université de BORDEAUX	**ANNÉE UNIVERSITAIRE 2020-2021** **Examen - Session 1 de Printemps** **Parcours :** Master CSI **UE :** 4TCY802U **Épreuve :** Cryptologie **Date :** 12 mai 2021 **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.

Exercice 1 – [LFSR]
Soit $s = (s_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ la suite périodique de période 14 et dont les 14 premiers termes sont $1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0$.

1) Déterminer la complexité linéaire de s et la plus courte relation de récurrence linéaire satisfaite par s.

2) Soit $t = (t_i)_{i\geq 0} = (s_{2i})_{i\geq 0}$. Quelle est la période de t ? La suite t est-elle une MLS ? Justifier.

Exercice 2 – [Un système peu sûr]
Alice et Bob décident d'utiliser un système asymétrique plus économique que RSA en termes de coût du déchiffrement. Alice choisit un module RSA $N = pq$ et un entier g premier avec N. Elle prend au hasard des entiers $r_1, r_2 > 0$, calcule $g_1 = g^{r_1(p-1)} \bmod N$ et $g_2 = g^{r_2(q-1)} \bmod N$. Sa clé publique est (N, g_1, g_2), sa clé secrète est (p, q). Bob, qui désire lui envoyer $m \in \mathbb{Z}/N\mathbb{Z}$, prend au hasard deux entiers $s_1, s_2 > 0$, calcule $c_1 = mg_1^{s_1} \bmod N$ et $c_2 = mg_2^{s_2} \bmod N$ et envoie $c = (c_1, c_2)$ à Alice.

1) Comment Alice peut-elle déchiffrer c efficacement ?

2) Expliquer en quoi ce système n'est pas sûr.

Exercice 3 – [RSA]
Bob utilise RSA et sa clé publique est $(N, 3)$. Alice veut lui envoyer deux messages $m_1, m_2 \in \{0, 1, \ldots, N-1\}$ vérifiant $0 < m_1 < m_2$. Les chiffrés sont c_1 et c_2. Ève les intercepte et un espion lui communique $\delta = m_2 - m_1$.

1) Exprimer $3\delta^3 + 3\delta^2 m_1 + 3\delta m_1^2$ et $3m_1^3 + 3\delta^2 m_1 + 3\delta m_1^2$ en fonction de c_1, c_2 et δ.

2) En déduire comment Ève peut retrouver m_1 et m_2 si $3\delta^3 + 3\delta^2 m_1 + 3\delta m_1^2 \neq 0 \bmod N$. On donnera le détail de ses calculs.

Exercice 4 – [RSA]
Soient $N = pq$ un module RSA et $0 < e < \varphi(N)$ un exposant de chiffrement RSA, vérifiant donc $\mathrm{pgcd}(e, \varphi(N)) = 1$. On a coutume de prendre comme exposant de déchiffrement l'entier $0 < d < \varphi(N)$ vérifiant $ed = 1 \bmod \varphi(N)$.

1) Montrer qu'en fait un entier $0 < d < \varphi(N)$ est un exposant de déchiffrement valable <u>si et seulement si</u> $ed = 1 \bmod \lambda(N)$, où $\lambda(N) = \dfrac{\varphi(N)}{\mathrm{pgcd}(p-1, q-1)}$.

2) Combien y a-t-il de tels d dans l'intervalle $]0, \varphi(N)[$ et comment choisir p et q pour minimiser ce nombre ?

Exercice 5 – [Rabin]
Soient p et q deux premiers distincts congrus à 3 modulo 4 et $N = pq$.

1) Soit c un carré de $(\mathbb{Z}/N\mathbb{Z})^\times$. Combien c admet-il de racines quatrièmes ? Justifier.

2) On prend $p = 31$, $q = 43$ et $N = 1333$. Vérifier que 470 est un carré de $(\mathbb{Z}/N\mathbb{Z})^\times$ et déterminer ses racines quatrièmes.

Exercice 6 – [Logarithme discret]
Soit un premier p vérifiant $p = 5 \bmod 8$.

1) Montrer que $2^{\frac{p-1}{2}} = -1 \bmod p$.

2) En étudiant le cas $p = 109$, montrer que 2 n'est pas nécessairement une racine primitive modulo p.

3) Soit c un carré non nul modulo p.

(a) Montrer que $c^{\frac{p-1}{4}} = \pm 1 \bmod p$.

