Cryptographie et arithmétique – Corrigé de l'examen 2014

Exercice 1.

1. Si $x \not\equiv \pm y \mod N$ et $x^2 \equiv y^2 \mod N$, alors N ne divise pas $x \pm y$ mais divise $x^2 - y^2 = (x-y)(x+y)$. La première condition de congruence implique donc que $\operatorname{pgcd}(N, x \pm y) \neq N$, et la seconde que $\operatorname{pgcd}(N, x \pm y) \neq 1$ (si p est un diviseur premier de N, alors par le lemme d'Euclide il divise $x-y$ ou $x+y$) : le pgcd de N et $x \pm y$ est donc un diviseur non trivial de N.

2. On peut résoudre ceci de manière systématique, sans faire des essais au hasard. Je prends le temps de détailler la méthode, mais cela n'est pas nécessaire d'en faire autant dans la rédaction (voir les corrections en TD).
On cherche à obtenir une congruence du type $x^2 \equiv y^2 \mod N$, en prenant pour x un produit de certains nombres du membre de gauche ; le membre de droite est alors un carré (noté y^2) si -1 et les nombres premiers apparaissant dans le membre de droite (dont on s'est débrouillé pour qu'ils soient dans $\mathcal{B}$), une fois le produit formé, sont tous à une puissance paire. Mathématiquement, ceci revient à trouver des entiers α_1, …, α_8 dans $\{0,1\}$ tels que, dans

$$(-1)^{\alpha_1+\alpha_2+\alpha_3+\alpha_7+\alpha_8} 2^{2\alpha_3+\alpha_4+\alpha_7+2\alpha_8} 3^{\alpha_3+\alpha_4+4\alpha_5+\alpha_6+\alpha_7} 5^{2\alpha_1+2\alpha_2} 7^{\alpha_3+\alpha_6} 11^{\alpha_5+\alpha_7+\alpha_8} 13^{\alpha_6+\alpha_7+\alpha_8} 17^{\alpha_1} 23^{\alpha_2} 37^{\alpha_4},$$

toutes les puissances soient paires ($\alpha_i = 0$ si le i-ième nombre de notre colonne ne figure pas dans le produit, et 1 sinon). Ceci revient donc à résoudre le système suivant modulo 2, donc dans $\mathbb{Z}/2\mathbb{Z}$:

$$\begin{cases} \alpha_1+\alpha_2+\alpha_3+\alpha_7+\alpha_8 &= 0,\\ \alpha_4+\alpha_7 &= 0,\\ \alpha_3+\alpha_4+\alpha_6+\alpha_7 &= 0,\\ \alpha_3+\alpha_6 &= 0,\\ \alpha_5+\alpha_7+\alpha_8 &= 0,\\ \alpha_6+\alpha_7+\alpha_8 &= 0,\\ \alpha_1 &= 0,\\ \alpha_2 &= 0,\\ \alpha_4 &= 0. \end{cases}$$

On peut encore le simplifier un peu avant de le résoudre, puisqu'on voit immédiatement que $\alpha_1 = \alpha_2 = \alpha_4 = 0$ (et donc que 21049, 22984 et 48669 ne figureront pas dans le produit x) :

$$\begin{cases} \alpha_3+\alpha_7+\alpha_8 &= 0,\\ \alpha_7 &= 0,\\ \alpha_3+\alpha_6+\alpha_7 &= 0,\\ \alpha_3+\alpha_6 &= 0,\\ \alpha_5+\alpha_7+\alpha_8 &= 0,\\ \alpha_6+\alpha_7+\alpha_8 &= 0. \end{cases}$$

On en arrive facilement à $\alpha_3 = \alpha_5 = \alpha_6 = \alpha_8$, le reste étant nul. Donc $\alpha_3 = \alpha_5 = \alpha_6 = \alpha_8 = 1$ est une solution, ce qui signifie que

$$x = 47607 \cdot 67495 \cdot 67747 \cdot 88633 = 19294251454456364715$$

fournit une solution à notre problème (il est bien sûr plus commode de plutôt prendre $x \equiv 925744 \mod 5680267$). On a dans ce cas $y^2 = 2^4 3^6 7^2 11^2 13^2 = 108108^2$, et :

$$\operatorname{pgcd}(N, x-y) = 2879, \quad \operatorname{pgcd}(N, x+y) = 1973,$$

calculés grâce à l'algorithme d'Euclide étendu, qui sont deux diviseurs non triviaux de N (en vérité, ce sont deux diviseurs premiers, et ce sont les seuls).

Exercice 2.

