Partiel de Cryptologie

16 mars 2022
Durée 1h30

Auteurs
Valérie Ménissier-Morain, Jérémy Berthomieu, Maxime Roméas

Version du 22 avril 2022

Le seul document autorisé est une feuille manuscrite A4 recto-verso.
L'utilisation d'un appareil électronique est proscrite pendant toute la durée de l'épreuve.
Le barème sur 32 points est indicatif. La note finale sera le minimum entre les points obtenus et 20.

Exercice 1 – Questions diverses – 5,5 points + 1 point bonus

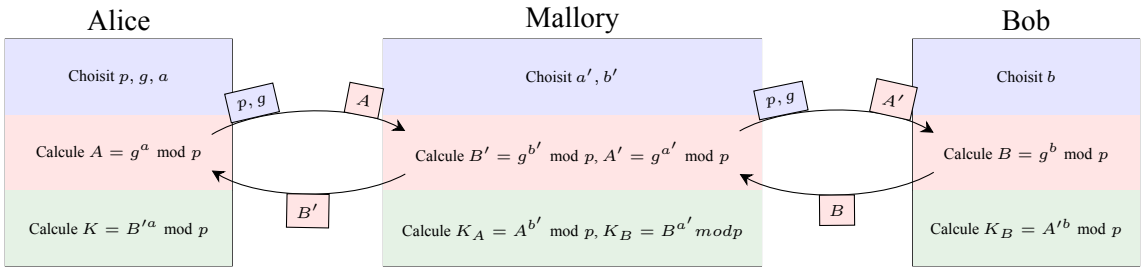
1. (**1 point principe – 1 point bonus schéma**) Quel principe de sécurité est violé par le concept *Man In The Middle* ? Vous en expliquerez le mécanisme sur un exemple.

Solution :

Authentification : un intrus s'introduit entre deux personnes en se faisant passer pour l'une à la place de l'autre dans leurs échanges.

De plus l'interception rompt aussi le principe de confidentialité et l'interposition celui d'intégrité des messages.

Exemple pour l'échange de clef de Diffie-Hellman-Merkle :



Mallory intercepte les échanges d'Alice et Bob et peut se faire passer pour l'un à la place de l'autre.

2. (**0.5 point**) Pourquoi ne peut-on pas utiliser la technique des indices de coïncidence et indices de coïncidence mutuelle pour déterminer la clé de chiffrement ou le texte clair correspondant à un texte chiffré par substitution ?

Solution :

Parce que ces opérateurs statistiques sont invariants par substitution. Quand bien même on pourrait énumérer toutes les substitutions possibles en un temps raisonnable (ce qui n'est pas le cas), tous les textes déchiffrés ainsi obtenus partagent le même indice de coïncidence, qui est celui du chiffré, donc il n'est pas possible d'identifier lequel est le clair à partir de cette information.

3. (**1 point**) Expliquez pourquoi la méthode de corrélation de Pearson donne de meilleurs résultats que la méthode des indices de coïncidence pour la cryptanalyse de Vigenère.

Solution :
Parce que pour terminer la cryptanalyse avec la méthode des IC on s'appuie uniquement sur le caractère le plus fréquent du texte en supposant qu'il correspond au caractère le plus fréquent de la langue.
En revanche pour la corrélation de Pearson, on essaie de faire correspondre non seulement les caractères les plus fréquents du texte chiffré et de la langue mais la distribution complète des fréquences.

4. (**Algorithme d'Euclide étendu – 3 points**) En utilisant l'algorithme d'Euclide étendu, dites si $a = 819$ est inversible modulo $n = 861$? Si oui quel est son inverse ? Est-ce un diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$? Si oui exhibez un témoin de diviseur de zéro de a pour n.
Mêmes questions pour $n = 859$.
Vous justifierez rigoureusement vos réponses.

