# Examen de Cryptologie

# 24 juin 2019

# Durée 2h

**Auteurs**
Valérie Ménissier-Morain & Jérémy Berthomieu

Version du 21 juin 2019

*Le seul document autorisé est une feuille manuscrite A4 recto-verso.*
*L'utilisation d'un appareil électronique est proscrit pendant toute la durée de l'épreuve.*
*Le barème, sur 20, est indicatif.*

## Exercice 1 – Questions de cours – 4+ points

1. (**RSA – 2 points**)
   a. Donner les relations qui lient les différents paramètres utilisés dans RSA.

   **Solution :**
   Les paramètres de RSA sont
   - deux nombres premiers distincts $p$ et $q$ ;
   - un entier $n = pq$ ;
   - l'indicatrice d'Euler de $n$, $\varphi(n) = n - p - q + 1$ ;
   - un entier $d$ premier avec $\varphi(n)$ et son inverse $e$ modulo $\varphi(n)$.

   b. Parmi ces paramètres, lesquels sont publiques et lesquels restent secrets ?

   **Solution :**
   La clef publique est constituée de $n$ et $e$.
   La clef privée est constituée de $p$, $q$, $d$ et $\varphi(n)$.

   c. Décrire comment utiliser ces paramètres pour chiffrer un message clair $m$ et déchiffrer naïvement un message chiffré $c$.

   **Solution :**
   Pour chiffrer $m$, on calcule $c = m^e \bmod n$ en n'utilisant que la clef publique.
   Pour déchiffrer naïvement $c$, on calcule $m = c^d \bmod n$ en utilisant la clef privée $d$.

2. (**Signature – 2+ points**) Qu'est-ce que la signature en cryptologie ? Peut-on utiliser tous les cryptosystèmes pour signer ? Citer les cryptosystèmes vus en cours pour la signature et détaillez le fonctionnement d'au moins un de ces algorithmes de signature (comment signer un message, comment vérifier la signature et prouver la pertinence de cette signature).

**Solution :**

La signature sert à authentifier l'expéditeur d'un message.

On utilise un système de chiffrement et éventuellement une fonction de hachage. L'expéditeur du message signe son message avec sa clef privée, il transmet au destinataire le message lui-même et sa signature. Le destinataire utilise la clef publique de l'expéditeur correspondante pour vérifier que la signature correspond à ce message et cet expéditeur.

Il faut nécessairement utiliser un système de chiffrement asymétrique donc à clef publique pour que l'information de vérification de la signature ne puisse servir à signer d'autres messages.

Usuellement pour que la signature ait une taille raisonnable on signe non pas le message lui-même mais l'empreinte du message pour une fonction de hachage cryptographique connue.

En cours, ont été vus les algorithmes de signatures pour RSA (slides 53–55), DSA (slide 131) et ECDSA (tableau). L'exercice 11 du TD2 reprend la signature avec RSA et DSA.

Pour RSA, on utilise $N = pq$ un entier RSA, $(e, d)$ un couple d'exposants de chiffrement/déchiffrement choisis par l'expéditeur, l'expéditeur publie $(N, e)$ et signe le message $m$ par la signature $s = m^d \bmod N$. Le destinataire reçoit $(m, s)$ et vérifie que $s^r \bmod N = m$.

Pour DSA, l'expéditeur utilise une fonction de hachage $H$, deux premiers $p$, $q$ de tailles respectives 1024 et 160 bits tels que $p-1$ est un multiple de $q$, $g$ un entier d'ordre $q$ modulo $p$ et choisit un entier secret $t$ associé à un entier public $h = g^t \bmod p$ (DLP). Il publie $p, q, g, h$ et indique la fonction de hachage $H$ utilisée.

L'expéditeur choisit un entier $k_m$ au hasard (différent pour chaque message), calcule $r = (g^{k_m} \bmod p) \bmod q$ et $s = k^{-1} - m(H(m) + t \times r) \bmod q$. Si $rs \neq 0$ alors la signature de $m$ est le couple $(r, s)$ sinon on recommence avec une nouvelle valeur de $k_m$.

