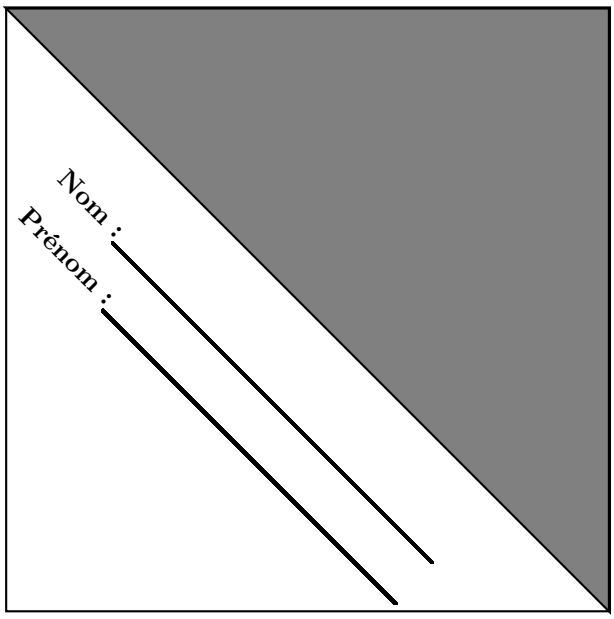
Université de Nice-Sophia Antipolis
SI5, Caspar & M2 informatique et interactions
Cryptographie & Sécurité 2020–2021

Examen de octobre 2021

Durée : 1h30

Note :



L'examen comporte 3 parties indépendantes. Veuillez répondre sur la copie avec clarté et concision.

1 Construction d'une boîte S et analyse [11 points]

1. On travaille dans dans GF(2^3), corps à 8 éléments obtenu par la relation $\mathbb{F}_2[x]/(x^3+x+1)\mathbb{F}_2[x]$. On associera à la valeur octale 6 le mot binaire 110 (bit de poids faible à gauche) et le polynôme x^2+x. Complétez la table de multiplication en exprimant les éléments en binaire.

		000	001	010	100	011	101	110	111
		0	1	x	x^2	$x+1$	x^2+1	x^2+x	x^2+x+1
000	0	000	000	000	000	000	000	000	000
001	1	000	001	010	100	011	101	110	111
010	x	000	010	100	011	110	001	111	101
100	x^2	000	100	011	110	111	010	101	001
011	$x+1$	000	011	.	.	.	.	.	.
101	x^2+1	000	101	.	.	.	.	.	.
110	x^2+x	000	110	.	.	.	.	.	.
111	x^2+x+1	000	111	101	001	010	110	100	011

2. Grace à la table de multiplication, complétez la table des inverses des éléments de GF(2^3).

1	001	1	1	001	1
2	010	x	x^2+1	101	5
3	011	$x+1$	.	.	.
4	100	x^2	.	.	.

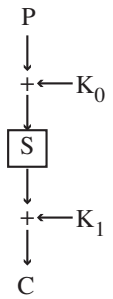
Au moyen de ces calculs préliminaires, on construit une boîte S selon la construction de S-AES :

1. convertir le nibble d'entrée en un polynôme $p(x)$;
2. inverser le polynôme obtenu précédemment pour obtenir le polynôme $\text{inv}(x)$;
3. associer à $\text{inv}(x)$ son polynôme dans $\mathbb{F}_2[y]/y^3 - 1 = N(y)$
4. calculer $a(y)N(y) + b(y) \mod y^3 - 1$ avec $a(y) = y^2$ et $b(y) = y$.

3. Complétez la table de la boîte S ci-dessous :

$p(x)$	$N(y)$	$N(y) * (y^2)$	$+y$	résultat
000	000	000	010	010
001	001	100	110	110
010	101	110	100	100
011	.	.	.	.
100	.	.	.	.
101	010	001	011	011
110	.	.	.	.
111	.	.	.	.

On considère le chiffre suivant (appelé Even et Mansour Additif) qui utilise la boîte S ci-dessus et deux clés de tour K_0 et K_1. La boîte S est la permutation définie ci-dessus et les '+' représentent des additions dans le corps de Galois GF(2^3) engendré par le polynôme $x^3 + x + 1$. Cette addition correspond ici à une opération de ou exclusif bit à bit.



4. Précisez quelle est la taille de P en bits et quelle est la taille de la clé (complète) en bits.

5. Expliquez comment on peut déchiffrer un cryptogramme au moyen de ce chiffre.

6. Cherchez les valeurs de ΔY pour un ΔX fixé à la valeur octale de 4 (100 en binaire) :

X	Y	X'	Y'	ΔY
000				
001				
010				
011				
100				
101				
110				
111				

7. Listez celles qui apparaîssent le plus fréquemment en donnant les probabilités associées :

8. Listez les bonnes paires associées à $(\Delta X, \Delta Y) = (100, 111)$.

9. Combien de tirages aléatoires peut-on réaliser pour "deviner" l'entrée de la boîte S avec les bonnes paires de la question **8** ?

10. Quelle est la complexité d'une attaque par recherche exhaustive de clé ?

2 Secret parfait [5 points]

Soit $n > 0$ un entier. Un *carré latin* de rang n est un tableau T de taille $n \times n$ qui contient les entiers $\{1, \ldots, n\}$ tel que chacun de ces n entiers apparaît une fois sur chaque ligne et sur chaque colonne (pour $n = 9$, c'est par exemple la solution d'un problème de sodoku).

1. Donnez un exemple de carré latin de rang 5.

Etant donné un carré latin T de rang n, on lui associe un chiffre pour lequel l'espace des clairs, des chiffrés et des clés est l'ensemble $\{1, \ldots, n\}$. Le clair m est chiffré avec la clé k en lisant le contenu $T[m, k]$ (ligne m, colonne k).

2. En utilisant l'exemple de la question **1.**, donnez un exemple de chiffrement sur un alphabet réduit à $\{1, \ldots, 5\}$.

3. Comment pourrait-on faire pour coder l'alphabet des lettres latines minuscules sur l'alphabet réduit à $\{1, \ldots, 5\}$? Vous pourrez identifier les lettres `i` et `j` pour simplifier.

4. Montrez que ce chiffre est parfait en expliquant sous quelles conditions.

3 Déchiffrement [4 points]

Déchiffrez le chiffré suivant obtenu par transposition simple à tableau avec le mot clé `MELANGE`.
`UCNU CSTA UAEE ELAA BNRT DRNA EEOS NIMA RNUA SEUA SRUB DUDE NHCE EOOA`

M	E	L	A	N	G	E

Le chiffré en français est un haiku [1] et le caractère de bourrage est la lettre `A`.
Inscrivez ci-dessous le haiku déchiffré :

1. Un haiku est un poème –japonais– court composé de 3 vers et de 17 découpages de phonèmes ;