Solution :
On va appliquer l'algorithme d'Euclide étendu à$n = 861$ et $a = 919$ (puis $n = 859$).
Dans le tableau suivant chaque ligne à partir de la ligne $i = 1$ se lit :
- la partie gauche (colorée en rose), si $r_i \neq 0$, la division euclidienne de r_{i-1} par r_i est $r_{i-1} = q_i * r_i + r_{i+1}$ qui définit le quotient $q_i = \lfloor \frac{r_{i-1}}{r_i} \rfloor$ et le reste suivant $r_{i+1} = r_{i-1} - q_i * r_i$; sinon on s'arrête.
- pour la partie droite (colorée en jaune), $u_{i+1} = u_{i-1} - q_i * u_i$ et $v_{i+1} = v_{i-1} - q_i * v_i$
- avec l'initialisation (partie en haut, colorée en bleu) : $r_0 = a$, $r_1 = b$, $u_0 = v_1 = 1$, $v_0 = u_1 = 0$
- à chaque étape on a $r_i = u_i\, n + v_i\, a \ \ \forall i$.

On exploite cette information sur les deux dernières lignes du tableau (cadres rouge et vert) :
- avant-dernière ligne (de numéro k), on trouve r_{k+1} (dans la cinquième colonne) le dernier reste positif, c'est-à-dire le pgcd de n et a et $r_{k+1} = u_{k+1}\, n + v_{k+1}\, a$ est une relation de Bézout.
  Si $r_{k+1} = 1$, alors v_{k+1} mod n est l'inverse de a modulo n, a n'est pas diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$.
- à la dernière ligne (de numéro $k+1$ donc), on trouve $0 = r_{k+2} = n\, u_{k+2} + a\, v_{k+2}$.
  Si $r_{k+1} > 1$, alors a n'est pas inversible modulo n, c'est un diviseur de 0 dans $\mathbb{Z}/n\mathbb{Z}$, $|v_{k+2}| < n$ donc v_{k+2} est un témoin de diviseur de 0 pour a dans $\mathbb{Z}/n\mathbb{Z}$.

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
-1					1	0
0			861	819	0	1
1	861	1	819	42	1	-1
2	819	19	42	21	-19	20
3	42	2	21	0	39	-41

Ici $k = 2$, on constate que pgcd$(a, n) = r_{k+1} = 21 > 1$ donc a n'est pas inversible modulo n, c'est un diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$ de témoin $v_{k+2} = -41$.
On procède de la même façon pour $n = 859$.

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
-1					1	0
0			859	819	0	1
1	859	1	819	40	1	-1
2	819	20	40	19	-20	21
3	40	2	19	2	41	-43
4	19	9	2	1	-389	408
5	2	2	1	0	819	-859

Ici $k = 4$, on constate que pgcd$(a, n) = r_{k+1} = 1$ donc a est inversible modulo n d'inverse $v_{k+1} = 408$. 819

n'est pas diviseur de zéro pour 859.

Exercice 2 – Message chiffré – 3 points pour le raisonnement + 2 points pour le message déchiffré

En 1627 commence le siège de La Rochelle, cité huguenote, par le roi de France. L'armée du Roi assiège la ville en bloquant tout d'abord tout ravitallement par voie de terre puis par la construction d'une digue en contrôlant l'accès du port.

Le maire de La Rochelle appelle leur allié anglais à la rescousse par le message suivant chiffré par la méthode de Vigenère

```
PMYMM UMRYV RQJYJ UITWI QWAMI QKKLG OMJYX RCZYT DZZHS XABIY
VLKGE QLUHW DAYCW WITWI SWALV RUVLI FMHFS FCYME QAJYP DQMIH
HNXIC PIOLI GMRUV RKNYP OM
```

Saurez-vous dire quel est le contenu de ce message ?
Vous détaillerez votre raisonnement.

Solution :

On effectue une attaque par clair probable. On s'attend à trouver `La Rochelle`, au début ou à la fin du message, en espérant que la clef n'est pas aussi longue que ce mot.

Le début du texte peut contenir La Rochelle (ou une formule de politesse pour s'adresser à son interlocuteur au duc, mais la formule employée n'est pas évidente), on cherche donc La Rochelle au début du texte.

On regarde les 10 premiers caractères (10=longueur de la chaîne `LAROCHELLE` :

```
  PMYMM UMRYV
- LAROC HELLE
-------------
= EMHYK NHGNR
```

On ne s'embarrassait pas d'une clef incompréhensible donc cela semble mal parti, inutile d'essayer le déchiffrer le reste.

