



RSA, ECC

Version du 11 avril 2025

TD

1 RSA

Exercice 1 – C’est dans les détails que se cache le diable !

Un cryptosystème a beau se baser sur des principes mathématiques très forts, il suffit que le cryptosystème soit mal utilisé pour que la sécurité escomptée soit mise à mal. C’est ce que nous allons voir sur la signature RSA.

Alice a mis à la disposition du public les clés publiques n et e du cryptosystème RSA. Elle garde secret l’exposant de déchiffrement d .

Pour signer un document $1 < m < n$, Alice associe à m la signature $s_m = m^d \bmod n$ et envoie le couple (m, s_m) à ses interlocuteurs. Ces derniers peuvent alors vérifier l’identité de l’expéditeur du message m en vérifiant que $m = s_m^e \bmod n$.

Où l’on demande à Alice de chiffrer n’importe quoi !

1. Soit un message chiffré $c = m^e \bmod n$ pour Alice. L’attaquant Albert obtient c et veut pouvoir retrouver le message de départ m .

Montrer que si Albert sait qu’Alice utilise les mêmes clés (e, n) , (d, p, q) pour signer et chiffrer ses messages et qu’il est capable de la persuader de lui envoyer un message personnel de la forme xc à signer (donc avec les clés (d, n)) alors il pourra retrouver le message de départ m . (Indication : x est le résultat d’un chiffré $r^e \bmod n$ à clair r choisi.)

2. Qu’en déduisez-vous sur l’utilisation de RSA ?

Où l’on partage ses secrets !

Un groupe de k amis ont décidé, pour se faciliter la vie, d’utiliser le même module n mais des exposants de chiffrement e_1, \dots, e_k différents.

1. Montrer que si un attaquant Albert connaît les messages chiffrés c_1 et c_2 d’un même message clair m pour des exposants e_1 et e_2 qui sont premiers entre eux alors il est facile pour Albert de retrouver m .
2. Qu’en déduisez-vous sur l’utilisation de RSA ?

Où l’on chiffre avant de signer !

Alice veut communiquer avec Bob de manière sûre. Pour cela elle explique publiquement qu’elle va chiffrer son message m avec les clés publiques (n_B, e_B) de Bob et elle signe ce message chiffré avec ses clés privées (n_A, d_A) . Ainsi elle envoie à Bob le couple chiffré-signature

$$c = m^{e_B} \bmod n_B, \quad s_m = (m^{e_B} \bmod n_B)^{d_A} \bmod n_A$$

1. Montrer qu’après réception, Bob pourra publier une nouvelle paire de clés publiques (n'_B, e'_B) permettant de prétendre la réception d’un message m' de son choix (avec quelques aménagements éventuellement) chiffré avec ces nouvelles clés et signé par Alice.
2. Qu’en déduisez-vous sur l’utilisation de RSA ?

Exercice 2 – Signer avec RSA et le DLP

1. Rappeler le principe de la signature utilisant RSA. Faire de même pour la signature DSA reposant sur le DLP.
2. Montrer que la vérification de la signature DSA est correcte.
3. **(Ce que SONY aurait du savoir !)** Montrer que si l'on connaît deux couples $(m_1, s_{m_1}), (m_2, s_{m_2})$ de message/-signature obtenus en utilisant DSA avec la même valeur aléatoire k_m alors on peut retrouver très facilement la clé secrète t .

Exercice 3 – RSA petit exposant de chiffrement (2010 ; 7 points)

Dans cet exercice on s'intéresse à une attaque sur RSA. On supposera tout au long de cet exercice que l'exposant de chiffrement e est égal à 3 quel que soit le module RSA N utilisé.

Scenario : Un même message m est chiffré et envoyé à 4 personnes différentes utilisant des modules RSA différents N_1, \dots, N_4 . On supposera donc que l'entier m est strictement inférieur à $\min(N_1, N_2, N_3, N_4)$.

