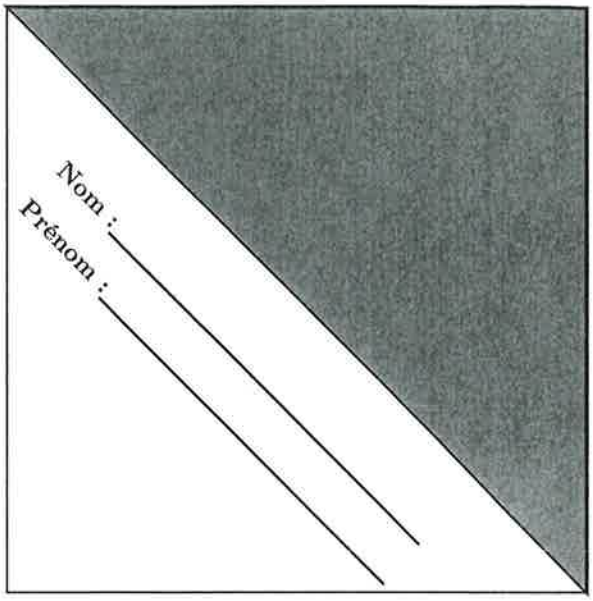
Université Côte d'Azur
SI5, Caspar & M2 informatique et interactions
Cryptographie & Sécurité 2020–2021

Examen octobre 2020

Durée : 1h30

Note :



L'examen comporte 2 parties indépendantes. Veuillez répondre sur la copie avec clarté et concision.

1 Cryptanalyse différentielle [16 points]

On définit une boîte S sur des mots binaires de longueur 3 au moyen de la substitution sur des entiers modulo 8 : $x \mapsto 3x + 7 \mod 8$. Les mots binaires sont représentés avec le bit de poids fort à gauche (par exemple 6 en décimal s'écrira 110 en binaire).

1. Décrivez la boîte S en base 8 (octal) et en binaire :

bin	oct	bin	oct
000	0	111	7
001	1	010	2
010	2	101	5
011	3	000	0
100	4	011	3
101	5	110	6
110	6	001	1
111	7	100	4

1

2. On utilise d'abord cette boîte S directement pour construire une clé pour le mode OFB. Calculez la suite des z_i pour $i = 1, 2, 3$ en choisissant 011 comme valeur initiale.

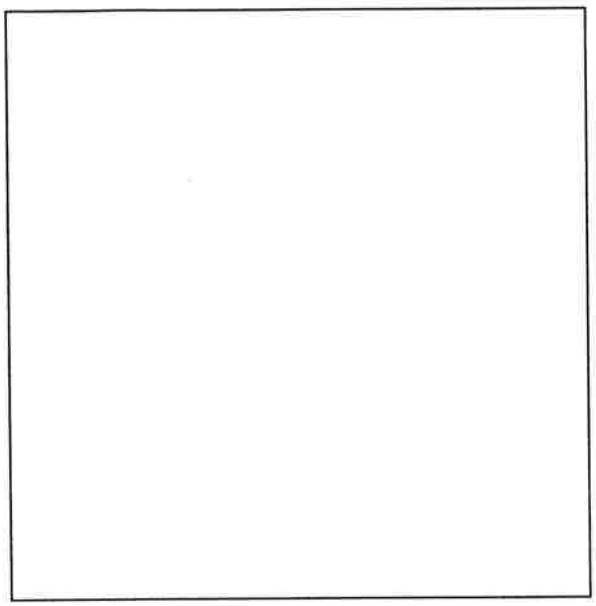
011 → 010 → 101 → 110.

1 **011 – 000 – 111 – 100**

3. Quel est l'intérêt cryptographique d'utiliser une valeur initiale non nulle ?

Assurer l'authentification A et B partagent IV.

1



La suite de l'exercice concerne l'étude de la cryptanalyse différentielle de la boîte S puis son intégration dans un modèle simplifié de chiffre.

