

université BORDEAUX	ANNÉE UNIVERSITAIRE 2018-2019 Examen - Session 1 de Printemps Parcours : Master CSI UE : 4TCY802U Épreuve : Cryptologie Date : 30 Avril 2019 Heure : 14h30 Durée : 3h Documents : aucun document autorisé Épreuve de M. Cerri	Collège Sciences et Technologies
--------------------------------	---	---

L'usage de la calculatrice est autorisé.
La qualité de l'argumentation et de la rédaction sera un facteur d'appréciation.
Six exercices parfaitement traités donneront la totalité des points.

Exercice 1 - [LFSR]

On considère les suites $u = (u_i)_{i \geq 0}$ et $v = (v_i)_{i \geq 0}$ de \mathbb{F}_2^N définies par les relations de récurrence

$$\begin{cases} u_{i+4} = u_{i+1} + u_i \\ v_{i+5} = v_{i+4} + v_{i+1} + v_i \end{cases}$$

pour tout $i \geq 0$, et de graines respectives $(1, 0, 0, 0)$ et $(1, 0, 0, 1, 1)$.

1) Montrer que $X^4 + X + 1$ est un polynôme irréductible primitif de $\mathbb{F}_2[X]$.

2) En déduire la période de u .

3) Quelle est la période de v ?

4) Déterminer les 15 premiers termes de u .

Soient $U(X)$ et $V(X)$ les séries génératrices de u et v .

5) Déterminer ces deux séries. On les mettra sous forme de fractions irréductibles.¹

6) En déduire la relation de récurrence la plus courte vérifiée par v .

7) Calculer la série génératrice de $w = u + v$ et en déduire la relation de récurrence la plus courte vérifiée par w .

8) Montrer que la période de w divise 60 et ne peut être ni un multiple de 4 ni un multiple de 15 strictement inférieur à 60.

9) Quelle est la période de w ?

Exercice 2 - [LOGARITHME DISCRET ET DERNIER BIT]

Soient n un entier impair, G un groupe cyclique de cardinal n et g un générateur de G . Admettons que l'on dispose d'un algorithme polynomial (en la taille de n) qui pour tout $h \in G$ retourne le dernier bit de l'unique $k \in \{0, 1, \dots, n-1\}$ tel que $h = g^k$. Le but de cet exercice est de prouver que l'on est alors en mesure de résoudre le problème du logarithme discret dans G en temps polynomial. Soit $y \in G$. On cherche à déterminer l'unique $x \in \{0, 1, \dots, n-1\}$ tel que $y = g^x$. Supposons que $n-1$ s'écrit avec s bits et notons $b_{s-1}b_{s-2} \dots b_1b_0$ l'écriture binaire de x , écriture pouvant commencer par des zéros. On a $x = \sum_{i=0}^{s-1} b_i 2^i$.

1) On soumet y à notre algorithme qui retourne donc b_0 . Montrer que si $b_0 = 0$, alors $y^{\frac{n-1}{2}}$ est égal à g^{x_1} où l'écriture binaire de x_1 est $b_{s-1}b_{s-2} \dots b_1$.

2) Trouver une formule qui donne g^{x_1} si $b_0 = 1$.

¹Pour u , on pourra soit chercher à réduire la fraction, soit expliquer pourquoi $U(X) = (aX^3 + bX^2 + cX + d)/(X^4 + X^3 + 1)$ où $a, b, c, d \in \mathbb{F}_2$ et obtenir a, b, c, d par identification.

3) En déduire un algorithme polynomial (en la taille de n) qui calcule x . Le décrire avec précision.

4) Expliquer pourquoi Oscar rêve de disposer d'un algorithme équivalent pour n pair.

