Le corps $\mathbb{F}_{256}$ est une structure algébrique qui possède 256 éléments pour lesquels des opérations d'addition, de multiplication, de soustraction et même de division sont disponibles. Mathématiquement, c'est l'unique corps à 256 éléments, à isomorphisme près. *Les calculs dans $\mathbb{F}_{256}$ sont utilisés dans des codes correcteurs d'erreurs (notamment le code CIRC des disques compacts) et dans certains systèmes cryptographiques (comme l'AES et Whirlpool), chaque octet étant vu comme un élément de cette structure abstraite.*

Il s'agit donc de représenter les 256 éléments de $\mathbb{F}_{256}$ par chacun des 256 octets. La représentation choisie détermine les tables d'addition et de multiplication utilisées. Il est naturel cependant de choisir l'octet 0 pour représenter l'élément neutre de l'addition et l'octet 1 pour l'élément neutre de la multiplication (mais ce n'est pas obligatoire !). Le choix de la représentation des 256 éléments par des octets (et donc le choix des tables de calculs) est important, surtout lorsque des données sont échangées entre des applications distinctes.

De manière classique, la représentation d'un octet par un élément de $\mathbb{F}_{256}$ s'appuie sur une interprétation en terme de polynômes à coefficients dans $\{0,1\}$. L'ensemble de ces polynômes dispose lui aussi d'opérations d'addition et de multiplication, ainsi que d'une division euclidienne (utilisée notamment dans de nombreux codes correcteurs). L'objectif de cette séance est de rappeler ces opérations classiques puis de construire les tables de calculs dans $\mathbb{F}_{256}$. Ces dernières seront utilisées ultérieurement dans le codage de l'AES.

L'ensemble des deux bits $\{0,1\}$ est noté $\mathbb{F}_2$. Il est classiquement muni d'une addition et d'une multiplication données par les tables suivantes : [1]

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Ainsi l'addition correspond au Ou-exclusif ($\oplus$) et la multiplication au Et-logique ($\wedge$) si 0 représente « faux » et 1 représente « vrai. »

On désigne par $\mathbb{F}_2[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{F}_2$, c'est-à-dire l'ensemble des suites de bits a_0, a_1,..., a_n,... nulles à partir d'un certain rang. Un tel polynôme sera noté formellement $\sum a_k.X^k$ ou plus simplement $a_n.X^n + a_{n-1}.X^{n-1} + ... + a_0$ si tous les termes à partir de a_{n+1} sont nuls. Le *degré* d'un polynôme non nul $A = a_n.X^n + a_{n-1}.X^{n-1} + ... + a_0$ est le plus grand entier $k \geqslant 0$ tel que $a_k \neq 0$. De plus, par convention, le degré du polynôme nul est $-\infty$.

Exercice I.1 Addition dans l'anneau des polynômes $\mathbb{F}_2[X]$ L'ensemble $\mathbb{F}_2[X]$ est muni d'une addition. Si $A = a_n.X^n + a_{n-1}.X^{n-1} + ... + a_0$ et $B = b_n.X^n + b_{n-1}.X^{n-1} + ... + b_0$ alors $A + B = \sum c_k.X^k$ où $c_k = a_k \oplus b_k$, c'est-à-dire que les coefficients de $A + B$ sont les XOR bit-à-bit des coefficients de A et de B. Ainsi le degré de $A + B$ est toujours inférieur aux degrés de A et de B.

Nous ne considérerons aujourd'hui que des polynômes de degré inférieur à 31, qui seront représentés par des entiers de type `int`. Ainsi $X^{10} + X^3 + 1$ correspond à la suite 10010000001000...0... et à l'entier $(10000001001)_2 = 1 + 2^3 + 2^{10} = 1 + 8 + 1024 = 1033$.

Question 1. Que vaut $8 + 7$? Et $7 + 1$?

Question 2. Écrire une fonction `int Add_F2X(int A, int B)` qui renvoie la valeur de $C = A + B$ *vus évidemment comme des polynômes sur* $\mathbb{F}_2$. ☺

Question 3. Expliquer pourquoi $A + B = B + A$ dans $\mathbb{F}_2[X]$. Expliquer pourquoi $A + A = 0$ dans $\mathbb{F}_2[X]$.

Question 4. Si A est fixé, quels sont les polynômes B tels que $A + B = 0$?

Exercice I.2 Multiplication dans $\mathbb{F}_2[X]$ L'ensemble $\mathbb{F}_2[X]$ est également muni d'une multiplication. Si $A = a_n.X^n + a_{n-1}.X^{n-1} + ... + a_0$ et $B = b_n.X^n + b_{n-1}.X^{n-1} + ... + b_0$ alors $A \times B = \sum c_k.X^k$ où, comme d'habitude, $c_k = \sum_{i=0}^{i=k} a_i \times b_{k-i}$, c'est-à-dire $c_k = \bigoplus_{i=0}^{i=k} a_i \wedge b_{k-i}$, puisque l'addition correspond au Ou-exclusif ($\oplus$) et la multiplication au Et-logique ($\wedge$). Ainsi le degré de $A \times B$ est toujours égal à la somme des degrés de A et de B (y compris si A ou B est nul).

1. Si l'on désigne par $\overline{x}$ le reste de l'entier x dans la division euclidienne par 2, alors l'addition et la multiplication dans $\mathbb{F}_2$ sont caractérisées par les formules : $\overline{x} + \overline{y} = \overline{x + y}$ et $\overline{x} \times \overline{y} = \overline{x \times y}$. Il s'en suit que toutes les identités algébriques valables pour $\mathbb{Z}$: commutativites, associativités, distributivité, sont aussi valables pour $\mathbb{F}_2$.

