université de BORDEAUX	**ANNÉE UNIVERSITAIRE 2017-2018** **Examen - Session 1 de Printemps** **Parcours :** Master CSI **UE :** 4TCY802U **Épreuve :** Cryptologie **Date :** 2 Mai 2018 **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 la relation de récurrence linéaire

$$(E): \ s_{i+7} = s_{i+5} + s_{i+3} + s_{i+2} + s_i \quad \text{pour tout } i \geqslant 0.$$

Soit $(u_i)_{i\geqslant 0} \in \mathbb{F}_2^{\mathbb{N}}$ engendrée par (E) et de vecteur initial $(1,0,0,1,0,1,1)$.

1) Quelle est la période de $(u_i)_{i\geqslant 0}$?

2) Déterminer la série génératrice de $(u_i)_{i\geqslant 0}$.

3) En déduire la complexité linéaire de $(u_i)_{i\geqslant 0}$, ainsi que la plus courte relation de récurrence linéaire satisfaite par $(u_i)_{i\geqslant 0}$.

4) À l'aide des questions précédentes, factoriser $X^7 + X^5 + X^3 + X^2 + 1$ dans $\mathbb{F}_2[X]$.

5) Déterminer une suite $(v_i)_{i\geqslant 0} \in \mathbb{F}_2^{\mathbb{N}}$ engendrée par (E) et de période 15.

6) Quelles sont la complexité linéaire et la période de $(u_i + v_i)_{i\geqslant 0}$?

Exercice 2 – [RSA]

Alice et Bob utilisent RSA. La clé publique d'Alice est (n, e) avec $n = pq$.

1) On s'intéresse ici, sous certaines hypothèses, aux messages M vérifiant $M^{10000} = 1 \bmod n$.

a) Soit ℓ un nombre premier tel que $\ell \equiv 1 \bmod 10000$. Montrer que dans $\mathbb{Z}/\ell\mathbb{Z}$ l'équation $x^{10000} = 1$ admet exactement 10000 solutions.

b) On suppose dans cette question (mais pas dans la suivante) que p et q sont congrus à 1 modulo 10000. Combien de messages $M \in \{0, 1, 2, \ldots, n-1\}$ vérifient $M^{10000} = 1 \bmod n$?

2) Bob envoie $C = M^e \bmod n$ à Alice et Ève intercepte C. Un espion a confié à Ève que M vérifie $M^{10000} = 1 \bmod n$. Ève remarque que $2 \nmid e$ et $5 \nmid e$. Montrer comment Ève peut retrouver M.

Exercice 3 – [RSA et Log Discret]

Soient $n = pq$ un module RSA et $a \in \{0, 1, \ldots, n-1\}$ premier avec n.

1) Montrer que l'ordre de a dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est égal au ppcm des ordres de a dans $\mathbb{F}_p^\times$ et $\mathbb{F}_q^\times$.

2) Soit $d = \text{pgcd}(p-1, q-1)$. On note φ l'indicatrice d'Euler. Montrer qu'il existe $a \in \{0, 1, \ldots, n-1\}$ premier avec n dont l'ordre dans $(\mathbb{Z}/n\mathbb{Z})^\times$ vaut $\varphi(n)/d$.

3) On suppose ici que p, $q > 3$ et que $d = 2$. Soit a comme dans la question précédente. On note G le sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$ engendré par a. On suppose que l'on dispose d'un oracle sachant résoudre le problème du Log Discret de base a dans G.

a) On soumet $b = a^n \bmod n$ à l'oracle. Exprimer ce qu'il retourne en fonction de n et $\varphi(n)$. *Indication* : on pourra montrer que $2n < 3\varphi(n)$.

b) En déduire que l'on peut facilement factoriser n.

Exercice 4 – [Rabin]

1) Soit $n = pq$ où p et q sont deux premiers impairs distincts congrus à 3 modulo 4. Soit $x \in \{0, 1, \ldots, n-1\}$ premier avec n. Supposons que x soit un carré modulo n. Combien x admet-il de racines carrées modulo n ? Justifier.

2) Sous les mêmes hypothèses, combien de racines quatrièmes x admet-il ? Justifier.

3) Soit $n = 1081 = 23 \times 47$.

a) Montrer que 3 est un carré modulo n

b) Déterminer les racines quatrièmes de 3 modulo n.

