Examen de Cryptologie

14 mai 2019
Durée 2h

Auteurs
Valérie Ménissier-Morain & Jérémy Berthomieu

Version du 23 mai 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.
La note finale est le minimum entre 20 *et la somme des points obtenus sur* 34.

Exercice 1 – Questions – 2,5 points

1. (**0,5 point**) Qu'est-ce que le *social engineering* ? Donner deux exemples.

> **Solution :**
> Il s'agit d'attaques reposant sur les faiblesses humaines.
> Par exemple :
> — faiblesse des mots de passe (nom de l'animal famillier, date d'anniversaire,…) ;
> — interrogatoires détournés ;
> — taupe ;
> — lecture derrière l'épaule ;
> — hameçonnage.

2. (**0,5 point**) Sur quelle faiblesse repose l'attaque de Wiener ?

> **Solution :**
> Elle repose sur le choix d'un petit exposant secret d dans RSA.
> Plus précisément, si $d < \frac{\sqrt[4]{n}}{\sqrt{6}}$, alors on peut retrouver d par un calcul de fractions continues (de $\frac{e}{\varphi(n)}$ mais en pratique) de $\frac{e}{n}$.

3. (**1 point**) Que vous évoque le nom de Kocher ?

> **Solution :**
> Il s'agit d'une attaque matérielle sur RSA.
> Cette attaque consiste à mesurer le temps d'exécution de l'exponentiation dans RSA pour en déduire une information sur le développement binaire de l'exposant secret.
> Cette attaque peut être contrée en y rajoutant des calculs inutiles. Par exemple, à chaque tour de boucle du *square and multiply*, en plus de l'élévation au carré, on effectue toujours le produit mais l'on ne garde le résultat du produit que si nécessaire.

4. (**0,5 point**) Comment se nomme le protocole prédécesseur de TLS (*Transport Layer Security*) ? Donner le nom d'un logiciel ou d'une bibliothèque l'implémentant.

Solution :
Le prédécesseur de TLS est SSL (*Secure Sockets Layer*).
On peut utiliser `openssl` et en particulier la bibliothèque `libssl`.

Exercice 2 – RSA – 11 points

1. (**Alice ouvre ses oreilles – 2.5 points**) Alice choisit $p = 17, q = 19$ et $e = 91$ pour chiffrer ses messages avec RSA. Quelle clef publique publie-t-elle et quelle clef privée conserve-t-elle par devers elle ? Vous détaillerez les calculs d'Alice.

Solution :
Alice publie $N = p * q = 323$ et $e = 91$. Elle garde secret p et q ainsi que $d = e^{-1} \bmod \varphi(N)$. p et q sont premiers donc $\varphi(p) = p - 1 = 16$ et $\varphi(q) = q - 1 = 18$ et puisque p et q sont premiers entre eux $\varphi(N) = \varphi(p) * \varphi(q) = 16 * 18 = 288$.
Pour connaître la valeur de d on applique l'algorithme d'Euclide étendu à $e = 91$ et $\varphi(N) = (p-1)(q-1) = 16 * 18 = 288$:

$$\begin{cases} u_0 = 1, & v_0 = 0, & r_0 = a \\ u_1 = 0, & v_1 = 1, & r_1 = b \\ u_{i+1} = u_{i-1} - q_i u_i, & v_{i+1} = v_{i-1} - q_i v_i, & r_{i+1} = r_{i-1} - q_i r_i \quad i \geqslant 1 \end{cases}$$

avec $q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor$ si $r_i \neq 0$ et arrêt sinon.
À chaque étape $u_i * a + v_i * b = r_i$ donc quand $r_{n+1} = 0$, $u_n * a + v_n * b = r_n = \text{pgcd}(a, b)$ est la relation de Bézout.

i	r_{i-1}	r_i	q_i	r_{i+1}	u_{i+1}	v_{i+1}
				288	1	0
0		288		91	0	1
1	288	91	3	15	1	-3
2	91	15	6	1	-6	19
3	15	1	15	0	91	-288

On déduit donc de la dernière étape avec reste non nul (encadré en rouge) que $-6 * 288 + 19 * 91 = 1$, e est donc bien inversible modulo $\varphi(N) = 288$ et d'inverse $d = 19$ modulo $\varphi(N)$. Alice garde donc secrets $p = 17$, $q = 19$ et $d = 19$.