1. Les N_i sont supposés premiers entre eux deux à deux. Dans le cas contraire, un attaquant pourrait-il retrouver facilement le message clair m ? Si oui expliquer l'attaque.
2. Soit c_1, \dots, c_4 les chiffrés du message m correspondant respectivement aux modules N_1, \dots, N_4 . Montrer que l'on peut contruire un entier c tel que $c = m^3 \pmod{N_1 \times N_2 \times N_3 \times N_4}$. Quelle est la complexité de ce calcul?
3. Montrer que l'entier m^3 est strictement inférieur à $(N_1 \times N_2 \times N_3 \times N_4)$.
4. Sachant que le calcul de la partie entière d'une racine cubique d'un entier a se fait en temps polynomial en $\log(a)$, donner une attaque permettant de retrouver m à partir c_1, \dots, c_4 (Vous argumenterez précisément). Cette attaque peut-elle encore fonctionner si le nombre de chiffrés c_i connus est moindre? Si oui combien en faut-il au minimum (argumentez votre réponse)? Si non, quelle est la raison?

Exercice 4 – RSA (extrait de 2013bis ; 3 points)

1. **(1 point)** Soit (n, e) une clé publique RSA. Pour $n = 21$, exhiber toutes les valeurs possibles pour e . Plus généralement, pour $n = pq$ donné, expliquer de manière concise comment choisir e judicieusement.
2. **(2 points)** Soit $n = 221$ un module RSA et $d = 121$ un exposant de déchiffrement. Déchiffrer le chiffré $C = 2$ en utilisant le CRT. Que pensez-vous d'un tel message?

2 Courbes elliptiques**Exercice 5 – Courbe elliptique**

Dans tout cet exercice, nous étudierons la courbe elliptique E définie sur le corps fini \mathbb{F}_{11} par l'équation

$$E : y^2 = x^3 + x + 9$$

1. Vérifiez qu'il s'agit bien d'une courbe elliptique.
2. Déterminez l'ensemble des points de E .
3. Montrer que E est de cardinal 8.
4. Montrer que les points $P_1 = (0, 3)$ et $P_2 = (6, 0)$ de E sont d'ordre 4 et 2 respectivement. Montrer que tout point de E peut s'écrire $[i]P_1 + [j]P_2$ avec i et j des entiers.
5. Montrer qu'il n'existe pas de point de E qui soit d'ordre 8.
6. Le groupe E est-il isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/8\mathbb{Z}$ ou aucun des deux? Justifiez votre réponse.

Exercice 6 – Courbe Elliptique (2013 ; 17 points)

Dans tout cet exercice, on s'intéresse à une courbe elliptique définie sur le corps fini $\mathbb{K} = \mathbb{F}_{17}$ et au groupe qui s'en déduit. Cette courbe est définie par l'équation

$$\mathcal{E} : y^2 = x^3 + 2x - 1$$

1. **(1.5 points)** Étant donné le tableau partiellement rempli qui suit. Dédurre, sans faire aucun calcul, le cardinal du groupe E construit à partir de \mathcal{E} et montrer que ce groupe possède trois points d'ordre 2. (Vous argumenterez précisément vos réponses.)

x	$z = x^3 + 2x - 1$	$\left(\frac{z}{17}\right)$	Points
0		1	
1	2	1	$(1, \pm 6)$
2	11	-1	\emptyset
3		1	
4		-1	
5		1	
6	6	-1	
7	16	1	$(7, \pm 4)$
8		0	
9	15	1	
10		1	
11		1	
12		0	
13		-1	
14	0	0	
15		1	
16	13	1	