On essaie donc cette même chaîne de caractères à la fin du texte :

```
  RUVRK NYPOM
- LAROC HELLE
-------------
= GUEDI GUEDI
```

On en déduit que la clé est de longueur 5 et est le mot `DIGUE`, le message est donc

```
MESSI RELER OIDEF RANCE NOUSE NCERC LEDET OUTEP ARTNO USVOU
SDEMA NDONS ASSIS TANCE POURR OMPRE CEBLO CUSSA NSDEL AIGOD
EFROY MAIRE DELAR OCHEL LE
```

ou en rétablissant la forme de la phrase :
Messire, le Roi de France nous encercle de toute part. Nous vous demandons assistance pour rompre ce blocus sans délai. Godefroy, maire de La Rochelle.

Et qu'est-ce que les outils automatiques que nous avons élaborés en TME auraient produit sur ce cryptogramme de 122 caractères ? la méthode de la corrélation de Pearson marche parfaitement ; en revanche les méthodes qui s'appuient sur les indices de coïncidence trouvent la bonne longueur de clé mais un seul caractère de la clé est correct.

Exercice 3 – Groupe fini – 12 points + 1,5 point de bonus

On considère l'ensemble $\mathcal{E}$ muni de la loi $\circ$, supposée associative. Les éléments de $\mathcal{E}$ sont tous de la forme $P = (x, y)$ avec x et y modulo 13 sauf un, noté $\mathcal{O}$. De plus, $P = (x, y) \in \mathcal{E}$ si, et seulement si, $y^2 = x^3 + 3x + 5 \mod 13$.

1. **(1 point)** Vérifier que $(1, 3), (4, 4), (12, 12) \in \mathcal{E}$.

Solution :
- $1^3 + 3 \times 1 + 5 = 9$ et $3^2 = 9$;
- $4^3 + 3 \times 4 + 5 = (16 + 3) \times 4 + 5 = 6 \times 4 + 5 = 3$ et $4^2 = 16 = 3$;
- $12^3 + 3 \times 12 + 5 = (-1)^3 + 3 \times (-1) + 5 = 1$ et $12^2 = (-1)^2 = 1$.

On admet dans la suite qu'avec $(1, 10), (4, 9), (11, 2), (11, 11), (12, 1)$, ce sont les seuls éléments de $\mathcal{E} - \{\mathcal{O}\}$.

2. **(0,5 point)** Pour $P, Q \in \mathcal{E}$, on note $R = P \circ Q \in \mathcal{E}$. De plus,

(i). si $Q = \mathcal{O}$, alors $R = P$, sinon si $P = \mathcal{O}$, alors $R = Q$;

(ii). sinon, si $P = (x_1, y_1)$ et $Q = (x_1, -y_1)$, alors $R = \mathcal{O}$;

(iii). sinon, $P = (x_1, y_1)$, $Q = (x_2, y_2) \neq (x_1, -y_1)$ et $R = (x_3, y_3)$ avec

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$$

et $\lambda = 8(x_1^2 + 1)y_1^{-1} \mod 13$ si $P = Q$ ou $\lambda = (y_2 - y_1)(x_2 - x_1)^{-1} \mod 13$ sinon.

Quel est le neutre pour $\circ$? Quel est l'inverse de $P \in \mathcal{E}$ pour $\circ$?

Solution :
Par la propriété (i), $\mathcal{O}$ est le neutre.
Donc si $P = \mathcal{O}$, alors naturellement il est son propre inverse. Sinon, la propriété (ii) nous dit que l'inverse de (x_1, y_1) est $(x_1, -y_1)$.

3. **(1 point)** Montrer que $(\mathcal{E}, \circ)$ est un groupe.

Solution :
Par hypothèse, si $P, Q \in \mathcal{E}$, alors $P \circ Q \in \mathcal{E}$ et $\circ$ est associative. De plus, $\circ$ admet un élément neutre $\mathcal{O}$ et pour tout $P \in \mathcal{E}$, il existe un inverse de P, noté P^{-1}, tel que $P \circ P^{-1} = \mathcal{O}$. Ainsi $(\mathcal{E}, \circ)$ est un groupe.

4. **(2 points+1 point bonus)** Justifier, de deux manières distinctes, s'il existe ou non des éléments d'ordre 2 dans $\mathcal{E}$.

Solution :
Un point P est d'ordre 2 si $[2]P = P \circ P = \mathcal{O}$.
D'après la propriété (ii), ceci est équivalent à $P = (x_1, 0)$.
Or, il n'existe aucun point de cette forme dans $\mathcal{E}$ donc il n'existe pas de point d'ordre 2 dans $\mathcal{E}$.

