Université Côte d'Azur
SI5 & M2 informatique CyberSec
Cryptographie & Sécurité 2024–2025

Examen d'octobre 2024

Durée : 1h30

Note :

Nom :
Prénom :

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

1 Chiffre 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.

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

On souhaite utiliser le chiffrement par carré latin sur l'alphabet latin pour lequel on identifie les lettres `i` et `j`. Cet alphabet de 25 lettres est identifié à $\mathbb{Z}_{25}$.

4. Expliquez comment recoder cet alphabet de 25 lettres sur l'alphabet précédent à 5 symboles.

5. Donnez ensuite une manière de chiffrer le texte `BON` par la méthode du carré latin. Vous préciserez en particulier si votre méthode conserve la propriété du secret parfait.

2 Construction et analyse d'une boîte S [7 points]

On définit une boîte S comme dans S-AES, dans $\mathbb{F}_8 = \mathbb{F}_2[x]/x^3 + x + 1$. Les E/S sont des entiers qui ont une représentation binaire ou polynomiale associée comme par exemple : $3 \to 011 \to x + 1$. Rappelons la construction de la boîte S :

— convertir chaque nibble (de 3 bits) en polynôme ;
— inverser chaque nibble dans $\mathbb{F}_8$;
— associer à l'inverse son polynôme dans $\mathbb{F}_2[y]/y^3+1 = N(y)$;
— calculer $a(y)N(y)+b(y) \mod y^3+1$ avec $a = y^2$ et $b = 1$;

La table des inverses de $\mathbb{F}_8$ est donnée ci-dessous :

1	001	1	1	001	1
2	010	x	x^2+1	101	5
3	011	$x+1$	x^2+x	110	6
7	111	x^2+x+1	x^2	100	4

1. Vérifiez tout d'abord que x^2+1 est bien l'inverse de x dans $\mathbb{F}_8$.
2. Quelle est l'image de O (ou 000 en binaire) par la boîte S (justifiez) ?
3. Quelle est l'image de 5 (ou 101 en binaire) par la boîte S (justifiez) ?

4. Complétez enfin la table de la boîte S ci-dessous :

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

Votre service de cryptanalyse vous fournit la table des différentiels pour cette boîte S :

$\Delta Y >$	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	0	0	0	2	2	2	2
2	0	0	2	2	0	0	2	2
3	0	0	2	2	2	2	0	0
4	0	2	0	2	0	2	0	2
5	0	2	0	2	2	0	2	0
6	0	2	2	0	0	2	2	0
7	0	2	2	0	2	0	0	2

5. Retrouvez les valeurs de la table des différentiels pour $\Delta X = 5$ (ou 101 en binaire) :

X		$S(X)$	$X' = X \oplus \Delta X$	$S(X')$	ΔY	
int	bin	bin	bin	bin	bin	int
0	000					
1	001	111				
2	010	110				
3	011	000				
4	100	010				
5	101					
6	110	011				
7	111	100				

6. On cherche à trouver les bonnes paires pour la valeur de $\Delta X = 5$ et de $\Delta Y = 1$. Pour cela, aidez-vous du tableau précédent à partir duquel vous pouvez trouver l'information en expliquant votre démarche.
7. Expliquez pourquoi vous n'avez obtenu que deux bonnes paires.

3 Cryptanalyse différentielle [8 points]

On considère le chiffre de la figure 1 qui chiffre un clair $P = P_1P_2P_3$ de 3 bits en un chiffré $C = C_1C_2C_3$ de 3 bits. Le chiffre fonctionne en deux tours. Chaque tour i consiste en :
— un XOR avec la clé de tour K_i
— une substitution définie par une boîte S dont la permutation est définie par :

in	0	1	2	3	4	5	6	7
out	1	5	7	2	6	0	4	3

Il n'y a pas d'algorithme de séquencement de la clé. La clé K est de 6 bits $K = K_0K_1$.
1. Chiffrez le clair `100` avec la clé `100 001`.
2. Expliquez comment déchiffrer puis déchiffrez le chiffré `010` avec la clé `100 001`.