2. (**Bob parle à Alice – 4.5 points**) Bob adresse à Alice les messages chiffrés $c_1 = 10$, $c_2 = 7$ et $c_3 = 16$. Alice déchiffre ces messages, quels messages clairs m_1, m_2 et m_3 obtient-elle ? Quels calculs effectuent-elles pour cela ? Que pensez-vous du message m_3 ?

Solution :
Alice doit calculer $m_1 = c_1^d \bmod N$, $m_2 = c_2^d \bmod N$ et $m_3 = c_3^d \bmod N$. Le calcul direct nécessiterait trop de temps à la main et générerait trop d'erreurs humaines. On va donc utiliser le CRT pour se ramener à un calcul moins difficile.
Alice va calculer $m_1 = c_1^d \bmod p$ et $m_1 = c_1^d \bmod q$ et reconstruire m_1 à partir de ces deux valeurs et des coefficients de Bézout pour p et q.

p et q sont voisins donc en tâtonnant on trouve facilement (sinon on utilise l'algorithme d'Euclide étendu bien entendu) que $17 * 9 - 19 * 8 = 1$.

D'après le théorème d'Euler $a^d \bmod k = a^{d \bmod \varphi(k)} \bmod k$ pour tout $k \neq 0$ donc $c_1^d \bmod p = c_1^{d \bmod (p-1)} \bmod p$ et $c_1^d \bmod q = c_1^{d \bmod (q-1)} \bmod q$. On calcule $d_p = d \bmod (p-1) = 19 \bmod 16 = 3$ et $d_q = d \bmod (q-1) = 19 \bmod 18 = 1$.

On va donc calculer $c_1^{d_p} \bmod p = 10^3 \bmod 17 = (-7)^3 \bmod 17 = (-2) * (-7) \bmod 17 = 14$ et $c_1^{d_q} \bmod q = 10^1 \bmod 19 = 10$.

Il reste donc à résoudre $m_1 = \begin{cases} 14 \bmod 17 \\ 10 \bmod 19 \end{cases}$, ce qui nous donne $m_1 = 14 * (-19 * 8) + 10 * (17 * 9) = 14 * (-152) + 10 * 153 = 10 - 4 * 152 = -598 \bmod 323 = 48 \bmod 323$.

De même on calcule $c_2^{d_p} \bmod p = 7^3 \bmod 17 = (-2) * 7 \bmod 17 = -14 \bmod 17 = 3$ et $c_1^{d_q} \bmod q = 7^1 \bmod 19 = 7$.

Il reste donc à résoudre $m_2 = \begin{cases} 3 \bmod 17 \\ 7 \bmod 19 \end{cases}$, ce qui nous donne $m_1 = 3 * (-19 * 8) + 7 * (17 * 9) = 3 * (-152) + 7 * 153 = 7 + 4 * 152 = 615 \bmod 323 = 292 \bmod 323$.

Enfin on calcule $c_3^{d_p} \bmod p = 16^3 \bmod 17 = (-1)^3 \bmod 17 = 16$ et $c_3^{d_q} \bmod q = 16^1 \bmod 19 = 16$, par conséquent $m_3 = 16 \bmod N = c_3$. Chiffrer m_3 n'a en rien protégé le contenu du message puisque le clair et le chiffré sont identiques. On a intérêt à modifier un peu le message d'origine pour avoir une valeur chiffrée différente du clair.

3. (**RSA+CRT − 4 points**) Expliquer comment utiliser le CRT pour déchiffrer plus efficacement un message chiffré avec RSA et quel est le facteur gagné dans le cas d'une multiplication naïve et dans le cas d'une multiplication avec l'algorithme de Karatsuba.

Solution :

On reçoit y et on doit calculer $x = y^d \bmod n$. On doit donc calculer $x_p = y^d \bmod p$ et $x_q = y^d \bmod q$ puis reconstruire x à partir de x_p et x_q par le CRT.