Question 1. Que vaut 3×2 ? Et 3×3 ? Et 4×3 ? Et $2^k \times 3$?

Question 2. Écrire une fonction `int Mul_par_Xk_F2X(int A, int k)` qui calcule la valeur $A \times X^k$.

Question 3. Écrire une fonction `int Mul_F2X(int A, int B)` qui calcule la valeur $C = A \times B$.
Indication : On pourra s'appuyer sur la remarque suivante. Si $B = \sum_{i=0}^{31} b_i.X^i$ alors par distributivité de l'addition sur la multiplication, $A \times B = \sum_{i=0}^{31}(A \times b_i.X^i)$. Il s'agit ici d'une somme de polynômes, que l'on sait déjà coder. D'autre part, il est facile de multiplier A par $b_i.X^i$: si b_i vaut 0, ça vaut 0, et sinon ça vaut $A * X^i$, que l'on sait déjà calculer.

Exercice I.3 Degré d'un polynôme Écrire une fonction `degre(int A)` qui retourne le degré de A.

Exercice I.4 Division euclidienne dans $\mathbb{F}_2[X]$ Étant donnés deux polynômes A et B avec $B \neq 0$, les mathématiciens nous disent qu'il existe un couple de polynômes (Q, R) unique tel que

$$A = B \times Q + R \text{ avec degré}(R) < \text{degré}(Q)$$

Les polynômes Q et R sont respectivement appelés le *quotient* et le *reste* de la *division euclidienne* de A par B.

Question 1. Que vaut la division de 4 par 3 dans $\mathbb{F}_2[X]$?

Question 2. Pour calculer le quotient et le reste, vous avez appris en Licence qu'il suffit de procéder récursivement. Si le degré de B vaut 0, alors $B = 1$ et $R = 0$: il n'y a rien à faire : il suffit de renvoyer $Q = A$ et $R = 0$. Si le degré de A est strictement inférieur au degré de B, il n'y a plus rien à faire non plus : il suffit de renvoyer $Q = 0$ et $R = A$. Sinon, on considère $A' = A + X^k \times B$ avec $k = \deg(A) - \deg(B)$; alors $\deg(X^k \times B) = \deg(A)$ et donc $\deg(A') < \deg(A)$. Si la division de A' par B retourne le quotient Q' et le reste R' alors $A' = Q' \times B + R'$, avec $\deg(R') < \deg(B)$ et $A = (Q' + X^k) \times B + R'$. Le résultat cherché est donc $Q = Q' + X^k$ et, plus important pour nous, $R = R'$. Ainsi, le calcul du reste R de la division de A par B suit les règles suivantes :
   — Si $B = 1$ alors $R = 0$. On peut donc supposer $\deg(B) \geqslant 1$.
   — Si $\deg(A) < \deg(B)$ alors $R = A$.
   — Si $\deg(A) \geqslant \deg(B)$ alors on peut remplacer A par $A' = A + X^k \times B$ avec $k = \deg(A) - \deg(B)$ et recommencer.

   Écrire une fonction `int Reste_F2X(int A, int B)` qui calcule le reste de la division euclidienne de A par B sous l'hypothèse $B \neq 0$.

Les 256 octets représentent les 256 éléments de $\mathbb{F}_{256}$; de plus, chaque octet est vu comme un polynôme de degré 7. Ils seront codés en pratique par une variable de type `unsigned char`, noté `uchar`.

Exercice I.5 Addition dans $\mathbb{F}_{256}$ L'addition dans $\mathbb{F}_{256}$ est très simple : elle correspond à l'addition dans $\mathbb{F}_2[X]$: c'est un simple XOR bit-à-bit. Écrire une fonction `uchar Add_F256(uchar A, uchar B)` qui retourne $C = A$ `+` B où A et B sont vus comme des éléments de $\mathbb{F}_{256}$.

Exercice I.6 Multiplication dans $\mathbb{F}_{256}$ Pour la multiplication, en revanche, c'est un peu plus compliqué. Nous fixons pour la suite le polynôme $G = X^8 + X^7 + X^2 + X + 1$. Ce polynôme est fixé par la norme de l'AES et n'a pas été choisi au hasard, comme nous le verrons. Pour multiplier A par B, on multiplie d'abord $C = A \times B$ où A, B et C vus comme des polynômes de $\mathbb{F}_2[X]$. Le degré de C vaut $\deg(A) + \deg(B)$, qui peut dépasser 7. Le résultat de la multiplication de A par B, vus comme des éléments de $\mathbb{F}_{256}$ est simplement le reste de la division euclidienne de C par G : c'est bien un polynôme de degré inférieur à 7. Écrire une fonction `uchar Mul_F256(uchar A, uchar B)` qui retourne $C = A$ `×` B.

Exercice I.7 Pour les mathématiciens dans la salle Notons $\widetilde{A}$ le reste du polynôme A dans la division euclidienne par G. Autrement dit, nous avons $A = P \times G + \widetilde{A}$ où $\widetilde{A}$ est un polynôme de degré inférieur à 7. Ainsi A est un représentant de l'élément $\widetilde{A}$ de $\mathbb{F}_{256}$. L'addition `+` et la multiplication `×` dans l'ensemble $\mathbb{F}_{256}$ satisfont les formules classiques suivantes : A `+` $B = \widetilde{A + B}$ et A `×` $B = \widetilde{A \times B}$.

Question 1. Expliquer pourquoi $\widetilde{A}$ `+` $\widetilde{B} = \widetilde{A + B}$ et $\widetilde{A}$ `×` $\widetilde{B} = \widetilde{A \times B}$ quels que soient $A, B \in \mathbb{F}_2[X]$.

Question 2. Expliquez pourquoi toutes les identités classiques sont valables dans $\mathbb{F}_{256}$: commutativités, associativités, distributivité.