Par la question 1, $\mathcal{E} = \{\mathcal{O}, (1, 3), (1, 10), (4, 4), (4, 9), (11, 2), (11, 11), (12, 1), (12, 12)\}$ donc $\mathcal{E}$ est d'ordre 9. Les ordres possibles, par le corollaire du théorème de Lagrange, des éléments de $\mathcal{E}$ sont tous les diviseurs de $|\mathcal{E}| = 9$, à savoir 1, 3 et 9. Il n'existe donc pas de point d'ordre 2 dans $\mathcal{E}$.

5. **(3,5 points)** Montrer que $\circ$ est commutative.

Solution :
Il faut montrer que $P \circ Q = Q \circ P$.
C'est vrai si P ou Q est $\mathcal{O}$.
Si $Q = P$ ((i)), c'est évident donc on peut supposer $Q \neq P$.
Si P et Q sont d'ordonnées opposées ((ii)), $R = P \circ Q = \mathcal{O}$ et $S = Q \circ P = \mathcal{O}$.
On peut donc supposer que P et Q sont distincts et d'ordonnées non nulles et non opposées.
Par définition, si $P = (x_1, y_1)$, $Q = (x_2, y_2) \neq (x_1, -y_1)$ alors :

- $R = P \circ Q = (x_3, y_3)$ avec $x_3 = \lambda^2 - x_1 - x_2$, $\quad y_3 = \lambda(x_1 - x_3) - y_1$ et $\lambda = (y_2 - y_1)(x_2 - x_1)^{-1}$ mod 13.
- $S = Q \circ P = (x_4, y_4)$ avec $\quad x_4 = \mu^2 - x_2 - x_1$, $\quad y_4 = \mu(x_1 - x_4) - y_2$ et $\mu = (y_1 - y_2)(x_1 - x_2)^{-1}$ mod 13.

$\mu = (y_1 - y_2)(x_1 - x_2)^{-1}$ mod $13 = (y_2 - y_1)(x_2 - x_1)^{-1}$ mod $13 = \lambda$.
Par conséquent $x_4 = \lambda^2 - x_1 - x_2 = x_3$.
Il reste à montrer que $y_4 = \lambda(x_2 - x_3) - y_2 = y_3$. On calcule $y_3 - y_4 = \lambda(x_1 - x_3) - y_1 - \lambda(x_2 - x_3) + y_2 = \lambda(x_1 - x_2) - (y_1 - y_2) = (y_2 - y_1)(x_2 - x_1)^{-1}(x_1 - x_2) - (y_1 - y_2) = 0$.
Donc $S = R$ et $\circ$ est commutative.

6. **(1,5 point +0,5 point de bonus si (ii) dûment invoqué pour conclure)** Soient $P_0 = (4, 4)$ et $P_1 = (4, 9)$ dans $\mathcal{E}$. Montrer que $[3]P_i = P_i \circ P_i \circ P_i = \mathcal{O}$ pour $i \in \{0, 1\}$.

Solution :
On note $P_i = (4, y_1)$ et $[2]P_i = (x_2, y_2)$.
Par la propriété (iii), on calcule $\lambda = 8(4^2 + 1)y_1^{-1}$ mod $13 = 6y_1^{-1}$ mod 13. Si $y_1 = 4$, alors $y_1^{-1} = 10$ et $\lambda = 8$. Si $y_1 = 9 = -4$, alors $y_1^{-1} = 3$ et $\lambda = 5$. On a alors $x_2 = \lambda^2 - 2x_1 = 12 - 2 \times 4 = 4$. Et $y_2 = \lambda(x_1 - x_2) - y_1 = \lambda(4 - 4) - y_1 = -y_1$. Donc si $y_1 = 4$, alors $y_2 = -4 = 9$ et si $y_1 = 9$, alors $y_2 = -9 = 4$.
Autrement dit, $[2]P_i = [-1]P_i = P_{i+1 \bmod 2}$ par la propriété (ii).
Par la propriété (ii), $[3]P_i = P_i \circ [2]P_i = (4, y_1) \circ (4, -y_1) = \mathcal{O}$ donc P_i est d'ordre 3.

7. **(1,5 point)** Soit $Q = (12, 12)$. Montrer que $[3]Q = P_1$.