Le destinataire vérifiera l'authenticité de l'expéditeur en calculant $u_1 = H(m) \times s^{-1} \bmod q$, $u_2 = r \times s^{-1} \bmod q$, $v = (g^{u_1} h^{u_2} \bmod p) \bmod q$ et en vérifiant finalement que $v = r \bmod q$.

## Exercice 2 – Chiffrement et déchiffrement – 4 points

Dans cet exercice on apportera un soin particulier au principe et au detail du raisonnement.

1. (**Déchiffrement de Vigenère – 1 point**) Un message clair $m$ a été chiffré avec la clef `RATTRAPAGE` pour chiffrement de Vigenère, ce qui donne le message chiffré `CAVKP PIORS XIXXJ TAAYG ZEGVV DJSKG IEM`. Quel est le message $m$ ?

**Solution :**

On numérote les caractères de l'alphabet pour mémoire lors des calculs :

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

La clef a 10 caractères, on écrit donc le texte sur 10 colonnes :

```
  CAVKPPIORS XIXXJTAAYG ZEGVVDJSKG IEM
- RATTRAPAGE RATTRAPAGE RATTRAPAGE RAT
------------
  LACRYPTOLO GIEESTLASC IENCEDUSEC RET
```

explication pour le premier caractère : `C` en position 2 modulo 26 soit $2 + 26 = 28$ a été décalé de `R` en position 17 donc de 17 position, son clair correspond donc au caractère en position $28 - 17 = 11$ modulo 26 soit `L`.

Le message $m$ était donc *La cryptologie est la science du secret.*

2. (**Chiffrement de Playfair – 3 points**) Chiffrer ce message $m$ avec le carré de Playfair :

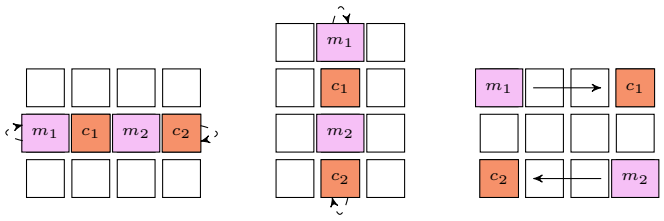
| | | | | |
|---|---|---|---|---|
| H | O | W | T | K |
| Y | U | D | X | V |
| N | B | F | L | C |
| E | S | I | R | A |
| G | Z | Q | P | M |

S'il est nécessaire d'avoir recours à du *padding*, on utilisera pour ce faire le caractère `X` comme vu en cours.

**Solution :**

Rappelons le principe : on décompose le texte par blocs de 2 caractères. Soit ces caractères sont identiques, soit ils sont placés dans le carré sur la même ligne ou la même colonne, soit ils sont sur des lignes et des colonnes différentes, formant ainsi un rectangle.

Dans le schéma ci-dessous on décrit la règle qui s'applique à chacun de ces cas : on doit chiffrer les caractères sur les cases violettes en leur substituant les caractères placés sur les cases couleur saumon.




Règle ligne wrap si nécessaire — Règle colonne wrap si nécessaire — Règle rectangle

S'il ne reste qu'un seul caractère à chiffrer ou si les deux caractères sont identiques : on ajoute une lettre neutre telle que X après le premier caractère et on applique à nouveau les règles à partir du premier caractère.

Passons au chiffrement demandé. On découpe ce texte par blocs de 2 caractères :

`LA CR YP TO LO GI EE ST LA SC IE NC ED US EC RE T`

Les deux lettres du bloc `LA` se trouvent disposés en rectangle dans le carré de Playfair, on y associe les lettres disposées aux deux autres coins de ce rectangle ce qui donne le bloc `CR`.

Évidemment réciproquement le bloc suivant `CR` est chiffré en le bloc `LA`.

On chiffre de la même façon `YP` en `XG`.

