voir la figure ci-dessus à droite).

	2	3	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49
		53	55		59
61			65	67	
71		73		77	79
		83	85		89
91			95	97	

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	49
		53			59
61				67	
71		73		77	79
		83			89
91				97	

On fait disparaître les multiples de 3 (figure de gauche ci-dessus) et on en déduit que 5 est le nombre premier suivant. On retire de la liste les multiples de 5 (figure de droite ci-dessus) et on découvre le nombre premier qui suit : 7.

Le début de la liste des nombres premiers se lit sur le tableau qui suit (voir la figure de gauche) : 2, 3, 5, 7. On enlève les multiples de 7 parmi les nombres qui n'ont pas déjà été retirés ; le nombre 11 est le suivant de la liste (voir la figure de droite ci-dessous). On remarque que les multiples de 11 non encore considérés commencent avec 11^2, qui est supérieur à 100.

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	49
		53			59
61				67	
71		73		77	79
		83			89
91				97	

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	
		53			59
61				67	
71		73			79
		83			89
				97	

Pour disposer de la liste des nombres premiers inférieurs à 100, il suffit de lire les nombres

restants dans le crible (ci-dessus à droite) :
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

- Code RSA

Il s'agit d'une méthode cryptographique à clef publique proposée par Ronald Rivest, Adi Shamir et Leonard Adleman en 1978 ("A method for obtaining digital signatures and public-key cryptosystems", *Communications of the Association for Computing Machinery*, 1978).
La clef publique est d'une part un nombre n produit de deux nombres premiers distints p et q: $n = pq$ et d'autre part un "exposant" e compris entre 1 et $\varphi(n) = (p-1)(q-1)$ et premier avec ce dernier : $e \wedge \big((p-1)(q-1)\big) = 1$. Un message "en clair" est un nombre m compris entre 1 et n. Le message crypté u est égal à m^e, calculé *modulo* n: $u \equiv m^e \pmod{n}$ et $1 \leq u < n$. Le calcul de u à partir de m ne demande de connaitre que le couple (n, e), clef publique du code RSA.
La clef privée est composée des deux nombres premiers p et q ainsi que l'inverse d *modulo* $((p-1)(q-1))$ de l'exposant e: $ed \equiv 1 \pmod{((p-1)(q-1))}$. Nous allons prouver que $m \equiv u^d \pmod{n}$, ce qui pemet d'expliciter le message en clair m à partir du message crypté u.

- Une proposition préliminaire

On se donne un entier n produit de deux nombres premiers distints p et q: $n = pq$. Si k est un entier congru à 1 *modulo* $(p-1)(q-1)$, alors pour tout entier m, $m^k \equiv m \pmod{n}$.
On montre d'abord que $m^k \equiv m \pmod{p}$. Si p divise m, alors $m \equiv 0 \pmod{p}$ et ce premier résultat partiel est vrai. Si p ne divise pas m, alors m et p sont premiers entre eux car p est premier. Alors $m^{p-1} \equiv 1 \pmod{p}$ d'après le petit théorème de Fermat. Si un nombre k est de la forme $k = 1 + \ell(p-1)(q-1)$, alors $m^k = m\left(m^{p-1}\right)^{\ell(q-1)}$ qui est donc congru à m *modulo* p. On peut ensuite échanger les rôles de p et q et $m^k \equiv m \pmod{q}$. On a donc la double relation $m^k = m + \alpha p = m + \beta q$ pour deux entiers α et β. De la relation $\alpha p = \beta q$, on déduit que p divise le produit βq. Mais p et q sont des nombres premiers différents, donc premiers entre eux. Le lemme de Gauss assure donc que p divise β, donc qu'on peut écrire $\beta = pw$ pour un certain entier w. On a donc $m^k = m + pqw = m + nw$. Cette relation exprime que $m^k \equiv m$ *modulo* n et établit la propriété.

- Pourquoi le décodage du code RSA fonctionne

On rappelle que $u \equiv m^e \pmod{n}$ avec $e \wedge \big((p-1)(q-1)\big) = 1$. On introduit l'inverse d de e *modulo* $(p-1)(q-1)$: $ed \equiv 1 \pmod{(p-1)(q-1)}$. D'après la proposition précédente, pour tout entier m, $m^{ed} \equiv m \pmod{n}$. Alors $u^d = (m^e)^d = m^{ed}$ qui est congru à m *modulo* n.

