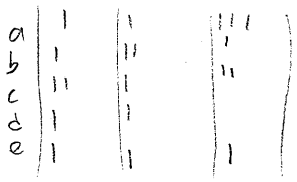
université de BORDEAUX	**ANNÉE UNIVERSITAIRE 2022-2023** **Examen - Session 1 de Printemps 2023** **Parcours :** Master CSI **UE :** 4TCY802U **Épreuve :** Cryptologie **Date :** 10 mai 2023 **Heure :** 14h30 **Durée :** 3h Documents : aucun document autorisé Épreuve de M. Cerri	**Collège Sciences et Technologies** **Masters**

L'usage de la calculatrice est autorisé.
La qualité de l'argumentation et de la rédaction sera un facteur d'appréciation.

Exercice 1 – On considère un système cryptographique à clé secrète. L'espace des messages clairs est $\mathcal{M} = \{x, y, z\}$, celui des messages chiffrés est $\{a, b, c, d, e\}$ et celui des clés supposées équiprobables est $\mathcal{K} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Le principe du chiffrement est explicité dans le tableau incomplet suivant.

$\mathcal{M}$ \ $\mathcal{K}$	1	2	3	4	5	6	7	8	9
x	a	α	ϕ	b	b	c	c	d	e
y	b	c	d	a	c	e	b	α	a
z	c	d	b	c	a	a	a	e	b



Comme d'habitude, on suppose que les variables K et M sont indépendantes.

(1) Compléter le tableau de manière à ce que le système soit à confidentialité parfaite. Justifier.
(2) Quelles sont les probabilités d'imposture et de substitution de ce système ?
(3) En utilisant toujours 9 clés, 3 clairs, 5 chiffrés (ils doivent tous être utilisés), proposer un système à confidentialité parfaite dont les probabilités d'imposture et de substitution sont meilleures que celles du précédent système. Présenter ce système sous forme de tableau et justifier les valeurs des probabilités d'imposture et de substitution. On supposera toujours les clés équiprobables et, pour simplifier, on supposera également les clairs équiprobables. Les clés chiffrent bien sûr différemment : les colonnes du tableau sont deux à deux distinctes.

Exercice 2 – Soit $s = (s_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ la suite définie par la relation de récurrence linéaire

$$s_{i+6} = s_{i+5} + s_{i+2} + s_{i+1} + s_i \quad \text{pour tout } i \geq 0,$$

et de graine $1, 0, 0, 0, 0, 0$. Soit $t = (t_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ la suite *périodique* de période 15 et dont les 15 premiers termes sont $1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0$.

(1) Sans chercher à calculer les premiers termes de s, déterminer sa période.
(2) Trouver la plus courte relation de récurrence linéaire satisfaite par t.
(3) Quelle est la complexité linéaire de $s + t$? La suite $s + t$ est-elle une MLS ?

Exercice 3 –

(1) On considère le système RSA de clé publique $(N, 3)$ où $N = 23 \times 47 = 1081$. Trouver tous les messages clairs M dont le chiffré C vérifie $C + M = 0 \bmod N$.
(2) Même question avec la clé publique $(N, 3)$ où $N = 17 \times 41 = 697$.
(3) Combien de clairs M chiffrés C vérifient $C + M = 0 \bmod N$ pour un système RSA de clé publique $(N, 3)$ quelconque ? On discutera suivant le choix des premiers impairs p et q tels que $N = pq$.
(4) Pour un système RSA de clé publique $(N, 3)$, combien de clairs M signés S (sans recours à une fonction de hachage) vérifient :
   (a) $S + M = 0 \bmod N$?
   (b) $S = M$?
(5) Si Alice utilise un système RSA de clé publique $(N, 3)$ et envoie un message $M \neq 0, \pm 1 \bmod N$ signé $S = M$ à Bob, celui-ci est-il en mesure de factoriser N ? Et si oui, comment ?

Exercice 4 –

(1) Soient un entier $k > 0$ et r un premier impair. Montrer qu'un entier x vérifie $x^2 = 1 \bmod r^k$ si et seulement si $x = \pm 1 \bmod r^k$.
(2) On considère le système RSA de clé publique (N, e) où $N = pq$. On note E sa fonction de chiffrement.
   (a) Montrer que la fonction E permet également de déchiffrer, i.e. E est involutive, si et seulement si $\text{ppcm}(p - 1, q - 1)$ divise $e^2 - 1$.

(b) On prend $N = 37 \times 101 = 3737$. À l'aide du théorème des restes chinois et de la question 1, trouver *tous* les exposants de chiffrement $0 < e < \varphi(N)$ vérifiant $e \neq \pm 1 \bmod (p-1)$, $e \neq \pm 1 \bmod (q-1)$ et tels que E soit involutive.