4. Cherchez les valeurs de ΔY pour un ΔX fixé à la valeur octale de 2 (010 en binaire) :

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

2

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

1 $Pr(\Delta Y = 010 | \Delta x = 010) = 1$

5. Sauriez-vous expliquer le résultat particulier que vous avez obtenu ?

Tout est linéaire ! $S(x) = y = 3x - 1 \bmod 8$.

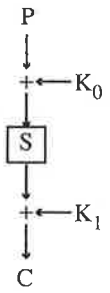
2 $x \to 3x - 1 = y$ ⟹ $\Delta x \Rightarrow 3\Delta x - 2 = \Delta y \Rightarrow \Delta y$ constant

$x' \to 3x' - 1 = y'$

6. Quelle serait la probabilité d'apparition de chaque ΔY si la boîte S était parfaite ?

1 1/8

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 $x^3 + x^2 + 1$.



7. On travaille dans dans GF(2^3), corps à 8 éléments obtenu par la relation $\mathbb{F}_2[x]/(x^3+x^2+1)\mathbb{F}_2[x]$. On associera à la valeur octale 6 le mot binaire 110 (comme ci-dessus) et le polynôme x^2+x. Donnez la table d'addition 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	001	010	100	011	101	110	111
001	1	001	000	011	101	010	100	111	110
010	x	010	011	000	110	001	111	100	101
100	x^2	100	101	110	000	111	001	010	011
011	$x+1$	011	010	001	111	000	110	101	100
101	x^2+1	101	100	111	001	110	000	011	010
110	x^2+x	110	111	100	010	101	011	000	001
111	x^2+x+1	111	110	101	011	100	010	001	000

2

8. Expliquez comment déchiffrer un cryptogramme en connaissant la clé.

On fait "remonter" C : $S^{-1}(C+K_1)+K_0$

1

9. Retrouvez le clair correspondant au chiffré 001 obtenu avec les clés de tour $K_0K_1 = 011.101$.

001 + 101 = 100 → 111 + 011 = 100

C + K_1 S^{-1} K_0

1

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

La clé est sur 6 bits. Rech. exhaustive : 2^6

1

11. Expliquez le fonctionnement d'une cryptanalyse différentielle sur ce chiffre et dites s'il vaut mieux faire une attaque par force brute ou une cryptanalyse.

On cherche des bits de K_1 avec une attaque CPA
On a les clairs P, les chiffrés correspondants et on cherche K_1 avec un ΔP fixé. Ici les bonnes paires d'entrées = sortie.

2

Il vaut mieux faire une attaque par force brute

2 Secret parfait [4 points]

Soit M un mot de ℓ lettres sur l'alphabet $\{a, \ldots, z\}$. Chaque lettre m_i du message est codée par un entier modulo 26. la clé k définit un décalage comme dans le chiffre de César. L'opération de chiffrement est : $\text{Enc}(k, (m_1, \ldots, m_\ell)) = (m_1 + k \mod 26; \ldots, m_\ell + k \mod 26)$.

2

1. Montrez que le chiffre par substitution défini ci-dessus vérifie la condition du secret parfait lorsque $\ell = 1$.

Si $\ell = 1$, on vérifie la cond. du secret parfait. $\forall m, c \in \{a, \ldots, z\}$ seule une clé associe c à m d'où

$$\Pr[\text{Enc}(k, m) = c] = 1/26$$

Donc $\forall m_1, m_2 \in \{a, \ldots, z\}$ on a

$$\Pr[\text{Enc}(k, m_1) = c] = \Pr[\text{Enc}(k, m_2) = c] = 1/26$$
$$\Pr[C = c \mid M = m_1] = \Pr[C = c \mid M = m_2] = 1/26$$

✓

2. Expliquez la raison pour laquelle il n'est pas possible de généraliser ce résultat pour affirmer qu'un chiffre commme celui de Vigenère assure le secret parfait.

2

Vigenère est défini pour 1 long. de clé fixée (n). La ni clé est réutilisée au bout des n caractères, contredisant la non-réutilisation d'une clé.