2. **(1 point)** Soient D_1, D_2 et D_3 les trois points distincts d'ordre deux dans E . Montrer, sans faire aucun calcul, que $D_1 + D_2 = D_3$. Exhiber explicitement ces trois points.
3. **(3 points)** Soient a et b deux éléments, d'ordre respectif α et β , d'un groupe commutatif fini additif. Montrer que si $\text{pgcd}(\alpha, \beta) = 1$ alors $\text{ppcm}(\alpha, \beta)$ est l'ordre de l'élément $a + b$.
4. **(5 points)** Montrer que les points $P_1 = (9, 10)$ et $P_2 = (10, 4)$ sont respectivement d'ordre 4 et 3. Construire explicitement un point Q d'ordre 12.
5. **(3.5 points)** Soit $G = \{[k]Q : k = 1, \dots, 12\}$. Sachant qu'il existe D_i un point d'ordre 2 tel que $D_i \notin G$, montrer que

$$E \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$$

(indication : vous pourrez montrer qu'il n'y a pas d'élément d'ordre 24 dans E ou définir explicitement l'isomorphisme de groupe).

6. **(2 points)** En reprenant les mêmes notations que dans la question précédente. Montrer qu'il y a un unique point d'ordre 2 dans G . Exhiber explicitement un point D_i vérifiant la propriété de la question précédente.

Exercice 7 – Courbes elliptiques (2013bis ; 6 points)

Dans tout cet exercice, nous étudierons la courbe elliptique \mathcal{E} définie sur le corps fini \mathbb{F}_{11} par l'équation

$$\mathcal{E} : y^2 = x^3 + 2x + 2$$

1. **(1.5 points)** Montrer que le groupe E construit à partir de \mathcal{E} est de cardinal 9 et qu'il ne possède aucun élément d'ordre pair.
2. **(2 points)** Soit $P_1 = (2, 5)$ un élément de E . Calculer $[2]P_1$ et en déduire que P_1 est d'ordre 9. Donner la structure du groupe E (Argumenter votre réponse).

3. **(1.5 points)** Montrer, sans faire aucun calcul, que E ne contient que 2 points d'ordre 3 et montrer qu'ils sont opposés l'un de l'autre.
4. **(1 point)** Exhiber les deux points d'ordre 3 de la question précédente.

Exercice 8 – Courbes Elliptiques (2014bis ; 8 points)

Dans tout cet exercice on s'intéresse au groupe additif E défini à partir des points rationnels de la courbe elliptique définie par l'équation $y^2 = x^3 + 3x + 7$ sur \mathbb{F}_{11} .

1. **(0.5 point)** Justifiez qu'il s'agit bien d'une courbe elliptique.
2. **(3 points)** Donner, sous la forme de tableaux comme vus en cours/TD, l'ensemble des points rationnels définissant E . Montrer que E est de cardinal 10.
3. **(0.5 point)** Soit $P = (8, 2)$ et $Q = (5, 9)$; vérifier que ce sont bien deux points de E .
4. **(1.5 points)** Montrer que $P + Q$ est un point d'ordre 2.
5. **(1.5 points)** Sachant que $Q = [4]P$, montrer que P n'est ni d'ordre 2 ni d'ordre 5.
6. **(1 point)** Montrer que E est un groupe cyclique. Exhiber un générateur de ce groupe.

3 Symbole de Legendre

Exercice 9 – Symbole de Legendre et polynômes irréductibles

Dans tout cet exercice nous allons étudier le corps fini \mathbb{F}_{307} de cardinal l'entier premier 307.

1. En utilisant la réciprocité quadratique (et d'autres propriétés du symbole de Legendre), calculer les symboles $\left(\frac{13}{307}\right)$ et $\left(\frac{17}{307}\right)$.
2. Lorsque cela est possible, calculer une racine carrée de 17 et 13 dans \mathbb{F}_{307} . (Indication : 17 est d'ordre 3 dans \mathbb{F}_{307}^\times .)
3. Les polynômes $P_1 = X^2 - 13 \in \mathbb{F}_{307}[X]$ et $P_2 = X^2 - 17 \in \mathbb{F}_{307}[X]$ sont-ils irréductibles ? Si oui, démontrer le, sinon, donner une décomposition en facteurs irréductibles.

Exercice 10 – Être ou ne pas être carré...(2018bis – 5 points)

306 est-il un carré modulo 547 ? Vous justifierez en détail votre réponse.