1. Notons d'abord que $c \equiv m^e \mod N$ par définition, et donc $c \equiv m^e \mod p$ et $\mod q$.
   Montrons que $c^d \equiv m \mod p$ et $\mod q$. Par le théorème des restes chinois, la congruence sera alors vraie modulo N. Comme d est l'inverse de e modulo R, on a $de \equiv 1 \mod R$, et donc $de \equiv 1 \mod p-1$. En particulier, il existe un entier k tel que $de = 1 + (p-1)k$. Ainsi,

   $$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{1+(p-1)k} \equiv m \cdot (m^{p-1})^k \equiv m \mod p$$

   dans tous les cas : si m n'est pas premier à p, alors $m \equiv 0 \mod p$ et donc $c \equiv 0 \mod p$, si bien que $c^d \equiv 0 \equiv m \mod p$ trivialement, sans même avoir à effectuer tous ces calculs [*], tandis que si m est premier à p, alors $m^{p-1} \equiv 1 \mod p$ par le petit théorème de Fermat. On a bien montré que $c^d \equiv m \mod p$, et on procède de même modulo q, d'où le résultat.
2. Ici, $\phi(N) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$. Comme $(p-1)(q-1)$ et R ont exactement les mêmes diviseurs premiers, qui sont ceux de $p-1$ et $q-1$ [†], être premier à R et être premier à $\phi(N)$ sont équivalents.
3. Si $N = 77 = 7 \times 11$ et $e = 7$, alors l'inverse de e modulo $\phi(N) = 60$ est 43 (on le calcule en établissant une relation de Bézout entre 60 et 7, grâce à l'algorithme d'Euclide étendu), tandis que l'inverse de e modulo $R = 30$ est 13 [‡].
4. Comme $N = pq$ et $\phi(N) = (p-1)(q-1) = N - (p+q) + 1$, la connaissance de N et $\phi(N)$ permet de connaître pq et $p+q$, et donc de connaître p et q en résolvant l'équation polynomiale $X^2 - (p+q)X + pq = 0$ (équivalente à $X^2 + (\phi(N) - N - 1)X + N = 0$). La résolution, dans notre exemple, donne $\{p, q\} = \{2897, 1901\}$.
5. On a $R = \text{ppcm}(p-1, q-1) = \frac{(p-1)(q-1)}{\text{pgcd}(p-1,q-1)}$, écriture qui permet de s'affranchir de factorisations de $p-1$ et $q-1$: on calcule en effet leur pgcd grâce à l'algorithme d'Euclide étendu, pour obtenir $\text{pgcd}(p-1, q-1) = 4$, et donc $R = 1375600$.
6. On doit choisir e premier à R. Ici, $\text{pgcd}(R, e) = 181$: c'est un mauvais choix.
7. Cette fois-ci, $\text{pgcd}(R, e) = 1$: e et R sont bien premiers entre eux.
8. Grâce à l'algorithme d'Euclide étendu, on trouve une relation de Bézout entre $e = 547$ et $R = 1375600$, et l'inverse de $e \mod R$ est $d = 812283$.
9. Comme $547 = 2^9 + 2^5 + 2^1 + 2^0$, on a :

   $$m^{547} = \left(\left(\left(\left(\left(\left(\left(\left(m^2\right)^2\right)^2\right)^2 \cdot m\right)^2\right)^2\right)^2\right)^2 \cdot m\Bigg)^2 \cdot m.$$

   On voit alors que m^{547} requiert 12 multiplications modulo N.

Exercice 3.

1. On a $y \oplus z \oplus e_B = x \oplus e_B \oplus e_A \oplus e_B = x \oplus e_A = m \oplus e_A \oplus e_A = m$. Donc Bob a juste besoin d'ajouter y et sa clé e_B au message z d'Alice pour retrouver m.
2. On a $x \oplus y \oplus z = x \oplus y \oplus (y \oplus e_A) = x \oplus e_A = m \oplus e_A \oplus e_A = m$. Donc la connaissance de x, y et z suffit à reconstituer le message m (sans connaître e_A ou e_B).

∗. C'est aussi pour traiter ce cas qu'il est très commode de passer par le théorème des restes chinois : si m n'est pas premier à N, on ne peut pas en déduire pour autant que $m \equiv 0 \mod N$ et conclure rapidement.

†. Car $p-1$ et $q-1$ divisent R qui, lui-même, divise $(p-1)(q-1)$, selon la définition du ppcm et le fait que $(p-1)(q-1)$ soit un multiple commun à $p-1$ et $q-1$.

