Université Côte d'Azur
SI5, CyberSec & M2 informatique et interactions
Cryptographie & Sécurité 2022–2023

Examen octobre 2022

Durée : 1h30

Note :

Nom :
Prénom :

L'examen comporte 2 parties indépendantes suivi d'un exercice de synthèse. Veuillez répondre sur la copie avec clarté et concision.

1 Sécurité parfaite [5 points]

On considère le tableau suivant qui permet une représentation graphique alternative des entiers de 1 à 9 en utilisant les traits qui encadrent ces nombres et le point pour représenter le zéro.

1	2	3
4	5	6
7	8	9

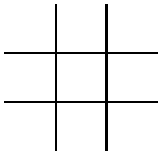
Par exemple 07 89 12 34 56 sera représenté comme indiqué par la figure 1.

FIGURE 1 – représentation de l'exemple 07 89 12 34 56 (ce n'est pas mon numéro de téléphone !)

1. Dites s'il s'agit d'une représentation qui assure le codage ou le chiffrement (ou les deux) en justifiant votre réponse.

On veut rendre cette représentation plus compliquée en appliquant aux entiers du tableau l'opération $x \mapsto 3.x \mod 10$.

2. Complétez le tableau issu de la transformation ci-dessus.



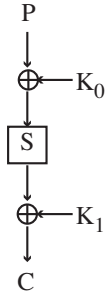
3. Donnez la représentation de 20221005 avec ce nouveau tableau.

4. Expliquez comment vous construiriez un chiffre à clé secrète utilisant cette représentation en expliquant notamment quel est l'espace des clairs, celui des clés et celui des chiffrés.

5. Cette représentation permet de construire un chiffre assurant le secret parfait. Pouvez-vous dire et justifier sous quelles conditions ?

2 Chiffre d'Even et Mansour [12 points]

On souhaite cryptanalyser le chiffre suivant (appelé Even et Mansour) qui utilise la boîte S ci-après et deux clés de tour K_0 et K_1



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

1. Chiffrez tout d'abord le clair `101` avec comme clés de tour : $K_0K_1 = 100.010$:

2. En expliquant comment procéder, déchiffrez ensuite le chiffré `101` avec les mêmes clés de tour : $K_0K_1 = 100.010$:

On veut utiliser ce chiffre avec la clé $K_0K_1 = 100.010$ en mode OFB pour chiffrer le texte `UN` (on rappelle que `A` est codé en `00000`, `B` en `00001`, ... ; la valeur de bourrage (padding) est `0`).
3. Expliquez comment `UN` est codé en binaire et donnez la chaîne binaire complète correspondante.

4. Chiffrez `UN` en mode OFB en utilisant le chiffre défini ci-dessus avec la clé $K_0K_1 = 100.010$ et d'IV=001 et donnez l'équivalent alphabétique correspondant.

On s'intéresse maintenant à la cryptanalyse différentielle de ce chiffre.

5. Cherchez les valeurs de ΔY pour un ΔX fixé à la valeur octale de 6 (110 en binaire) :

X	$Y = S(X)$	X'	$Y' = S(X')$	ΔY
000	001	110	011	
001	000			
010	111			
011	101			
100	010			
101	110			
110	011			
111	100			

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

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

7. Donnez les bonnes paires pour $\Delta X = 6$ et $\Delta Y = 2$.

8. Voici deux clés possibles : 001.010 et 100.001 ainsi que tous les couples clairs/chiffrés obtenus avec l'une des deux clés. Les couples sont dans l'ordre : clair en octal, clair en binaire et dans la dernière colonne, le chiffré en binaire.

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

Pouvez-vous dire quelle était la clé (parmi les deux proposées) qui a été utilisée (en le justifiant) ?

9. La question précédente fait référence à l'expérience de sécurité prouvée des deux messages. Exprimez-la et essayez de quantifier la probabilité de réussite de cette expérience.

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

11. A votre avis, quelle serait la meilleure tactique pour cryptanalyser ce chiffre ?

12. Dans la question 4, on a choisi une IV=001. Expliquer pourquoi l'IV n'est pas nulle ici et la propriété de sécurité qui est assurée. Comment peut-on transmettre la valeur de l'IV ?

3 Chaîne de chiffrement [3 points]

On veut combiner les deux systèmes de chiffrement précédents en utilisant le chiffre d'Even et Mansour pour chiffrer les clairs et le chiffre qui assure le secret parfait pour transmettre les clés utilisées par Even et Mansour.

1. Expliquez sous quel format vous transmettrez les diverses clés nécessaires au bon fonctionnement d'Even et Mansour.

2. Expliquez succinctement comment vous utiliseriez le chiffre assurant la sécurité parfaite pour chiffrer les diverses clés listées dans la question précédente.

3. Donnez les hypothèses nécessaires au bon fonctionnement de cette chaîne de chiffrement.