Pour le bloc suivant, `TO`, les deux caractères se trouvent sur la même ligne, on associe donc à chacun le caractère situé à sa droite sur cette ligne, ce qui nous donne `KW`.

On chiffre `LO` et `GI` avec la règle pour un bloc rectangle, ce qui donne `BT` et `QE` respectivement.

Le bloc suivant est composé des deux mêmes caractères donc on introduit un `X` entre les deux, ce qui nous donne à partir de là

`EX ES TL AS CI EN CE DU SE CR ET`

Pour terminer

| Clair | Règle | Chiffré |
|---|---|---|
| EX | rectangle | RY |
| ES | ligne | SI |
| TL | colonne | XR |
| AS | ligne | EI |
| CI | rectangle | FA |
| EN | colonne | GE |
| CE | rectangle | NA |
| DU | ligne | XD |
| SE | ligne | IS |
| ET | rectangle | RH |

et on reconstitue le chiffré

LA CR YP TO LO GI EX ES TL AS CI EN CE DU SE CR ET
CR LA XG KW BT QE RY SI XR EI FA GE NA XD IS LA RH

soit avec le formatage usuel CRLAX GKWBT QERYS IXREI FAGEN AXDIS LARH.

## Exercice 3 – Corps finis I – 2,75 points

Soit $p$ un nombre premier impair.

1. (**0,25 point**) Montrer que 2 est inversible dans $\mathbb{F}_p$.

**Solution :**
$\mathbb{F}_p$ étant un corps, tous les éléments non nuls de $\mathbb{F}_p$ sont inversibles, y compris 2 puisque $p > 2$.

2. (**0,5 point**) Montrer que le polynôme $P = x^2 + bx + c \in \mathbb{F}_p[x]$ admet des racines dans $\mathbb{F}_p$ si, et seulement si, $b^2 - 4c$ est un carré dans $\mathbb{F}_p$.

**Solution :**
$P = \left(x + 2^{-1}b\right)^2 - 4^{-1}b^2 + c = \left(x + 2^{-1}b\right)^2 - 4^{-1}(b^2 - 4c)$ de sorte que $P = 0$ est équivalent à $\left(x + 2^{-1}b\right)^2 = 4^{-1}(b^2 - 4c)$.
Autrement dit, $P = 0$ si, et seulement si, $4^{-1}(b^2 - 4c)$ est un carré dans $\mathbb{F}_p$, si, et seulement si, $b^2 - 4c$ est un carré dans $\mathbb{F}_p$.

3. (**1 point**) Résoudre l'équation $x^2 + 3x + 4 = 0$ dans $\mathbb{F}_7$, $\mathbb{F}_{11}$ et $\mathbb{F}_{13}$.

**Solution :**
On calcule $\Delta = b^2 - 4c = 9 - 16 = -7$.
- Dans $\mathbb{F}_7$, $\Delta = 0$ donc l'équation a une solution double $x_0 = -2^{-1}b = -2^{-1} \times 3$. Or, $2^{-1} = 4$ donc $x_0 = -12 = 2$.
- Dans $\mathbb{F}_{11}$, $\Delta = 4 = 2^2$ donc l'équation a deux solutions simples $x_1 = -2^{-1}(b + \sqrt{\Delta}) = -2^{-1}(3 + 2) = -2^{-1} \times 5$ et $x_2 = -2^{-1}(b - \sqrt{\Delta}) = -2^{-1}$. Or, $2^{-1} = 6$ donc $x_1 = 3$ et $x_2 = 5$.
- Dans $\mathbb{F}_{13}$, $\Delta = 6$. Or, les carrés de $\mathbb{F}_{13}$ sont $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 = 3$, $(\pm 5)^2 = 12$, $(\pm 6)^2 = 10$, donc $\Delta$ n'est pas un carré et l'équation n'a pas de solutions dans $\mathbb{F}_{13}$.