‡. Ce n'est pas un hasard si ces deux clés de déchiffrement diffèrent d'un multiple de R : pourquoi était-ce prévisible ?

3. Le cas où p divise m est trivial, donc on l'exclut.
Notons que Bob connaît $z \equiv y^{d_A} \equiv x^{d_A e_B} \equiv m^{d_A e_A e_B} \mod p$. Comme $e_A d_A \equiv 1 \mod p-1$ et $m^{p-1} \equiv 1 \mod p$, on a même $z \equiv m^{e_B} \mod p$, donc $z^{d_B} \equiv m \mod p$. Il suffit donc, pour Bob, d'élever le message chiffré z à la puissance d_B (qu'il connaît) pour connaître m.

4. L'homme du milieu choisit un entier e_C inversible modulo $p-1$ connu de lui seul, d'inverse d_C. Ensuite, interceptant un message d'Alice x, il lui renvoie $y = x^{e_C}$ en se faisant passer pour Bob, et enfin Alice calcule $z = y^{d_A}$ que l'homme du milieu intercepte encore à la place de Bob. Il peut décoder le message en calculant z^{d_C}, comme on l'a vu dans la troisième question, à l'insu d'Alice et Bob.

5. Sachant résoudre le problème du Log Discret, la connaissance de y et z permet de calculer $\log_y(z) = d_A$, et donc d'obtenir $x^{d_A} \equiv m \mod p$.

6. Non : n'importe quel élément m de $(\mathbb{Z}/p\mathbb{Z})^*$ peut donner $x = 1$ par un choix de e_A convenable (qui est multiple de l'ordre de m).

7. Soit G un groupe. Si $g \in G$ est d'ordre k, alors g^l est d'ordre $\frac{k}{\text{pgcd}(l,k)}$; c'est un résultat classique. Ainsi, si m est une racine primitive modulo p, alors m est d'ordre $p-1$, et $x \equiv m^{e_A} \mod p$ est d'ordre $\frac{p-1}{\text{pgcd}(p-1,e_A)}$. On a choisi e_A inversible modulo $p-1$, donc premier à $p-1$, signifiant que $\text{pgcd}(p-1, e_A) = 1$ et que x est d'ordre $p-1$, donc est une racine primitive. On raisonne de même pour la réciproque, puisque $m \equiv x^{d_A} \mod p$ (et d_A est premier à $p-1$).

8. Un groupe cyclique d'ordre d admet $\varphi(d)$ générateurs (on le voit en se ramenant, par isomorphisme, au cas de $(\mathbb{Z}/d\mathbb{Z}, +)$, engendré par tout entier premier à d). Comme $(\mathbb{Z}/p\mathbb{Z})^*$ a $p-1$ éléments, il admet $\varphi(p-1)$ générateurs (ou racines primitives $\mod p$, c'est la même chose). Ici,

$$\varphi(p-1) = \varphi(2)\varphi(7^2)\varphi(11^3) = 1 \times 7(7-1) \times 11^2(11-1) = 42350.$$

9. C'est un usage typique du théorème des restes chinois : on a

$$e_B \equiv 1 \times 7^2 \cdot 11^3 \cdot u_1 + 6 \times 2 \cdot 11^3 \cdot u_2 + 684 \times 2 \cdot 7^2 \cdot u_3 \mod 2 \times 7^2 \times 11^3,$$

où u_1 est l'inverse de $7^2 \cdot 11^3 \mod 2$, u_2 l'inverse de $2 \cdot 11^3 \mod 7^2$ et u_3 l'inverse de $2 \cdot 7^2 \mod 11^3$. Grâce aux indications de l'énoncé, on sait que $u_1 \equiv 1 \mod 2$, $u_2 \equiv -3 \mod 7^2$ et $u_3 \equiv 747 \mod 11^3$. Donc :

$$e_B \equiv 2015 \mod 130438.$$

Exercice 4.

1. Comme 0 et 1 ne sont pas racines de P, ses facteurs irréductibles ne peuvent pas être de degré 1, donc sont nécessairement de degré 2 ou 4 (un facteur irréductible de degré 3 en implique un autre de degré 1, P étant de degré 4, donc ce cas est exclu aussi). Or le seul polynôme de degré 2 irréductible sur $\mathbb{F}_2$ est $X^2 + X + 1$, et $(X^2 + X + 1)^2 = X^4 + X^2 + 1 \neq P$, donc P n'a pas de facteur de degré 2. Par conséquent, il est irréductible.