Exercice 5 – Soient p un grand premier, α une racine primitive modulo p et $\beta \in \mathbb{F}_p^\times \setminus \{1\}$. On identifie $\mathbb{F}_p$ et $\{0, 1, \ldots, p-1\}$. Soit un entier $n > 0$. Pour $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in \{0,1\}^n$, on pose

$$\begin{aligned} x_1 &= \beta^{\varepsilon_1}\alpha \bmod p \\ x_2 &= \beta^{\varepsilon_2}\alpha^{x_1} \bmod p \\ &\vdots \\ x_{i+1} &= \beta^{\varepsilon_{i+1}}\alpha^{x_i} \bmod p \\ &\vdots \\ x_n &= \beta^{\varepsilon_n}\alpha^{x_{n-1}} \bmod p \end{aligned}$$

et

$$F(\varepsilon) = x_n.$$

(1) Donner une condition suffisante sur n pour que F admette au moins une collision, i.e. pour qu'il existe ε et $\varepsilon' \in \{0,1\}^n$ vérifiant $\varepsilon \neq \varepsilon'$ et $F(\varepsilon) = F(\varepsilon')$.
(2) Admettons qu'on obtienne une collision. Montrer que l'on peut alors déterminer le logarithme discret de β en base α.

Exercice 6 – Alice utilise le chiffrement asymétrique de Goldwasser-Micali. Elle choisit deux grands premiers distincts p et q, calcule $n = pq$ et détermine un entier g qui n'est pas un carré modulo n et qui vérifie $\left(\frac{g}{n}\right) = 1$. Sa clé publique est (n, g) et sa clé privée (p, q). Pour chiffrer un bit $m \in \{0,1\}$, Bob tire au hasard $h \in (\mathbb{Z}/n\mathbb{Z})^\times$ et calcule $c = g^m h^2 \mod n$.

(1) Sur quel problème réputé difficile la sécurité du système repose-t-elle ?
(2) À quelle condition nécessaire et suffisante sur p et q peut-on prendre $g = n - 1$?
(3) Si m et m' sont chiffrés en c et c', construire un chiffré de $m \oplus m'$ et un chiffré de $1 \oplus m$, où $\oplus$ désigne l'addition modulo 2.
(4) Montrer qu'Alice peut déchiffrer en calculant un seul symbole de Legendre.
(5) Exemple pédagogique. Alice choisit $p = 59$, $q = 239$ et donc $n = 14101$.
  (a) Montrer que $g = 3365$ convient.
  (b) Alice choisit désormais ce g. Bob chiffre un bit m en $c = 2022$. Que vaut m ?
  (c) Alice, qui est curieuse, désire savoir quel h a utilisé Bob. Comment peut-elle procéder efficacement et combien de candidats obtiendra-t-elle ? On demande juste de décrire ses calculs, non de les effectuer.
  (d) Alice peut-elle recevoir le chiffré 2023 ?

Exercice 7 – Alice utilise le schéma de signature ElGamal de clé publique $(p, g, g^s \bmod p)$ et désire signer successivement les messages M_1, M_2, M_3, etc. Afin d'économiser du temps dans la génération des nombres aléatoires k qui sont utilisés pour signer les messages, Alice choisit deux entiers k et δ premiers avec $p-1$ puis signe le i-ième message en utilisant la valeur $k_i = k\delta^{i-1} \bmod (p-1)$, i.e. signe M_1 en utilisant k, M_2 en utilisant $k\delta$, M_3 en utilisant $k\delta^2$, etc. Ainsi, pour signer M_{i+1} elle utilise $k_{i+1} = k_i\delta \bmod (p-1)$, une seule mutiplication modulaire lui suffisant pour déterminer k_{i+1} à partir de k_i.

(1) Expliquer pourquoi les k_i utilisés sont des choix valides pour signer les messages M_i.
(2) Supposons qu'Oscar sait qu'elle procède ainsi et connaît δ. Il observe deux messages signés consécutifs M_i et M_{i+1} de signatures respectives (u_i, v_i) et (u_{i+1}, v_{i+1}).
  (a) Décrire comment Oscar peut chercher à calculer s la clef secrète d'Alice sans résoudre une instance du problème du logarithme discret. Combien de candidats obtient-il pour s ?
  (b) Application numérique jouet.
    (i) Soit le premier $p = 257$. Calculer $\left(\frac{5}{p}\right)$ à l'aide de la loi de réciprocité quadratique et en déduire que 5 est une racine primitive modulo p.
    (ii) La clé publique d'Alice est $(257, 5, 237)$, $M_i = 10$ est signé $(230, 212)$, $M_{i+1} = 38$ est signé $(97, 85)$ et Oscar sait que $\delta = 13$. Donner le détail des calculs d'Oscar et retrouver s.
  (c) Sous les mêmes hypothèses, est-ce que construire la signature à partir de $h(M)$ où h est une fonction de hachage publique résistante à la préimage permet d'éviter cette attaque ?