Exercice 5 – [Signature ElGamal]

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

1) Montrer que si elle signe un message $M \in \{1, 2, \ldots, p-1\}$ par $(u, 0)$ avec $\operatorname{pgcd}(u, p-1) = 1$, un adversaire qui intercepte le message signé peut retrouver la clé secrète s.

2) Alice signe deux messages $M \neq M'$ en utilisant le même aléa k. Montrer comment un adversaire qui intercepte les deux messages M et M' signés respectivement (u, v) et (u, v') peut procéder pour retrouver facilement s quand $\operatorname{pgcd}(u(v - v'), p-1)$ est petit.

3) Application numérique. On prend $p = 149$.

a) Montrer que 2 est racine primitive modulo p.

b) La clé publique d'Alice est $(149, 66)$. Elle signe les messages $M = 32$ et $M' = 56$ par $(79, 101)$ et $(79, 25)$ respectivement. Retrouver sa clé secrète s.

4) On considère la variante de la signature ElGamal suivante. La clé publique est encore $(p, \beta = \alpha^s)$ où α est une racine primitive modulo p et la clé secrète est $s \in \{0, 1, \ldots, p-2\}$ mais on impose à s de vérifier $\operatorname{pgcd}(s, p-1) = 1$. Le message $M \in \{1, 2, \ldots, p-1\}$ se signe (u, v) avec $u = \alpha^k \bmod p$ (où k est un aléa non nécessairement premier avec $p-1$) et $v = (M - uk)s^{-1} \bmod (p-1)$. Comment fonctionne la vérification ?

Exercice 6 – [Signature à la Fiat-Shamir]

Alice utilise le protocole de signature suivant. Elle choisit deux grands nombres premiers distincts p, q et calcule $n = pq$. Elle prend un entier s aléatoire premier avec n et calcule $u = s^{-2} \bmod n$. Sa clé publique est (n, u), sa clé secrète est (p, q, s). Pour signer un message $M \in \{0, 1, \ldots, n-1\}$ elle se sert d'une fonction de hachage publique $h : \{0,1\}^* \to \{0,1\}^m$ où $m \geqslant 1$. On identifie $\{0,1\}^m$ avec l'ensemble des entiers qui s'écrivent avec m bits : le m-uplet $(a_0, a_1, \ldots a_{m-1})$ est vu comme $\sum_{i=0}^{m-1} a_i 2^i$. Elle prend au hasard un entier $r \in \{1, 2, \ldots, n-1\}$, calcule $x = r^2 \bmod n$, $e = h(M \| x)$ et $y = rs^e \bmod n$. La signature de M est (e, y). Le vérificateur calcule $v = u^e y^2 \bmod n$ puis $e' = h(M \| v)$ et n'accepte la signature que si $e' = e$.

1) Montrer que ce schéma est correct, i.e. que si (e, y) est valide on a bien $e' = e$.

2) Supposons que z étant pris au hasard, la probabilité pour que $h(z)$ soit pair vaut $1/2$. Montrer comment un adversaire peut signer un message M donné, de façon probabiliste. On pourra commencer par traiter le cas $m = 1$.

Exercice 7 – [Chiffrement à clé publique de Schmidt-Samoa]

Soient p et q deux grands nombres premiers distincts vérifiant $p \nmid q-1$ et $q \nmid p-1$. On pose $n = p^2q$ et $r = \text{ppcm}(p-1, q-1)$.

1) Comment peut-on calculer r de façon économique à partir de p et q ?

2) Montrer que n est inversible modulo r. On notera d l'inverse de n modulo r.

3) Bob choisit p et q comme précédemment et publie n. Il calcule alors r et d. Comment procède-t-il pour calculer d ? La clé secrète de Bob est le triplet (p, q, d).

4) Alice désire envoyer un message à Bob. Les messages possibles sont les entiers M tels que $0 < M < pq$ et $\text{pgcd}(M, pq) = 1$ (que l'on peut identifier aux éléments de $(\mathbb{Z}/pq\mathbb{Z})^\times$). Montrer que $M^r \equiv 1 \bmod p$ et $M^r \equiv 1 \bmod q$.

5) Alice chiffre M en calculant $C = M^n \bmod n$, puis elle envoie C à Bob. Quels calculs Bob effectue-t-il pour retrouver M ?

6) Exemple. On prend $p = 13$, $q = 19$. Alice envoie $C = 2$ à Bob. Retrouver M.