2. Je donne l'expression de m à la fin de chaque étape et de chaque tour :

   (a) `AddRoundKey`(K_0) :

(1,0,0,0)	(1,1,0,0)
(0,0,0,0)	(0,0,0,0)

   (b) `SubBytes`, `ShiftRows`, `MixColumns`, `AddRoundKey`(K_1) : notons que tout élément $x \in \mathbb{F}_{16}$ vérifie $x^{15} = 1$. On en déduit, en particulier, que $(\alpha^3)^{-1} = \alpha^{12} = (\alpha^4)^3 = (\alpha+1)^3 = \alpha^3 + \alpha^2 + \alpha + 1$. Ce genre d'« astuce » permet de calculer les inverses rapidement, plutôt qu'en passant par des relations de Bezout (si on a l'aisance pour se le permettre). De même, $\alpha^3 + \alpha^2 = \alpha^2(\alpha+1) = \alpha^6$, dont l'inverse est $\alpha^9 = (\alpha^4)^2\alpha = (\alpha+1)^2\alpha = \alpha^3 + \alpha$. Je ne détaille pas le reste des calculs, on obtient :

(0,1,0,0)	(0,0,0,1)
(0,1,1,0)	(0,0,1,0)

(c) `SubBytes`, `ShiftRows`, `MixColumns`, `AddRoundKey`(K_2) : on obtient :

(0,0,0,1)	(1,0,0,0)
(1,0,1,0)	(1,1,0,1)

(d) `SubBytes`, `ShiftRows`, `AddRoundKey`(K_3) : on obtient :

(1,1,0,0)	(1,1,0,1)
(0,1,0,1)	(0,1,0,1)

3. Pour savoir déchiffrer ce message, il est facile de se convaincre qu'il suffit de savoir inverser les opérations `AddRoundKey`, `SubBytes`, `ShiftRows` et `MixColumns`.
L'opération `AddRoundKey` est la plus simple à inverser : il suffit de la réitérer pour retomber sur les quatre demi-octets précédents. La justesse du procédé vient du fait que $k_i + k_i = 2k_i = 0$ pour tout demi-octet k_i (les opérations se font dans un corps de caractéristique 2).
L'opération `ShiftRows` est également facile à inverser : il suffit de permuter les cases de la deuxième ligne à nouveau, puisque la transposition est involutive.
Pour inverser `SubBytes`, qui est la composée $S = f \circ I$ sur chaque demi-octet, on doit calculer $S^{-1} = I^{-1} \circ f^{-1}$. Comme $\left(x^{-1}\right)^{-1} = x$ pour $x \in \mathbb{F}_{16}$, on sait que $I^{-1} = I$, et f s'inverse comme toute fonction affine (on peut vérifier que A est bien inversible car de déterminant 1 modulo 2, donc f également). La résolution de $f(x) = y$ mène à $x = A^{-1}(y - B)$, donc f^{-1} est définie par $y \mapsto A^{-1}(y - B)$. En bref, l'inversion de `SubBytes`, qu'on note `InvSubBytes`, s'obtient par la composée $S = I \circ f^{-1}$, où $f^{-1} : \begin{cases} \mathbb{F}_{16} \simeq (\mathbb{F}_2)^4 & \to & \mathbb{F}_{16} \simeq (\mathbb{F}_2)^4 \\ y & \mapsto & A^{-1}(y - B) \end{cases}$ avec, après quelques calculs sommaires (grâce à l'algorithme du pivot de Gauss par exemple),

$$A^{-1} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Il reste à inverser `MixColumns`, qui consiste en une multiplication matricielle ; il suffit donc de savoir quel est l'inverse de cette matrice, et le calcul de l'inverse d'une matrice de taille 2×2 est élémentaire ; ici, on s'aperçoit que la matrice $\begin{pmatrix} \alpha & 1+\alpha \\ 1+\alpha & \alpha \end{pmatrix}$ est sa propre inverse. Donc cette opération, à l'instar de `AddRoundKey` et `ShiftRows`, s'inverse par réitération.
Pour résumer, on déchiffre un message en appliquant à c les transformations suivantes :
   (a) On effectue un tour qui comporte les trois étapes : `AddRoundKey`(K_3), `ShiftRows` et `InvSubBytes` ;
   (b) On effectue deux tours comprenant quatre étapes : `AddRoundKey`(K_i), `MixColumns`, `ShiftRows` et `InvSubBytes` pour $i = 2$ puis $i = 1$;
   (c) On applique `AddRoundKey`(K_0).
4. Le lecteur en exercice se chargera d'appliquer la méthode de la question précédente au déchiffrement de c.