Solution :
On note $Q = (x_3, y_3)$, $[2]Q = (x_4, y_4)$ et $[3]Q = (x_5, y_5)$
On commence par calculer $[2]Q$. On a $\lambda = 8(12^2 + 1)12^{-1}$ mod $13 = 8 \times 2 \times 12$ mod $13 = -16 = 10$. De sorte que $x_4 = \lambda^2 - 2x_3 = 10^2 - 2 \times 12 = 11$ et $y_4 = \lambda(x_3 - x_4) - y_3 = 10(12 - 11) - 12 = 11$.
On calcule ensuite $[3]Q = Q + [2]Q$. On a $\mu = (y_4 - y_3)(x_4 - x_3)^{-1}$ mod $13 = (11 - 12)(11 - 12)^{-1}$ mod $13 = 1$. De sorte que $x_5 = \mu^2 - x_3 - x_4 = 1^2 - 11 - 12 = 4$ et $y_5 = \mu(x_3 - x_5) - y_3 = 1(12 - 4) - 12 = 9$. Donc $[3]Q = (4, 9) = P_1$.

8. **(1 point)** $(\mathcal{E}, \circ)$ est-il cyclique ?

Solution :
Le point Q n'est pas d'ordre 1 ni d'ordre 3, il est donc nécesairement d'ordre 9. Ainsi, il engendre $\mathcal{E}$ et $\mathcal{E}$ est cyclique.

Exercice 4 – Divisibilité et PGCD – 7 points

Soient $a, b \in \mathbb{N}$ tels que $0 < a < b$.

1. **(1,5 point)** Montrer que si a divise b alors, pour tout $n \in \mathbb{N}$, $n^a - 1$ divise $n^b - 1$.

Solution :

Raisonnement Maxime

Comme $a \mid b$, il existe un entier k tel que $b = ka$.

Alors,

$$\begin{aligned} n^b - 1 &= n^{ka} - 1 \\ &= (n^a)^k - 1 \\ &= (1^k - 1) \bmod (n^a - 1) \\ &= 0 \bmod (n^a - 1) \end{aligned}$$

Ainsi, il existe un entier k' tel que $n^b - 1 = k'(n^a - 1)$. Donc $n^a - 1 \mid n^b - 1$.

Raisonnement Valérie

On peut simplement poser $b = k\,a$, $N = n^a$, d'après l'identité remarquable classique on a alors $n^b - 1 = N^k - 1 = (N-1)\,(N^{k-1} + N^{k-2} + \cdots + N + 1)$ et $n^a - 1 = N - 1 \mid N^k - 1 = n^b - 1$.

2. **(1,5 point)** Soit $n \in \mathbb{N}^*$, montrer que le reste de la division euclidienne de $n^b - 1$ par $n^a - 1$ est $n^r - 1$, où r est le reste de la division euclidienne de b par a.

Solution :

On écrit la division euclidienne de b par a. Il existe $(q, r) \in \mathbb{N} \times [0, a-1]$ tel que $b = aq + r$. Alors,

$$\begin{aligned} n^b - 1 &= n^{aq+r} - 1 \\ &= (n^a)^q n^r - 1 \\ &= 1^q n^r - 1 \bmod (n^a - 1) \\ &= n^r - 1 \bmod (n^a - 1) \end{aligned}$$

Donc il existe un entier k tel que $n^b - 1 = k(n^a - 1) + n^r - 1$.

Pour conclure, il reste à montrer que $0 \leq n^r - 1 < n^a - 1$. D'une part, $n^r \geq 1$ donc $n^r - 1 \geq 0$. D'autre part, $r < a$ donc $n^r < n^a$ et $n^r - 1 < n^a - 1$.

3. **(1,5 point)** Soit $n \in \mathbb{N}^*$, montrer que $\text{pgcd}(n^b - 1, n^a - 1) = n^d - 1$, où $d := \text{pgcd}(a, b)$.

Solution :

Raisonnement Valérie

Si la division euclidienne de b par a s'écrit $b = aq + r$, on a $\text{pgcd}(b, a) = \text{pgcd}(a, r)$ et d'après la question précédente la division euclidienne de $n^b - 1$ par $n^a - 1$ s'écrit $n^b - 1 = k\,(n^a - 1) + (n^r - 1)$, donc $\text{pgcd}(n^b - 1, n^a - 1) = \text{pgcd}(n^a - 1, n^r - 1)$. Les deux algorithmes d'Euclide vont donc s'écrire simultanément et quand pour le calcul du pgcd de b et a on arrive à $r_{k+1} = 0$, on a $n^{r_{k+1}} - 1 = n^0 - 1 = 0$ donc l'algorithme d'Euclide pour $n^b - 1$ et $n^a - 1$ se termine aussi et $\text{pgcd}(n^b - 1, n^a - 1) = n^{\text{pgcd}(b,a)} - 1$.