(b) Si $c^{\frac{p-1}{4}} = 1 \bmod p$, montrer que $c^{\frac{p+3}{8}}$ est une racine carrée de c modulo p.

(c) Si $c^{\frac{p-1}{4}} = -1 \bmod p$, calculer $(4c)^{\frac{p+3}{4}} \bmod p$ et en déduire une formule pour une racine carrée de c modulo p.

4) Dans la suite $p = 101$. Montrer que 2 est une racine primitive modulo p.

5) Soit $x \in \{0, 1, \dots, p-2\}$ tel que $2^x \bmod p = 55$. On note $x_{k-1} \cdots x_1 x_0$ l'écriture binaire de x, i.e. $x = \sum_0^{k-1} x_i 2^i$, où $k \geq 2$ est le nombre de bits de l'écriture binaire de $p-2$ (les x_i peuvent être nuls à partir d'un certain rang). Déterminer x_0.

6) En utilisant la question 3 déterminer x_1. On pourra admettre que $78^{25} = 1 \bmod p$ et que $78^{13} = 52 \bmod p$.

7) Sachant que $2^{17} = 75 \bmod p$, $2^{62} = 45 \bmod p$ et $55 \times 2^{56} = 15 \bmod p$, retrouver x et vérifier que les bits x_0 et x_1 précédemment calculés sont exacts.

Exercice 7 – [Signature de Schnorr]
Soient p et q deux premiers impairs tels qu'il existe un entier naturel r vérifiant $p = qr + 1$. Soit h un entier vérifiant $1 < h < p$ et $h^r \neq 1 \bmod p$. Posons $g = h^r \bmod p$ et considérons $G = \langle g \rangle$ le sous-groupe de $\mathbb{F}_p^\times$ engendré par g.

1) Montrer que G est l'unique sous-groupe de $\mathbb{F}_p^\times$ de cardinal q.

2) Montrer que tout $g' \neq 1$ de G est aussi un générateur de G.

3) Soit $x \in \mathbb{F}_p^\times$. Montrer que $x \in G$ si et seulement si $x^q = 1 \bmod p$.

4) On garde les notations précédentes et on suppose que le problème du logarithme discret est difficile dans G. Le protocole de signature de Schnorr est le suivant. Les messages à signer sont les éléments de $\{0,1\}^*$. Soit $h : \{0,1\}^* \to \mathbb{F}_q$ une fonction de hachage. Alice choisit $x \in \mathbb{F}_q^\times$ qui sera sa clé secrète. Elle calcule $y = g^x \in G$ qu'elle publie. Pour signer M elle prend un aléa $k \in \mathbb{F}_q^\times$ qu'elle garde secret, détermine ℓ l'écriture binaire de $g^k \in G$, calcule $e = h(\ell \| M)$ et $s = k - xe \bmod q$. Sa signature est le couple (s, e). La fonction h et les quantités p, q, g, y sont connues de tous. Comment Bob vérifie-t-il la signature d'Alice ?

5) Est-il dangereux de se servir du même aléa k pour signer deux messages différents ?

6) Quelle(s) propriété(s) doit posséder h pour se prémunir contre des falsifications existentielles ?

Exercice 8 – [Signature ElGamal]
Le but de cet exercice est d'étudier un cas particulier d'une attaque proposée par Bleichenbacher contre la signature ElGamal lorsque les paramètres du système sont mal choisis. On suppose que p est un premier vérifiant $p = 1 \bmod 4$ et que 2 est une racine primitive modulo p. La clé publique d'Alice qui utilise le système ElGamal est $(p, 2, 2^s \bmod p)$ et sa clé secrète est l'entier s. Dans la question 4 on utilise le protocole de signature ElGamal sans fonction de hachage.

1) Montrer que $2^{\frac{p-3}{2}} = \frac{p-1}{2} \bmod p$.

2) Montrer que $\frac{p-3}{2}$ et $p-1$ sont premiers entre eux.

3) Rappeler comment Ève peut déterminer la parité de s. Justifier.

4) Montrer comment Ève, qui ne connaît pas s, peut se faire passer pour Alice en signant n'importe quel message M par (u, v) en prenant $u = \frac{p-1}{2}$ et un v approprié que l'on définira. On distinguera les cas s paire et s impaire.

5) Le recours habituel à une fonction de hachage publique h, qui consiste à construire la signature à partir de $h(M)$ plutôt qu'à partir de M, permet-il d'éviter cet écueil ?