- Exemple de codage RSA

On prend $p = 3$, $q = 5$, donc $n = 3 \times 5 = 15$. Alors $\varphi(15) = 2 * 4 = 8$. On doit aussi choisir l'exposant de codage e premier avec 8 et compris entre 1 et 7, donc dans la liste 1, 3, 5, 7. Nous prenons par exemple $e = 3$. Alors l'exposant de décodage est très simple (trop !) : $d = 3$ car $3 \times 3 \equiv 1 \pmod{8}$. Abordons maintenant le codage d'un mot $m \in \{1, 2, \ldots, 14\}$. Par exemple $m = 7$ et $u \equiv 7^3 \pmod{15}$. Nous avons $7^2 = 49 = 3 \times 15 + 4$ donc $m^2 \equiv 4 \pmod{15}$ puis $7^3 \equiv 7^2 \times 7 \equiv 4 \times 7 = 28 = 15 + 13 \equiv 13 \pmod{15}$ et $u = 13$. Pour le décodage du mot

$u \in \{1, 2, ... , 14\}$ à l'aide de l'exposant $d = 3$, on calcule u^d *modulo* 15 :
$u^2 = 13 \times 13 = 11 \times 15 + 4$ donc $u^2 \equiv 4 \pmod{15}$. Puis $u^3 = 13^3 \equiv 13^2 \times 13 \equiv 4 \times 13$ et $52 = 3 \times 15 + 7 \pmod{15}$. On en déduit $u^3 \equiv 7 \pmod{15}$ et on a bien retrouvé la valeur initiale $m = 7$!

- Génération de certificats

La création d'un certificat "ssl" avec un ordinateur exploité par "linux-ubuntu" pour fixer les idées est relativement facile. On télécharge le paquet "openssl" :
`sudo apt-get install openssl`. Puis on génère la clef privée d'un code RSA de longueur de 64 bits (ce qui est très peu, du point de vue des applications opérationnelles) :
`openssl genrsa 64 > cle64.key`. On peut lire le fichier "cle64.key" obtenu :

-----BEGIN RSA PRIVATE KEY-----
MEACAQACCQCnQIUdEs291QIDAQABAghoLcI7pdvWyQIFANdlSQ8CBQDGx+LbAgUA
kPJh1QIFAIttCKECBQC7Wo8X
-----END RSA PRIVATE KEY-----

Rien n'est clair car la clef secrète est elle-même cryptée ! Afin de l'écrire "en clair", on rajoute la commande `openssl rsa -in cle64.key -text -noout > cle64.txt`. Le fichier "cle64.text" est alors explicite dans ses grandes lignes :

Private-Key: (64 bit)
modulus: 12051778962759466453 (0xa740851d12cdbdd5)
publicExponent: 65537 (0x10001)
privateExponent: 7506869715337991881 (0x682dc23ba5dbd6c9)
prime1: 3613739279 (0xd765490f)
prime2: 3334988507 (0xc6c7e2db)
exponent1: 2431803861 (0x90f261d5)
exponent2: 2339178657 (0x8b6d08a1)
coefficient: 3143274263 (0xbb5a8f17)

Les notations du logiciel sont bien entendu différentes des nôtres. On a
$n =$ modulus = 12051778962759466453, $p =$ prime1 = 3613739279
et q = prime2 = 3334988507. Le lecteur peut vérifier que
$pq = 3613739279 \times 3334988507 = 12051778962759466453 = n$. De plus
$(p-1)(q-1) = 3613739278 \times 3334988506 = 12051778955810738668$. Par ailleurs, on a
$e =$ publicExponent = 65537 et $d =$ privateExponent = 7506869715337991881 et
$ed = 40822 \times 12051778955810738668 + 1$. On vient de vérifier qu'un exemple de données numériques privées générées par un certificat informatique sont bien des données classiques d'un code RSA.

- Attaques du code RSA

Si on réussit à factoriser $n = pq$ en explicitant les deux nombres premiers p et q, le code RSA est cassé. Ce fut le cas pour un "RSA-155" en 1999. En témoigne le message d'une équipe de chercheurs du Centrum Wiskunde & Informatica d'Amsterdam le 26 août 1999 :

"On August 22, 1999, we found that the 512-bits number
RSA-155 = 109417386415705274218097073220403576120037329454492059909138421314763499842889347847179972578912673324976257528997818337970765372440271467435315933543338 97 can be written as the product of two 78-digit primes:
102639592829741105772054196573991675900716567808038066803341933521790711307779 * 106603488380168454820927220360012878679207958575989291522270608237193062808643". Une vingtaine d'informaticiens théoriciens des nombres et sept mois de travail !

"RSA-768" en 2009.
La factorisation a été trouvée à 20h16 GMT le 12 décembre 2009 :
"RSA-768, a 768-bit RSA modulus with 232-digit decimal representation
123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214 3413 is equal to the product
33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489 *
36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917. Both factors have 384 bits and 116 decimal digits."
Le travail de treize chercheurs appartenant aux six institutions suivantes : l'Ecole Polytechnique Fédérale de Lausanne (Suisse), l" Nippon Telegraph and Telephone Corporation (Tokyo, Japon), l'Université de Bonn (Allemagne), l'Institut National de Recherche en Informatique et Automatique (Nancy, France), Microsoft Research (Redmond, USA) et le CWI Amsterdam (Pays Bas).