Or $y^{p-1} = 1 \bmod p$ et $y^{q-1} = 1 \bmod q$ d'après le théorème d'Euler. On calcule donc $x_p = y^{d_p} \bmod p$ et $x_q = y^{d_q} \bmod q$ avec $d_p = d \bmod (p-1)$ et $d_q = d \bmod (q-1)$.

On a

$$x = \begin{cases} x_p \bmod p \\ x_q \bmod q. \end{cases}$$

On utilise le théorème chinois pour déduire x. La relation de Bézout pour p et q est $u\,p + v\,q = 1$ on a $x = u\,p\,x_q + v\,q\,x_p \bmod (p\,q)$ soit avec les notations $u_p = v\,q$ et $u_q = u\,p$, $x = u_p\,x_p + u_q\,x_q \bmod n$.

Le coût du calcul de $a^b \bmod c$ est $O(\log(b)\mathcal{M}(\log(c)))$, on met la constante C en évidence, ce coût est $C\,\log(b)\mathcal{M}(\log(c))$.

On remplace :

- l'exponentiation directe $y^d \bmod n$ de coût $C\,(\log(n))\mathcal{M}(\log(n))$ car $y < n$ et d est de l'ordre de n
- par :
  - deux exponentations $y^{d_p} \bmod p$ et $y^{d_q} \bmod q$ de coût $C\log(d_p)\mathcal{M}(\log(p))$ et $C\log(d_q)\mathcal{M}(\log(q))$ soit $C(\log(p)\mathcal{M}(\log(p)) + \log(q)\mathcal{M}(\log(q)))$ et en comptant que $\log(p) \simeq \log(q) \simeq \log(n)/2$ au final
  $$C\log(n)\mathcal{M}(\log(n)/2) \quad (1)$$
  - on applique la formule $x = u_p x_p + u_q x_q \bmod (pq)$ qui comporte deux multiplications de nombres inférieurs à n, une addition et trois réductions modulo n, donc une opération linéaire

et cinq opérations en $O(\mathcal{M}(\log(n)))$ en la taille de n, donc le coût de reconstruction de x à partir de x_p et x_q est en $O(\mathcal{M}(\log(n))$ qui est négligeable devant le $C\log(n)\mathcal{M}(\log(n)/2)$.
Avec la multiplication naïve : $\mathcal{M}(\ell/2) = \mathcal{M}(\ell)/4$ donc on passe de $C\log^3(n)$ à $C/4\log^3(n)$ d'où un facteur 4.
Avec la multiplication de Karatsuba on a $\mathcal{M}(\ell/2) = \mathcal{M}(\ell)/3$ donc on passe de $C\log^3(n)$ à $C/3\log^3(n)$ d'où un facteur 3.

Exercice 3 – DLP – 6,5 points

1. (**1 point**) On considère le groupe $G = \mathbb{F}_{53}^{\times}$. Quel est son ordre ? Est-il cyclique ?

Solution :
Il s'agit du groupe des inversibles du corps $\mathbb{F}_{53}$. Il est donc d'ordre $53-1 = 52$ et est cyclique.

2. (**0,5 point**) On considère $g = 2$ et $h = 37$. On souhaite calculer le plus petit entier a tel que $[a]g = g^a = h$ avec l'algorithme Baby-Step Giant-Step.
Justifier que les pas de géant qu'il faut faire sont de taille $s = 8$.

Solution :
La taille des pas de géant est $s = \lfloor\sqrt{52}\rfloor + 1 = 7 + 1 = 8$.

3. (**1,5 point**) Calculer $[s]g = g^s$ puis son inverse dans G.