Exercice 3 – [SIGNATURE ELGAMAL ET ALÉAS PROCHES]

1) Soient $n > 1$ un entier naturel et $a, b \in \mathbb{Z}/n\mathbb{Z}$. Admettons que l'équation $ax = b$ admette au moins une solution $x \in \mathbb{Z}/n\mathbb{Z}$. Montrer que l'ensemble de ses solutions dans $\mathbb{Z}/n\mathbb{Z}$ a pour cardinal $\text{pgcd}(a, n)$.

Alice utilise un système ElGamal de clé publique $(p, \alpha, \beta = \alpha^s \pmod{p})$ où α est une racine primitive modulo p et de clé secrète $s \in \{0, 1, \dots, p-2\}$.

2) Rappeler comment fonctionnent la signature ElGamal et sa vérification ?

Alice signe deux messages M et M' par (u, v) et (u', v') en utilisant des aléas k et $k' \geq k$ proches. Un adversaire qui intercepte les deux messages signés et qui a dressé une liste des petites puissances de g , remarque que $u'u^{-1} \pmod{p}$ figure dans cette liste. Il connaît donc i tel que $u'u^{-1} = \alpha^i \pmod{p}$.

3) Montrer comment il peut procéder pour retrouver s quand $\text{pgcd}(uv' - u'v, p-1)$ est petit.

4) Application numérique. On prend $p = 107$.

a) Montrer que 2 est racine primitive modulo p .
b) La clé publique d'Alice est $(107, 2, 94)$. Elle signe les messages $M = 33$ et $M' = 61$ par $(95, 74)$ et $(59, 62)$ respectivement. Retrouver sa clé secrète s .

5) Le recours à une fonction de hachage publique permet-il de lever ce problème ?

Exercice 4 – [HACHAGE]

Soit un entier $n \geq 1$ et $h : \{0, 1\}^{2n} \rightarrow \{0, 1\}^n$ une fonction de compression. On définit $h_i : \{0, 1\}^{4n} \rightarrow \{0, 1\}^n$ pour $1 \leq i \leq 3$ par :

$$\begin{cases} h_1(x\|y) &= h(x \oplus y) \\ h_2(x\|y) &= h(L(x)\|h(y)) \\ h_3(x\|y) &= h(h(x \oplus y)\|h(y)) \end{cases}$$

pour tout x et tout $y \in \{0, 1\}^{2n}$. Ici $L(x)$ désigne la partie gauche de x , i.e. les n premiers bits de x .

1) Supposons h résistante à la préimage. Pour quels i , h_i l'est-elle ?

2) Supposons h résistante aux collisions. Pour quels i , h_i l'est-elle ?

Exercice 5 – [CHIFFREMENT DE GOLDWASSER-MICALI]

Le chiffrement de Goldwasser-Micali est un système cryptographique à clé publique basé sur la difficulté de déterminer la résiduosité quadratique sous certaines conditions. Alice choisit deux grands premiers distincts p et q . Elle calcule $n = pq$ et détermine $y \in \{0, 1, \dots, n-1\}$ un non-résidu quadratique modulo n vérifiant $(\frac{y}{n}) = 1$. Sa clé publique est (n, y) , sa clé privée est (p, q) . Les clairs sont des suites finies de bits. Soit $M = (m_1, m_2, \dots, m_k) \in \{0, 1\}^k$ un message que Bob veut chiffrer pour l'envoyer à Alice. Il chiffre indépendamment chaque bit de M de la façon suivante : pour tout $1 \leq i \leq k$, il tire au hasard $x_i \in (\mathbb{Z}/n\mathbb{Z})^\times$, puis calcule $c_i = y^{m_i} x_i^2 \pmod{n}$. Le message chiffré est $C = (c_1, c_2, \dots, c_k)$.

1) Soient $C = (c_1, c_2, \dots, c_k)$ et $C' = (c'_1, c'_2, \dots, c'_k)$ des chiffrés de M et $M' \in \{0, 1\}^k$.

- Construire à partir de C et C' un chiffré de $M \oplus M'$.
- Construire à partir de C un chiffré de $(1, 1, \dots, 1) \oplus M$.

