INFMDI720
Contrôle de connaissance

Rappels mathématiques pour la cryptographie

22 novembre 2011

Consignes :

Les exercices sont complètement indépendants. Ils pourront être traités dans un ordre quelconque, mais on demande de faire apparaître de façon très visible dans les copies où commence chaque exercice.

Il n'est pas nécessaire de faire des réponses longues.

L'usage de tous les documents (notes de cours manuscrites ou imprimées, livres) est autorisé.

L'usage des calculatrices électroniques est interdit.

Durée : 2h

Exercice 1.

(1a) Rappeler pourquoi, si x n'est pas multiple de 13, alors $x^{12} \equiv 1 \pmod{13}$, et pourquoi, si x n'est pas multiple de 19, alors $x^{18} \equiv 1 \pmod{19}$.

(1b) En déduire que, si x n'est pas multiple de 13, alors $x^{36} \equiv 1 \pmod{13}$, et que, si x n'est pas multiple de 19, alors $x^{36} \equiv 1 \pmod{19}$.

(2) Conclure de la question précédente que si x est premier avec 247, alors $x^{36} \equiv 1 \pmod{247}$ (remarque : $247 = 13 \times 19$).

(3) Que vaut $\varphi(247)$ (où bien sûr φ désigne l'indicatrice d'Euler) ?

(4) En oubliant provisoirement les questions (1) et (2), quel théorème connu permettait d'énoncer le fait que $x^N \equiv 1 \pmod{247}$ si x est premier avec 247, pour un certain N (à préciser) ne dépendant pas de x ? Comparer ce résultat avec celui de la question (2), et commenter (lequel est le plus fort ?).

(5) Rappeler pourquoi il existe g_1 (resp. g_2) un élément de $(\mathbb{Z}/13\mathbb{Z})^\times$ (resp. $(\mathbb{Z}/19\mathbb{Z})^\times$) dont l'ordre multiplicatif vaut exactement 12 (resp. 18) : comment appelle-t-on un tel élément ?

(6) Rappeler pourquoi il existe $h \in (\mathbb{Z}/247\mathbb{Z})^\times$ tel que $h \equiv g_1 \pmod{13}$ et $h \equiv g_2 \pmod{19}$.

(7) Montrer que l'ordre multiplicatif (modulo 247) d'un tel h vaut exactement 36. Quel est l'ordre multiplicatif maximal possible d'un élément de $(\mathbb{Z}/247\mathbb{Z})^\times$?

(8) Dresser la table des puissances de 2 modulo 13 puis modulo 19.

(9) Montrer que 2 est d'ordre multiplicatif 36 modulo 247.

(10) Montrer que l'élément $\bar{3} \in (\mathbb{Z}/247\mathbb{Z})^\times$ *n'est pas* une puissance de 2 (on justifiera la réponse).

Exercice 2.

Soit p un nombre premier tel que $p \equiv 3 \pmod{4}$.

(1) Montrer que $(p-1)/2$ est impair. Que vaut $(-1)^{(p-1)/2}$?

(2) Si $z \in \mathbb{F}_p^\times$, que vaut $(z^2)^{(p-1)/2}$? En déduire qu'il n'existe pas de $z \in \mathbb{F}_p$ tel que $z^2 = -1$.

(3) Déduire de la question précédente que le polynôme $t^2 + 1 \in \mathbb{F}_p[t]$ est irréductible.

On pose maintenant $E = \mathbb{F}_p[t]/(t^2+1)$.

(4) Combien d'éléments a E ? Que peut-on dire de sa structure algébrique (est-ce un anneau, un corps...) ? Quel autre nom (à part « E ») pourrait-on lui donner ? Quelle est la forme générale d'un élément de E ?

On notera « $\sqrt{-1}$ » l'élément $\bar{t}$ de E, c'est-à-dire, la classe modulo t^2+1 de l'indéterminée t. (On ne cherchera pas à donner un sens à la notation $\sqrt{\ }$, encore

moins à faire un lien avec les nombres réels ou complexes : on se contentera de prendre $\sqrt{-1}$ comme une notation pour $\bar{t}$.)

(5) Que vaut le carré $(\sqrt{-1})^2$ de l'élément qu'on vient de décrire ?

(6) Quelles sont toutes les solutions de l'équation $z^2 = -1$ dans E ? En déduire quelle est la factorisation du polynôme $t^2 + 1$ vu, cette fois, comme un élément de $E[t]$.

(7) Expliquer pourquoi tout élément de E s'écrit de la forme $u + v\sqrt{-1}$ avec u, v deux éléments de $\mathbb{F}_p$ (uniquement déterminés). Donner des formules permettant de calculer la somme $(u_1 + v_1\sqrt{-1}) + (u_2 + v_2\sqrt{-1})$ et le produit $(u_1 + v_1\sqrt{-1}) \cdot (u_2 + v_2\sqrt{-1})$ de deux éléments de E, en les mettant sous la forme $u + v\sqrt{-1}$ (on demande donc de calculer u et v de la somme et du produit en fonction de u_1, v_1, u_2, v_2).

(8) Que vaut $(\sqrt{-1})^4$? Déterminer $(\sqrt{-1})^r$ en discutant suivant la valeur de l'entier r modulo 4.

On rappelle que $\mathrm{Frob}\colon E \to E$ désigne l'application $x \mapsto x^p$.

(9) D'après la question précédente, que vaut $\mathrm{Frob}(\sqrt{-1})$?

On rappelle pour la question suivante que $\mathrm{Frob}(x + y) = \mathrm{Frob}(x) + \mathrm{Frob}(y)$ et $\mathrm{Frob}(xy) = \mathrm{Frob}(x)\,\mathrm{Frob}(y)$ pour tous $x, y \in E$ (« le Frobenius est un morphisme de corps »), et aussi que $\mathrm{Frob}(a) = a$ si et seulement si $a \in \mathbb{F}_p$ (petit théorème de Fermat).

(10) Que vaut $\mathrm{Frob}(u + v\sqrt{-1})$ si $u, v \in \mathbb{F}_p$?

(11) En utilisant notamment la question précédente, montrer que l'on a : $(u + v\sqrt{-1})^{p+1} = u^2 + v^2$ pour tous $u, v \in \mathbb{F}_p$.

(12) Rappeler pourquoi il existe un élément g de $E^\times$ d'ordre multiplicatif $p^2 - 1$ (on ne demande pas de démontrer ce fait, mais de citer un théorème qui l'affirme) ; comment appelle-t-on un tel élément ?

Pour r entier, on définit u_r, v_r, éléments de $\mathbb{F}_p$, par la formule : $u_r + v_r\sqrt{-1} = g^{r(p-1)}$, où g est un élément comme dans la question précédente.

(13) Que vaut $u_r^2 + v_r^2$? Expliquer pourquoi les (u_r, v_r) avec $0 \leq r \leq p$ sont deux-à-deux distincts.

(14) Réciproquement, si u, v dans $\mathbb{F}_p$ vérifient $u^2 + v^2 = 1$, montrer que $u + v\sqrt{-1}$ peut s'écrire sous la forme $g^{r(p-1)}$ (on a donc $(u, v) = (u_r, v_r)$) pour un certain r qu'on peut trouver vérifiant $0 \leq r \leq p$. (On pourra commencer par écrire $u + v\sqrt{-1} = g^s$ pour un certain s, puis montrer que celui-ci est un multiple de $p - 1$ en utilisant $u^2 + v^2 = 1$.)

(15) Des questions précédentes, déduire le nombre de solutions (u, v) dans $\mathbb{F}_p$ de l'équation $u^2 + v^2 = 1$.