Université de Bordeaux
Collège Sciences et Technologies
Année 2022-2023

Master CSI
Cryptologie

Devoir Surveillé, 22 février 2023

Durée 1h30, documents interdits

La qualité de la rédaction sera un facteur d'appréciation.

Exercice 1 – On considère un cryptosystème symétrique dans lequel l'espace des clairs et l'espace des chiffrés sont finis de même cardinal : $|\mathcal{M}| = |\mathcal{C}|$. Quelles sont les probabilités d'imposture et de substitution de ce système ?

Exercice 2 – On considère un système de chiffrement symétrique où l'espace des messages clairs est $\mathcal{M} = \{a, b, c\}$, l'espace des messages chiffrés est $\mathcal{C} = \{1, 2, 3, 4, 5, 6\}$ et celui des clés est $\mathcal{K} = \{\text{i}, \text{ii}, \text{iii}, \text{iv}, \text{v}, \text{vi}, \text{vii}, \text{viii}, \text{ix}\}$. Le système est décrit par le tableau suivant dont certaines cases ont été effacées :

$\mathcal{M}$ \ $\mathcal{K}$	i	ii	iii	iv	v	vi	vii	viii	ix
a		1		5		4	2	6	6
b	2			1	6	3	5	2	4
c	6	5		4	1	1		3	

On suppose, comme d'habitude, que la clé est indépendante du message clair. On suppose également que les clés sont équiprobables et, pour simplifier, que les messages clairs le sont aussi.

(1) Remplir les cases vides de manière à rendre le système à confidentialité parfaite. Justifier.
(2) Quelles sont les probabilités d'imposture et de substitution du système ?

Exercice 3 – On s'intéresse ici au mode opératoire dit PCBC (Plaintext Cipher Block Chaining) utilisé pour un chiffrement par bloc à clé secrète. Le fonctionnement en est le suivant. Alice désire envoyer à Bob le clair $M = m_1 \| m_2 \| \dots \| m_s$ où les m_i sont des blocs de l bits et $s \geq 2$. Leur clé secrète est K, la fonction de chiffrement qui va de $\{0,1\}^l$ dans $\{0,1\}^l$ est notée E_K et celle de déchiffrement D_K.

- Elle prend un bloc aléatoire initial de l bits $IV = c_0$;
- Elle calcule $c_1 = E_K(m_1 \oplus c_0)$;
- Pour $2 \leq i \leq s$ elle calcule $c_i = E_K(m_i \oplus m_{i-1} \oplus c_{i-1})$;
- Le chiffré envoyé à Bob est $C = c_0 \| c_1 \| \dots \| c_s$.

(1) Décrire l'algorithme de déchiffrement.
(2) Un attaquant intercepte C et le transforme en substituant à un c_i un $c'_i \neq c_i$. Que se passera-t-il au cours du déchiffrement ?
(3) Alice et Bob veulent exploiter cette propriété en terminant toujours les messages clairs à envoyer par un bloc m_s fixé d'avance et connu d'eux seuls. Ainsi, si une attaque de ce type a lieu, Bob le saura car il ne retrouvera pas m_s lors du déchiffrement. Montrer que malgré tout, si $s \geq 4$, l'attaquant peut intervertir

deux blocs chiffrés consécutifs, c_j et c_{j+1} avec $1 < j < j+1 < s$, sans que Bob s'en aperçoive.

Exercice 4 – Soit $s = (s_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ une suite périodique de période 7 et dont les 7 premiers termes sont $0, 1, 0, 1, 1, 0, 0$. Soit $t = (t_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ la suite engendrée par la relation de récurrence linéaire $t_{i+8} = t_{i+7} + t_{i+4} + t_{i+3} + t_i$ pour tout $i \geq 0$ et de graine $1, 1, 0, 1, 0, 1, 0, 0$. Soit enfin $u = (u_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ la suite définie par $u_i = s_i + t_{2i}$ pour tout $i \geq 0$.

(1) Expliquer pourquoi s n'est pas une MLS.
(2) Déterminer la complexité linéaire de s et la plus courte relation de récurrence linéaire satisfaite par s.
(3) Montrer que X^5+X^2+1 est irréductible dans $\mathbb{F}_2[X]$ et en déduire la décomposition en produit d'irréductibles de $X^8 + X^7 + X^4 + X^3 + 1$.
(4) Déterminer la plus courte relation de récurrence linéaire satisfaite par t.
(5) Quelle est la période de t ? La suite t est-elle une MLS ?
(6) Déterminer la complexité linéaire de u et la plus courte relation de récurrence linéaire satisfaite par u.
(7) Quelle est la période de u ?

Exercice 5 – Soit le premier $p = 503$. Est-ce que 202 est un carré modulo p ?