4. (**0,75 point**) Parmi les anneaux $\mathbb{F}_7[x]/(x^2 + 3x + 4)$, $\mathbb{F}_{11}[x]/(x^2 + 3x + 4)$ et $\mathbb{F}_{13}[x]/(x^2 + 3x + 4)$, lesquels sont des corps ?

**Solution :**
L'anneau $\mathbb{F}_p[x]/(P)$ est un corps si, et seulement si, $P$ est irréductible dans $\mathbb{F}_p[x]$.
Or, un polynôme de degré 2 est irréductible dans $\mathbb{F}_p[x]$ si, et seulement si, il n'a pas de racines dans $\mathbb{F}_p$.
D'après la question précédente, $x^2+3x+4$ n'est irréductible que dans $\mathbb{F}_{13}[x]$ donc seul $\mathbb{F}_{13}[x]/(x^2+3x+4)$ est un corps. Il s'agit de $\mathbb{F}_{13^2} = \mathbb{F}_{169}$.

## Exercice 4 – Corps finis II – 4,75 points

Soit $\mathbb{F}_q$ un corps fini avec $q = p^r$, $p$ un nombre premier et $r \in \mathbb{N}^*$.

1. (**0,5 point**) Quel est l'ordre du groupe des inversibles de $\mathbb{F}_q$ ? Ce groupe est-il cyclique ?

**Solution :**
L'ordre est $q-1$ et le groupe est toujours cyclique.

2. (**0,25 point**) On suppose que $p > 2$. À quelle condition $q-1$ est-il premier ?

**Solution :**
Si $p > 2$, alors $q$ est impair et $q-1$ est pair. Ainsi, $q-1$ est premier si, et seulement si, $q-1 = 2$, $q = 3$.

3. (**0,5 point**) Montrer que $x-1$ divise $x^r - 1$.

**Solution :**
On a $(x-1)(x^{r-1} + \cdots + x + 1) = x^r - 1$.

4. (**0,75 point**) En déduire que $2^s - 1$ divise $2^{sr} - 1$ et que donc $2^r - 1$ ne peut être premier que si $r$ l'est.

**Solution :**
En substituant $2^s$ à $x$ dans la question précédente, on en déduit le résultat.
Si $r$ se factorise en $r = st$ avec $s, t > 1$, alors $2^r - 1 = (2^s)^t - 1 = (2^s - 1)\left((2^s)^{t-1} + \cdots + 2^s + 1\right)$ et aucun des deux facteurs n'est trivial. Par contraposée, on en déduit le résultat.

5. (**2,5 points**) Donner la liste des corps finis $\mathbb{F}_q$, avec $q < 3000$, tels que $\mathbb{F}_q^*$ est d'ordre premier.

**Solution :**
D'après les questions précédentes, on sait que l'on ne peut avoir comme valeurs de $q$ que 3, $2^2 = 4$, $2^3 = 8$, $2^5 = 32$, $2^7 = 128$ et $2^{11} = 2048$.
De plus, il est clair que $3 - 1 = 2$, $2^2 - 1 = 3$, $2^3 - 1 = 7$ et $2^5 - 1 = 31$ sont premiers.
Pour $2^7 - 1 = 127$, tester sa divisibilité par 3, 5, 7 et 11 nous assure qu'il est premier.
Pour $2^{11} - 1 = 2047$, tester sa divisibilité par 3, 5, 7, 11, 13, 17, 19 et 23 nous amène à remarquer que $2047 = 23 \times 89$ et qu'il n'est donc pas premier.
Il en résulte que $\mathbb{F}_q^*$ est d'ordre premier pour $q < 3000$ si, et seulement si, $q \in \{3, 2^2, 2^3, 2^5, 2^7\}$.

## Exercice 5 – Courbe Elliptique – 4,5 points

Dans tout cet exercice, on s'intéresse à une courbe elliptique définie sur le corps fini $\mathbb{K} = \mathbb{F}_7$ et au groupe qui s'en déduit. Cette courbe est définie par l'équation

$$\mathcal{E} : \; y^2 = x^3 + 2x + 4$$

1. (**0,5 point**) Donnez, sous la forme d'un tableau, la correspondance entre les images et les antécédents de l'application de $\mathbb{K}$ dans $\mathbb{K}$ qui à un élément $a$ fait correspondre son carré $a^2$.