- 2) Décrire avec précision l'algorithme de déchiffrement. Justifier.
- 3) Alice a choisi $p = 41$, $q = 59$, $y = 13$. Vérifier que y est un choix adapté.
- 4) Elle a reçu le chiffré $(362, 1562)$. Qu'obtient-elle à l'issue du déchiffrement ? On donnera le détail des calculs effectués par Alice.

Exercice 6 – [SYSTÈME CRYPTOGRAPHIQUE DU SAC À DOS DE NACCACHE-STERN]

Alice et Bob utilisent le système asymétrique suivant. Alice choisit un entier naturel n et dresse la liste des $n + 1$ premiers nombres premiers : $p_0 = 2, p_1 = 3, \dots, p_n$. Elle détermine un grand nombre premier p tel que $\prod_{i=0}^n p_i < p$. Elle choisit alors un entier naturel $s < p - 1$ (son secret) vérifiant $\text{pgcd}(s, p - 1) = 1$. Elle calcule enfin des entiers $0 < v_0, v_1, \dots, v_n < p$ vérifiant $v_i^s = p_i \bmod p$ pour tout i . Sa clé publique est

$$K_{\text{pub}} = (p, n, v_0, v_1, \dots, v_n).$$

Sa clé secrète est s .

Bob veut lui envoyer un message qui est une suite de $n + 1$ bits (m_0, m_1, \dots, m_n) . Il chiffre m en

$$c = \prod_{i=0}^n v_i^{m_i} \bmod p.$$

- 1) Comment Alice fait-elle pour déterminer les v_i ?
- 2) Comment Alice peut-elle retrouver m à partir de c et s ?
- 3) Exemple pédagogique. On prend $n = 2$, $p = 71$. La clé secrète d'Alice est $s = 33$. Dans les deux questions qui suivent, on cherchera à minimiser le nombre de multiplications modulaires à effectuer.
 - a) Quelle est la clé publique d'Alice ?
 - b) Alice a reçu le chiffré $c = 8$. Retrouver m .

Exercice 7 – [SIGNATURE DE BOYD]

On s'intéresse ici à la forme originelle d'un schéma de signature proposé en 1997 par C. Boyd et aux défauts qu'il comporte. Alice choisit p et q deux grands nombres premiers distincts de k bits tels que $p - 1$ soit divisible par un grand premier r de l bits ($l \approx 160$). Elle calcule $n = pq$. Soit $g \in (\mathbb{Z}/n\mathbb{Z})^\times$ d'ordre r dans ce groupe. La clé publique d'Alice est (n, g) , sa clé secrète est (p, q, r) .

- 1) Supposons qu'Alice connaisse α et β racines primitives modulo p et q respectivement. Comment peut-elle trouver un g adéquat ?

Les messages envoyés par Alice sont, pour simplifier, des entiers non nuls qui s'écrivent avec au plus l' bits où $l' < l$ et peuvent donc être vus comme des éléments de $(\mathbb{Z}/r\mathbb{Z})^\times$. La signature d'un message M est un entier $S > 0$ vérifiant $S^M = g \bmod n$.

- 2) Comment Alice peut-elle déterminer une signature S à partir de M ?
- 3) Que fait Bob pour vérifier la signature d'Alice ?
- 4) Supposons que $r \nmid q - 1$. Montrer que $g = 1 \bmod q$ et qu'un adversaire est alors en mesure de factoriser n .

On supposera donc dorénavant que $r \mid q - 1$.

- 5) Montrer que $r \mid n - 1$.
- 6) Soit M un message quelconque. Supposons que $\text{pgcd}(M, n - 1) = 1$ et soit a l'inverse de M modulo $n - 1$. Montrer qu'un adversaire est en mesure de contrefaire une signature de M à l'aide de a .
- 7) Montrer comment contrefaire une signature de M quand M n'est pas premier avec $n - 1$. On pourra s'inspirer de la question précédente.