Solution :
On a $[2]g = 4$, $[4]g = [2]4 = 16$ et $[8]g = [s]g = 44$.
Comme $44 = -9$ et $(-9)\times(-6) = 54 = 1 \bmod 53$, alors l'inverse de 44 est $-6 = 47$.
Alternativement, on inverse 44 modulo 53 *via* l'algorithme d'Euclide étendu appliqué à 44 et 53.

i	r_{i-1}	r_i	q_i	r_{i+1}	u_{i+1}	v_{i+1}
				53	1	0
0		53		44	0	1
1	53	44	1	9	1	-1
2	44	9	4	8	-4	5
3	9	8	1	1	5	-6
4	8	1	8	0	-44	53

On déduit donc de la dernière étape avec reste non nul (encadré en rouge) que $53\times 5 + 44\times(-6) = 1$ et donc que $g^{-s} = -6 = 47$ est l'inverse de $g^s = 44$.

4. (**3,5 points**) Déterminer a à l'aide de l'algorithme Baby-Step Giant-Step.

Solution :
On calcule la liste des pas de bébé $(j, g^j \bmod 53) = (j, 2^j \bmod 53)$ pour $j = 0,\dots,7$:
$(0,1),(1,2),(2,4),(3,8),(4,16),(5,32),(6,11),(7,22)$.
On calcule la liste des pas de géant $(i, h\,g^{-si} \bmod 53) = (i, h\,(g^{-s})^i \bmod 53) = (i, 37\times(-6)^i)$ jusqu'à trouver une collision avec la liste précédente :
$(0,37),(1,43),(2,7),(3,11)$. (Pour info, la liste continue comme suit $(4,40),(5,25),(6,9),(7,52)$.)
On a une collision pour $j = 6$ et $i = 3$ donc $a = i\times s + j = 3\times 8 + 6 = 30$.

Exercice 4 – Courbes Elliptiques – 14 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 $y^2 = x^3 + 2x + 1$ sur $\mathbb{F}_{13}$.

1. (**1 point**) Justifier que cette courbe est bien elliptique.

Solution :
La courbe est d'équation $y^2 = x^3 + ax + b$ définie sur $\mathbb{F}_{13}$ avec $a = 2$ et $b = 1$. Elle semble donc elliptique.
Elle est elliptique si, et seulement si, $\Delta = 16(4a^3 + 27b^3) \neq 0$. Or $4a^3 + 27b^2 = 4 \times 8 + 1 = 33 = 7 \neq 0$ et $\Delta \neq 0$.

2. (**0.5 point**) Donner l'ensemble des carrés dans $\mathbb{F}_{13}$.

Solution :

y	y^2
0	0
± 1	1
± 2	4
± 3	9
± 4	3
± 5	12
± 6	10

3. (**2 points**) Donner, sous la forme d'un tableau comme vu en cours/TD, l'ensemble des points rationnels définissant E. Montrer que E est de cardinal 8.

Solution :

x	$x^3 + 2x + 1$	Point(s)
0	1	$(0, \pm 1)$
1	4	$(1, \pm 2)$
2	0	$(2, 0)$
3	8	
4	8	
5	6	
6	8	
7	7	
8	9	$(8, \pm 3)$
9	7	
10	7	
11	2	
12	11	

Il y a donc un point d'ordre 2 sur l'axe des abscisses : $(2, 0)$ et 3 paires de points symétriques, ce qui donne 7 points rationnels plus le point à l'infini et au total on a donc 8 points.

4. (**0,5 point**) Soit $P = (8, 3)$ et $Q = (0, 12)$; vérifier que ce sont bien deux points de E.

Solution :
On voit qu'il y a dans notre tableau les paires $(8, \pm 3)$ et $(0, \pm 1)$ donc $P = (8, 3)$ et $Q = (0, -1) = (0, 12)$ sont bien des points de E.
Alternativement, $8^3 + 2 \times 8 + 1 - 3^2 = 5 + 3 + 1 - 9 = 0 \bmod 13$ et $0^3 + 2 \times 0 + 1 - (-1)^2 = 0 \bmod 13$.

5. (**1,5 point**) Montrer que $P+Q$ est un point d'ordre 2.