"RSA de 4096 bits" en 2016
Il s'agit d'une cryptanalyse acoustique qui a permis de "casser" une clef RSA de 4 096 bits, soit un nombre de 1233 chifres en écriture décimale. Les chercheurs utilisent un microphone pour écouter les bruits émis par un ordinateur lorsqu'il décrypte un message chiffré. "Lorsqu'ils fonctionnent, beaucoup d'ordinateurs émettent un bruit aigu qui est produit par la vibration de certains de leurs composants électroniques. Ces émanations acoustiques sont plus qu'une nuisance, elles peuvent véhiculer des informations sur le logiciel qui est exécuté et exposer des informations sensibles sur des traitements informatiques sécurisés". Ce travail, intitulé "Acoustic Cryptanalysis" dû à Daniel Genkin, Adi Shamir, Eran Tromer est publié dans le *Journal of Cryptology* en 2016.

La sécurité du codage RSA est un défi permanent. Les travaux décrits plus hauts sont proposés par des chercheurs universitaires. Mais on peut trouver sur internet les codes publics de sites comme gmail ou paypal. On imagine mal ce qui pourrait advenir si ces codes étaient cassés.

Exercices

- Règle classique de divisibilité

Montrer qu'un nombre écrit en base dix est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

- Cryptage avec le système RSA

On suppose que la clef publique est $n = 143$ et $e = 49$. On veut envoyer le message $m = 90$. Quel est le message crypté u ? [116]

- Introduction élémentaire au codage "RSA" [d'après le baccalauréat 2018]

Le but de cet exercice est d'envisager une méthode de cryptage à clef publique d'une information numérique, appelée système RSA, en l'honneur des mathématiciens Rivest, Shamir et Adleman, qui ont publié cette méthode de cryptage en 1978. On commence par calculer le reste de la division euclidienne de certaines puissances de l'entier 8 par 55.

a) Vérifier que $8^2 \equiv 9 \pmod{55}$.

b) Vérifier que $8^7 \equiv 2 \pmod{55}$.

c) En déduire le reste de la division euclidienne de 8^{21} par 55.

d) Déduire des questions précédentes le reste de la division euclidienne de 8^{23} par 55.

On considère maintenant l'équation (E) $23x - 40y = 1$, avec des inconnues $(x, y) \in \mathbb{Z}^2$.

e) Pourquoi l'équation (E) admet-elle au moins un couple solution ?

f) Expliciter une solution particulière (x_0, y_0) de l'équation (E).

g) Déterminer tous les couples d'entiers relatifs solutions de l'équation (E).

h) Expliciter la valeur de l'unique entier d vérifiant les conditions $0 \leq d < 40$ et $23\,d \equiv 1 \pmod{40}$.

Le cryptage avec le système RSA consiste pour une personne A à choisir deux nombres premiers p et q, puis à calculer les produits $n = pq$ et $f = (p-1)(q-1)$. Elle choisit également un entier naturel e premier avec f. La personne A publie le couple (n, e), qui est une clef publique permettant à quiconque de lui envoyer un nombre crypté. Les messages sont numérisés et transformés en une suite d'entiers compris entre 0 et $n-1$.

Pour crypter un entier m compris entre 0 et $n-1$, on procède ainsi : on calcule le reste u de la division euclidienne du nombre m^e par n, et le nombre crypté est l'entier u. Dans la pratique, cette méthode est sûre si la personne A choisit des nombres premiers p et q très grands, s'écrivant avec plusieurs dizaines de chiffres. On va l'envisager ici avec des nombres plus simples : $p = 5$ et $q = 11$. La personne A choisit également $e = 23$.

i) Calculer les nombres n et f.

j) Justifier que la valeur de e vérifie la condition voulue.

k) Un émetteur souhaite envoyer à la personne A le nombre $m = 8$. Déterminer la valeur du nombre crypté u.

Afin de mettre en œuvre le décryptage dans le système RSA, la personne A calcule dans un premier temps l'unique entier naturel d vérifiant les conditions $0 \leq d < f$ et $e\,d \equiv 1 \pmod{f}$. Elle garde secret ce nombre d qui lui permet, et à elle seule, de décrypter les nombres qui lui ont été envoyés cryptés avec sa clef publique. Pour décrypter un nombre crypté u, la personne A

calcule le reste m de la division euclidienne du nombre u^d par n. Alors le nombre "en clair", c'est-à-dire le nombre avant cryptage, est exactement le nombre m. Les nombres choisis par A sont encore $p = 5,\ q = 11$ et $e = 23$.

l) Quelle est la valeur de d ?

m) En appliquant la règle de décryptage, retrouver le nombre "en clair" m lorsque le nombre crypté est $u = 17$.

- Décryptage d'un système RSA

On note (n, e) la clef publique d'un système RSA.

a) Si $n = 35$, déterminer tous les choix de e possibles. [5, 7, 11, 13, 17, 19, 23]

b) Si $n = 211 \times 499$, peut-on prendre $e = 1623$? [non]

c) Si la clef publique est $(492153, 2237)$, quelle est la clef privée ? [311673]

d) Même question avec $(2173, 361)$. [121]

e) Que doit-on éviter dans les choix des nombres premiers p et q ?