**Solution :**

| $x$ | $x^2$ |
|---|---|
| 0 | 0 |
| $\pm 1$ | 1 |
| $\pm 2$ | 4 |
| $\pm 3$ | 2 |

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

| $x$ | $z = x^3z = x^3 + 2x + 4$ | $\left(\frac{z}{7}\right)$ | Points |
|---|---|---|---|
| 0 | | 1 | $(0, \pm 2)$ |
| 1 | 0 | 0 | |
| 2 | 2 | | $(2, \pm 3)$ |
| 3 | 2 | | |
| 4 | | $-1$ | |
| 5 | 6 | | $\emptyset$ |
| 6 | | | $(6, \pm 1)$ |

**Solution :**

- Pour la ligne $x = 0$, le symbole de Legendre est égal à 1 et il y a deux points.
- Pour la ligne $x = 1$, le symbole de Legendre est égal à 0 et il correspond à un seul point d'ordre 2.
- Pour la ligne $x = 2$, $z = 2$ et il y a deux points.
- Pour la ligne $x = 3$, $z = 2$ donc comme au-dessus, il y a deux points. Alternativement, le symbole de Legendre est égal à 1 par la question précédente.
- Pour la ligne $x = 4$, le symbole de Legendre est égal à $-1$, il ne correspond donc à aucun point.
- Pour la ligne $x = 5$, il n'y a aucun point.
- Pour la ligne $x = 6$, il y a deux points.

Cela fait donc $2 + 1 + 2 + 2 + 0 + 0 + 2 = 9$ points rationnels et il reste le point à l'infini, ce qui nous fait 10 points sur cette courbe elliptique.

Pour information, le tableau complet est

| $x$ | $z = x^3 + 2x + 4$ | $\left(\frac{z}{7}\right)$ | Points |
|---|---|---|---|
| 0 | 4 | 1 | $(0, \pm 2)$ |
| 1 | 0 | 0 | $(1, 0)$ |
| 2 | 2 | 1 | $(2, \pm 3)$ |
| 3 | 2 | 1 | $(3, \pm 3)$ |
| 4 | 6 | $-1$ | $\emptyset$ |
| 5 | 6 | $-1$ | $\emptyset$ |
| 6 | 1 | 1 | $(6, \pm 1)$ |

3. (**1 point**) À l'aide du théorème de structure, montrer que $(E, +)$ est un groupe cyclique.

**Solution :**

Par le théorème de structure, $(E, +) \simeq (\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}, +)$ avec $d_1 | (q-1)$, $d_1 | d_2$ et $d_1 d_2 = |E|$.

Or $q - 1 = 6$ et $|E| = 10$ donc $d_1 | \operatorname{pgcd}(6, 10) = 2$. Mais si $d_1 = 2$, alors $d_2 = 5$ et $d_1 \nmid d_2$ donc $d_1 = 1$ et $d_2 = 10$.

Autrement dit $(E, +) \simeq (\mathbb{Z}/10\mathbb{Z}, +)$, qui est cyclique.

4. (**1 point**) Sans calcul et sans justifier lequel, montrer que parmi les points de $\mathcal{E}$ donnés à la question 2, au moins un engendre $E$.

**Solution :**

Comme $E$ est d'ordre 10, $\varphi(10) = 4$ points engendrent $E$.

À la question 2, on peut lire 6 points de $E$, auxquels on rajoute le point d'ordre 2 (d'abscisse 1), le point à l'infini et les deux points d'abscisse 3. Or, ni le point d'ordre 2, ni le point à l'infini n'engendre $E$ donc parmi les 4 points qui engendrent $E$, au moins 2 sont déjà dans le tableau.