Solution :
$\lambda = \frac{y_Q - y_P}{x_Q - x_P} = \frac{12-3}{0-8} = \frac{9}{-8} = 9 \times 8 = 7$ donc $P+Q = (x,y)$ avec $x = \lambda^2 - x_P - x_Q = 7^2 - 8 - 0 = 2 \bmod 13$ (et $y = \lambda(x_P - x) - y_P = 7 \times (8-2) - 3 = 0$ mais on sait que si l'on ne s'est pas trompé alors c'est le point $(2,0)$).
$P + Q \neq \mathcal{O}$ et est d'ordonnée nulle donc est d'ordre 2.

6. (**2 points**) Montrer que $Q = [3]P$.

Solution :
— On calcule tout d'abord $[2]P$:
$\lambda = \frac{3x_P^2+2}{2y_P} = \frac{3\times 12+2}{6} = \frac{12}{6} = 2$ donc $P+Q = (x,y)$ avec $x = \lambda^2 - x_P - x_P = 2^2 - 8 - 8 = 1 \bmod 13$ et $y = \lambda(x_P - x) - y_P = 2 \times (8-1) - 3 = 11 \bmod 13$.
— On calcule ensuite $[3]P = P + [2]P$:
$\lambda = \frac{y_{[2]P} - y_P}{x_{[2]P} - x_P} = \frac{11-3}{1-8} = \frac{8}{-7} = 8 \times 11 = 10$ donc $P + [2]P = (x,y)$ avec $x = \lambda^2 - x_P - x_{[2]P} = 10^2 - 8 - 1 = 0 \bmod 13$ et $y = \lambda(x_P - x) - y_P = 10 \times (8-0) - 3 = 12$.

7. (**0,5 point**) En déduire que P n'est ni d'ordre 2 ni d'ordre 4.

Solution :
Comme $Q = [3]P$, alors $P + Q = [4]P$. Or, $P+Q$ est d'ordre 2 donc P n'est pas d'ordre 4 et *a fortiori* pas d'ordre 2.

8. (**1 point**) Montrer que E est un groupe cyclique. Exhiber un générateur de ce groupe.

Solution :
Puisque E est d'ordre 8 et que, d'après le théorème de Lagrange, l'ordre d'un élément d'un groupe fini divise l'ordre du groupe alors les seuls ordres possibles pour P sont :
— 1 (mais $P \neq \mathcal{O}$) ;
— 2 (mais P n'est pas d'ordre 2 d'après ce qui précède) ;
— 4 (mais P n'est pas d'ordre 4 d'après ce qui précède) ;
— 8.
On a éliminé tous les cas sauf le dernier donc P est d'ordre 8 maximal dans E donc P engendre le groupe cyclique E.

9. (**1 point**) Alice et Bob décident de procéder à un échange de clef *via* le protocole Diffie–Hellman–Merkle dans le groupe $(E,+)$.
   1. Ils se mettent d'accord pour prendre P comme générateur.
   2. Alice choisit comme clef secrète $a = 3$ et envoie $A = [a]P$ à Bob.
   3. Bob choisit comme clef secrète $b = 5$ et envoie $B = [b]P$ à Alice.

   Quelle est la clef privée partagée ?

Solution :
La clef privée partagée est $[a][b]P = [ab]P = [15]P$. Or E (ou P) est d'ordre 8 donc $[15]P = [7]P = -P$. Il s'agit donc du point qui, sommé avec P, donne $\mathcal{O}$. C'est-à-dire le symétrique de $P = (8,3)$ par rapport à l'axe des abscisses : $(8,-3) = (8,10)$.

10. (**0,5 point**) Justifier que le polynôme t^2-2 est irréductible dans $\mathbb{F}_{13}[t]$. En déduire que $\mathbb{F}_{169} = \mathbb{F}_{13}[t]/(t^2-2)$.

Solution :
D'après la question 2, 2 n'est pas un carré dans $\mathbb{F}_{13}$. Ainsi, le polynôme t^2-2 ne peut se factoriser en produit de deux polynômes de degrés 1 dans $\mathbb{F}_{13}[t]$. Il est donc irréductible.
$\mathbb{F}_{13}[t]/(t^2-2)$ est donc un corps fini de cardinal $13^2 = 169$.