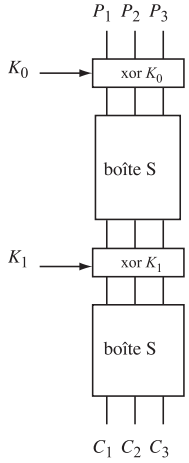

FIGURE 1 – Chiffre utilisé

3. Quelle est la complexité d'une attaque par recherche exhaustive de la clé ?
4. Expliquez pourquoi, dans le cas d'une cryptanalyse à clairs choisis, il est possible de considérer un chiffre plus simple, celui de la partie droite de la figure 2 où l'action de la seconde boîte S a été retiré. Dites pourquoi il est intéressant de retirer l'action de la dernière boîte S.

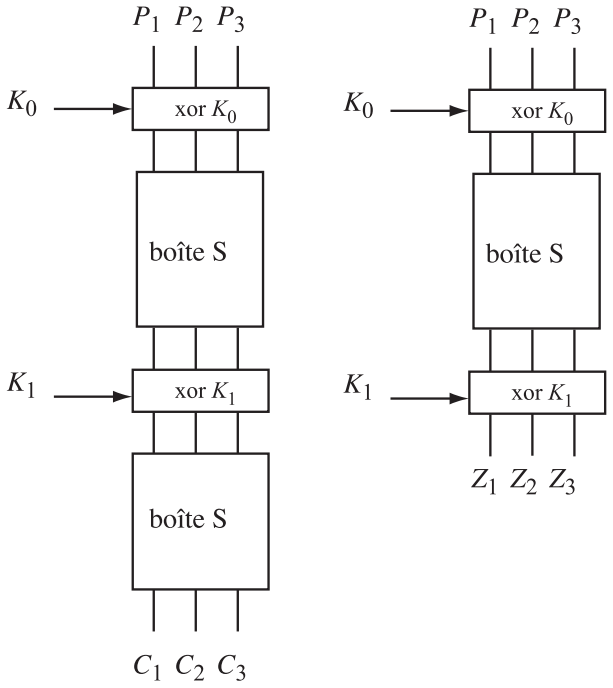

FIGURE 2 – Chiffre utilisé

On vous donne également la table des différentiels de la boîte S.

$\Delta Y >$	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	0	0	0	2	2	2	2
2	0	0	2	2	0	0	2	2
3	0	0	2	2	2	2	0	0
4	0	2	0	2	0	2	0	2
5	0	2	0	2	2	0	2	0
6	0	2	2	0	0	2	2	0
7	0	2	2	0	2	0	0	2

On cherche à effectuer la cryptanalyse différentielle du chiffre après avoir retiré l'action de la seconde boîte S, comme dans la partie droite de la figure 2 et qui satisfait l'égalité suivante :

$$Z = S(X) \oplus K_1 \qquad X = P \oplus K_0$$

pour $S(.)$ la fonction de la boîte S. On rappelle qu'il s'agit d'une attaque à clairs choisis.
Pour un $(\Delta X, \Delta Y)$ donné (ici `100`,`111`), seul un sous-ensemble de paires (P, P') correspond.
5. Déterminez la valeur de K_0 en supposant que $P' =$`001` a mené au $X' =$`100`.
6. Une fois déterminée la valeur de K_0, pour $P' =$`001`, montrez comment on peut retrouver K_1 sachant que $\{P'\}_{K=K_0K_1} =$`111` :
7. Comment peut-on vérifier que la clé K trouvée est la bonne et que doit-on faire si la clé K trouvée n'est pas la bonne ?
8. Dites en quoi on avait besoin de la table des différentiels pour conduire cette cryptanalyse.
Voici la liste des chiffrés en fonction du clair donné en entrée avec la clé à trouver :

P	0	1	2	3	4	5	6	7
$\{P\}_K$	6	7	3	1	5	0	4	2

La table des XOR sur les entiers est :

```
[0 1 2 3 4 5 6 7]
[1 0 3 2 5 4 7 6]
[2 3 0 1 6 7 4 5]
[3 2 1 0 7 6 5 4]
[4 5 6 7 0 1 2 3]
[5 4 7 6 1 0 3 2]
[6 7 4 5 2 3 0 1]
[7 6 5 4 3 2 1 0]
```