Raisonnement Maxime

On écrit l'algorithme d'Euclide utilisé sur le couple (b, a) :

$$\begin{aligned} b &= aq_1 + r_1 & 0 \leq r_1 < a \\ a &= r_1 q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 & 0 \leq r_3 < r_2 \end{aligned}$$

L'algorithme se termine avec

$$\begin{aligned} r_{n-2} &= r_{n-1}q_n + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} + 0 \end{aligned}$$

Le dernier reste non nul est $r_n = \text{pgcd}(b, a) = d$. En utilisant la question précédente, il existe des entiers $q'_1, q'_2, \ldots q'_{n+1}$ tels que :

$$\begin{aligned} n^b - 1 &= (n^a - 1)q'_1 + n^{r_1} - 1 & 0 \leq n^{r_1} - 1 < n^a - 1 \\ n^a - 1 &= (n^{r_1} - 1)q'_2 + n^{r_2} - 1 & 0 \leq n^{r_2} - 1 < n^{r_1} - 1 \\ n^{r_1} - 1 &= (n^{r_2} - 1)q'_3 + n^{r_3} - 1 & 0 \leq n^{r_3} - 1 < n^{r_2} - 1 \end{aligned}$$

Jusqu'à

$$\begin{aligned} n^{r_{n-2}} - 1 &= (n^{r_{n-1}} - 1)q'_n + n^{r_n} - 1 & 0 \leq n^{r_n} - 1 < n^{r_{n-1}} - 1 \\ n^{r_{n-1}} - 1 &= (n^{r_n} - 1)q'_{n+1} + 0 & (\text{car } n^0 - 1 = 0) \end{aligned}$$

On vient d'écrire l'algorithme d'Euclide entre $n^b - 1$ et $n^a - 1$. Le dernier reste non nul est $n^{r_n} - 1 = n^d - 1 = \text{pgcd}(n^b - 1, n^a - 1)$.

4. On rappelle que l'entier b vérifie $b > 1$.
   (a) **(0,5 point)** Soit $n \in \mathbb{N}$ tel que $n > 2$. Montrer que $n^b - 1$ est toujours composé.

Solution :
1 divise b. Donc, d'après Q1, $n - 1$ divise $n^b - 1$.
Comme $n > 2$, $n - 1 > 1$. De plus, comme $n > 1$ et $b > 2 > 1$, $n^b - 1 > n - 1$. Ainsi, $n - 1$ est un diviseur non trivial de $n^b - 1$ et $n^b - 1$ est donc composé.

   (b) **(1 point)** Montrer que si b est composé alors, $2^b - 1$ est composé.

Solution :
Comme b est composé, il existe $1 < a < b$ tel que a divise b. D'après Q1, $2^a - 1$ divise alors $2^b - 1$.
Or,

$$\begin{aligned} & 1 < a < b \\ \Rightarrow & 2^1 < 2^a < 2^b \\ \Rightarrow & 2 - 1 < 2^a - 1 < 2^b - 1 \\ \Rightarrow & 1 < 2^a - 1 < 2^b - 1 \end{aligned}$$

Donc $2^a - 1$ est un diviseur non trivial de $2^b - 1$, qui est donc composé.

   (c) **(1 point)** Donner une condition nécessaire pour que $n^b - 1$ soit premier.

Les nombres premiers de cette forme sont appelés premiers de Mersenne. Ils sont très utiles car l'arithmétique modulo un premier de Mersenne est très efficace sur un ordinateur binaire. En cryptographie, ils sont notamment utilisés pour générer des nombres aléatoires.

Solution :
D'après la question a), il faut que $n = 2$.
En utilisant la contraposée de la question b), il faut également que b soit premier.

Remarque : Cette condition n'est pas suffisante. En effet, pour p premier, tous les $2^p - 1$ ne sont pas premiers. Le plus petit contre-exemple est donné par $p = 11$. $2^{11} - 1 = 2047 = 23 \times 89$.