3 Cryptographie

Exercice 3.1 Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d’entiers $k$ premier avec $n$ tels que $1 \leq k \leq n$. Soit $n = pq$, où $p$ et $q$ sont deux nombres premiers $p$ et $q$ distincts.

1. À quoi est égal $\varphi(n)$ ?
2. Montrer que si l’on connait $n$ et $\varphi(n)$, on peut retrouver facilement $p$ et $q$.
3. Application : $n = 391 = pq$ et $\varphi(n) = 352$. Calculer $p$ et $q$.

Exercice 3.2 Dans un cryptosystème utilisant la méthode RSA, déterminer la clé secrète $(\varphi(n), d)$ et le message envoyé $M \in \mathbb{Z}/n\mathbb{Z}$ pour les clés publiques $(n, e)$ et les messages cryptés reçus $C = M^e$ suivants :

1. $n = 35$, $e = 5$, $C = 10$.
2. $n = 265$, $e = 139$, $C = 10$.

Exercice 3.3 Alice et Bob communiquent en utilisant la méthode RSA. Bob cherche donc deux nombres premiers $p$ et $q$, et calcule leur produit $n = 253$. Il rend public le couple $(n, 13)$.

1. Quelle est la clé secrète de Bob ?
2. Alice veut transmettre le message $M = 2$ à Bob. Quel message crypté $C$ ce dernier va-t-il recevoir ?
3. Bob a reçu d’Alice le message crypté $C = 22$. Quel est le message $M$ que Alice lui a envoyé ?

Exercice 3.4 Soit $P = X^4 + X + 1 \in \mathbb{F}_2[X]$. On note $K = \mathbb{F}_2[X]/P.\mathbb{F}_2[X]$ et $\alpha$ la classe de $X$ dans $K$.

1. Montrer $P$ est irréductible dans $\mathbb{F}_2[X]$.
2. Montrez que $K$ est un corps. Combien possède-t-il d’éléments ?
3. Quel est l’inverse de $1 + \alpha + \alpha^2$ dans $K$ ?
4. Montrer $\alpha$ est un générateur de $K^*$.

Exercice 3.5 On utilise le corps $K$ et son générateur $\alpha$ construit à l’exercice 3.4.

Alice choisit un entier $e$ qu’elle a gardé secret et a rendu public l’élément $\alpha^e = \alpha^2 + 1 \in K$.

Bob envoie des messages à Alice en utilisant l’algorithme de El Gamal.

1. Bob veut coder le message $M = 1 + \alpha$ pour l’envoyer à Alice, en utilisant $x = 3$. Que transmet-il à Alice ?
2. Même question avec $M = \alpha^3 + \alpha$ et $x = 4$.
3. Vous décidez de casser le code d’Alice. Ceci fait, vous interceptez le message $(\alpha^3, \alpha^3 + \alpha^2 + \alpha)$ i.e. le couple $(\alpha^x, Ma^x)$. Quel était le message $M$ de Bob ?

Exercice 3.6 Soit $Q = X^3 - X + 1 \in \mathbb{F}_3[X]$. On note $L = \mathbb{F}_3[X]/Q.\mathbb{F}_3[X]$ et $\beta$ la classe de $X$ dans $L$.

1. Montrer $Q$ est irréductible dans $\mathbb{F}_3[X]$.
2. Montrez que $L$ est un corps. Combien possède-t-il d’éléments ?
3. Calculer $\beta^3$, $\beta^9$ puis $\beta^{12}$ et montrer enfin que $\beta^{13} = -1$.
4. Montrer $\beta$ est un générateur de $L^*$.

Exercice 3.7 On utilise le corps $L$ et son générateur $\beta$ construit à l’exercice 3.6.

Alice et Bob décident de fabriquer une clé $\gamma$ à l’aide du protocole de Diffie-Helman et d’échanger des messages cryptés avec cette clé.

Alice choisit $a = 9$. Bob choisit un entier $b$ et envoie à Alice $\beta^b = -\beta^2 + \beta - 1$. 
1. Calculer la clé secrète $\gamma$ d’Alice et Bob ?

2. Alice souhaite faire passer à Bob le message $M = \beta^2 - 1$. Elle lui transmet le message crypté $C = M\gamma$. Calculer $C$.

3. En réponse, Alice reçoit le message crypté $C' = -\beta$. Quel est le message $M'$ de Bob ?

**Exercice 3.8** On considère le cryptosystème (sans clé) suivant : un grand nombre entier $p$ est public ; les messages sont des éléments de $(\mathbb{F}_p)^*$ (représentés par des entiers $M$ tels que $1 \leq M \leq p - 1$) ; si Alice veut envoyer un message $M$ à Bob, ils procèdent comme suit :

(a) Alice choisit un entier $a$ premier avec $p - 1$ et tel que $1 < a < p - 1$.
Elle envoie à Bob $C = M^a \in (\mathbb{F}_p)^*$.

(b) Bob choisit un entier $b$ premier avec $p - 1$ et tel que $1 < b < p - 1$.
Il envoie à Alice $D = C^b \in (\mathbb{F}_p)^*$.

(c) Alice calcule l'inverse $a'$ de $a$ dans $\mathbb{Z}/(p - 1)\mathbb{Z}$.
Elle renvoie à Bob $E = D^{a'} \in (\mathbb{F}_p)^*$.

(d) Bob calcule l'inverse $b'$ de $b$ dans $\mathbb{Z}/(p - 1)\mathbb{Z}$.
Il calcule enfin $F = E^{b'} \in (\mathbb{F}_p)^*$.

On admettra (cf. le cours) que si $a \in (\mathbb{F}_p)^*$, alors $a^{p-1} = 1$.

1. Montrer que $F = M$.

2. Faire les calculs pour $p = 47$, $a = 5$, $b = 11$ et $M = 10$.
(La table de multiplication de $\mathbb{F}_{47}$ est donnée en annexe.)
Table de multiplication de $\mathbb{F}_{47}$