11. (**1 point**) On note E' le groupe additif défini à partir des points rationnels de la courbe elliptique définie par l'équation $y^2 = x^3 + 2x + 1$ sur $\mathbb{F}_{169}$. On admet que E' est d'ordre 160.
En utilisant le théorème de structure, montrer que seules les situations suivantes sont possibles :

$$(E',+) \simeq (\mathbb{Z}/160\mathbb{Z},+),$$
$$(E',+) \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/80\mathbb{Z},+),$$
$$(E',+) \simeq (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z},+).$$

Solution :
D'après le théorème de structure, on a $(E',+) \simeq (\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z},+)$ avec $d_1 d_2 = 160$, $d_1 | d_2$ et $d_1 | (q-1) = 168$. Donc d_1 est un diviseur de $\text{pgcd}(168, 160) = 8$.
Cependant, si $d_1 = 8$, alors $d_2 = 20$ et $d_1 \nmid d_2$. Il ne reste alors que les trois autres cas, $(d_1, d_2) = (1, 160)$, $(d_1, d_2) = (2, 80)$ et $(d_1, d_2) = (4, 40)$.

12. (**1,5 point**) Montrer que $x^3 + 2x + 1$ admet 2, $2t + 12$ et $11t + 12$ comme racines dans $\mathbb{F}_{169}$. Que peut-on en déduire sur le nombre de points d'ordre 2 dans E' ?

Solution :
D'après la question 3, 2 est bien une racine du polynôme.
De plus si $\varepsilon \in \{1, -1\}$, on a

$$(2\varepsilon t + 12)^3 + 2(2\varepsilon t + 12) + 1 = (2\varepsilon t - 1)^3 + 2(2\varepsilon t - 1) + 1$$

puisqu'on calcule dans $\mathbb{F}_{13}$.
En factorisant $2\varepsilon t - 1$ on a :

$$(2\varepsilon t + 12)^3 + 2(2\varepsilon t + 12) + 1 = ((2\varepsilon t - 1)^2 + 2)(2\varepsilon t - 1) + 1 = (4t^2 - 4\varepsilon t + 3)(2\varepsilon t - 1) + 1.$$

On fait apparaître $t^2 - 2$ qui vaut 0 dans $\mathbb{F}_{169}$ dans le premier facteur :

$$(2\varepsilon t+12)^3+2(2\varepsilon t+12)+1 = (4(t^2-2)-4\varepsilon t+11)(2\varepsilon t-1)+1 = (-4\varepsilon t+11)(2\varepsilon t-1) = -8t^2+26\varepsilon t-10.$$

On fait apparaître t^2-2 à nouveau et on obtient $(2\varepsilon t+12)^3+2(2\varepsilon t+12)+1 = -8(t^2-2)+26\varepsilon t-26 = 0$ puisque $t^2 - 2 = 0$ dans $\mathbb{F}_{169}$ et $26 = 0 \bmod 13$.
Par conséquent $2\varepsilon t + 12$ est racine du polynôme $x^3 + 2x + 1$ dans $\mathbb{F}_{169}$ pour $\varepsilon \in \{1, -1\}$ ce qui nous donne finalement 2, $2t + 12$ et $11t + 12$ comme racines du polynôme.
La courbe E' a donc 3 points d'ordonnée nulle : $(2, 0)$, $(2t + 12, 0)$ et $(11t + 12, 0)$ et donc 3 points d'ordre 2.

13. (**1 point**) Montrer que dans $(\mathbb{Z}/160\mathbb{Z},+)$, il n'existe qu'un seul élément $h \neq 0$ tel que $[2]h = 0$. En déduire que $(E',+) \neq (\mathbb{Z}/160\mathbb{Z},+)$.

Solution :
Si $[2]h = 0 \bmod 160$, alors $2h = 160k$, $k \in \mathbb{Z}$ et $h = 80k$. Ainsi, modulo 160, $h = 0$ ou $h = 80$ et 80 le seul non nul.
Comme dans $\mathbb{Z}/160\mathbb{Z}$, il n'y a qu'un élément d'ordre 2 et que dans E, il y en a 3, on en déduit que $(E', +) \not\simeq (\mathbb{Z}/160\mathbb{Z}, +)$.