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

Examen octobre 2022

Durée : 1h30

Note :
15

Nom : DESOU
Prénom : Fanny

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.

C'est du ~~chiffrement~~ et codage si. En effet car le signal est codé mais on n'a ~~pas~~ clé qui est le tableau en lui même. donc c'est aussi du chiffrement.

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	6	9
2	5	8
1	4	7

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.

Avec un message m, on a une clé secrète k, on prend dans le tableau $T[m,k]$ qui donne le chiffré. Ainsi le chiffré de $m=3$ pour $k=2$ est 4 i.e. $\square$ $m \in \{1,2,3\}$ $k \in \{1,2,3\}$ $c \in \{\text{⊥}, \text{U}, \text{L}, \text{⅂}, \sqcap, \Gamma, \text{⅂}, \sqcap, \Gamma\}$

0

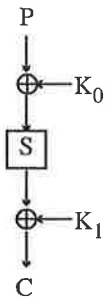
5. Cette représentation permet de construire un chiffre assurant le secret parfait. Pouvez-vous dire et justifier sous quelles conditions ?

Il faut que la table soit différente pour chaque chiffrement.
Ainsi alors on a k qui est choisi entre $\{1,2,3\}$ avec une probabilité de $1/3$
Et pour tout m relié à un chiffré, on a toutes un unique k qui correspond.
Ainsi suivant le théorème de Shannon, on a bien un secret parfait.

1

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

4

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

$C = S(P \oplus K_0) \oplus K_1 = S(101 \oplus 100) \oplus 010 = S(001) \oplus 010$

$C = 000 \oplus 010 = 010$

$\boxed{C = 010}$

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

On fait le chemin inverse : $P = S^{-1}(C \oplus K_1) \oplus K_0$

$P = S^{-1}(101 \oplus 010) \oplus 100 = S^{-1}(111) \oplus 100 = 010 \oplus 100$

$\boxed{P = 110}$

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.

On code U et N séparément, en mettant leur position dans l'alphabet -1 en binaire.

U = 10100 N = 01101 donc UN est codé 10100.01101 bourrage

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.

$z_0 = IV = 001$ $z_1 = ek(z_0) = ek(001) = S(001 \oplus 100) \oplus 010 = 100$

$z_1 = 100$ $z_2 = ek(z_1) = S(100 \oplus 100) \oplus 010 = 001 \oplus 010 = 011$

$z_2 = 011$

$x_1 \oplus z_1 = y_1$ $x_2 \oplus z_2 = y_2$

$10100 \oplus 10000 = 00100$ $01101 \oplus 00011 = 01110$

chiffré de U chiffré de N

→ "U" devient "D" → "N" devient "O" en chiffré

→ chiffré DO

mauvaise application du mode OFB

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	010
001	000	111	100	100
010	111	100	010	101
011	101	101	110	011
100	010	010	111	101
101	110	011	101	011
110	011	000	001	010
111	100	001	000	100

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

$P(\Delta Y = 010 \mid \Delta X = 110) = 2/8$; $P(\Delta Y = 100 \mid \Delta X = 110) = 2/8$

$P(\Delta Y = 101 \mid \Delta X = 110) = 2/8$; $P(\Delta Y = 011 \mid \Delta X = 110) = 2/8$

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

La probabilité d'apparition de chaque ΔY si S était parfaite serait **1/8**

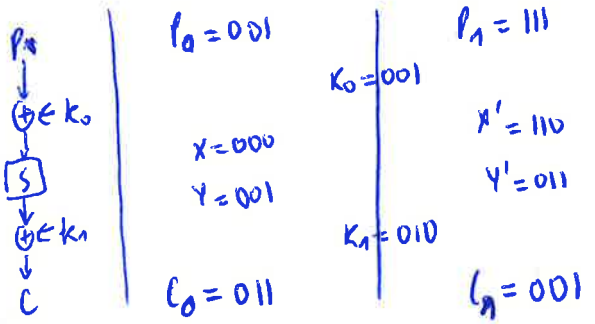
7. Donnez les bonnes paires pour $\Delta X = 6$ et $\Delta Y = 2$. (010)

$X = (000, 110)$ $X' = (110, 000)$

$Y = (001, 011)$ $Y' = (011, 001)$

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.

P	bin	C
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) ?

~~Prenons P=000 et C=000, on a donc $010 = S(K_0) \oplus K_1$~~

~~et $K_1 = S(101 \oplus K_0)$ donc $010 = S(K_0) \oplus S(101 \oplus K_0)$~~

~~Supposons $K_0 = 001$ alors $010 = S(101 \oplus 001) = S(100) = 010$~~

Prenons P_0 au hasard : $P_0 = 001$ pour $P_1 = P_0 \oplus \Delta X = 001 \oplus 110 = 111$

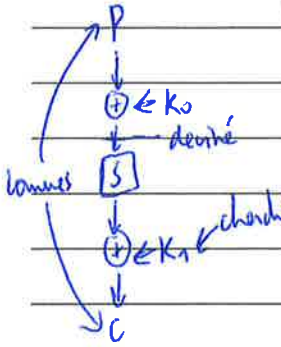
Nous les chiffrés correspondant C_0 et C_1 tq $C_0 = 011$ et $C_1 = 001$.
On a maintenant $C_0 \oplus C_1 = 04$ donc $\Delta Y = 011 \oplus 001 = 010$. On choisit une bonne paire de la Question précédente $X = 000$; $X' = 110$; $Y = 001$; $Y' = 011$

$K_0 = P_0 \oplus X = 001 \oplus 000 = 001 = P_1 \oplus X' = 111 \oplus 110 = 001 = K_0$

$K_1 = C_0 \oplus Y = 011 \oplus 001 = 010 = C_1 \oplus Y' = 001 \oplus 011 = 010 = K_1$

donc la clé est 001, 010

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.



On connaît P et C, et avec l'aide des bonnes paires correspondantes, on arrive à retrouver K_0 et K_1.

On a besoins au maximum de N_0 clairs choisis. avec $N_0 \approx \frac{c}{p_0}$ soit ici $\frac{c}{\frac{2}{8}} = 4c$ avec c une constante.

0

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

complexité exponentielle. $2^{\text{nb bit clé}}$ soit 2^6

1

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

0

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 ?

le fait que N ne soit pas nulle ici permet d'assurer l'Authentification du message, en effet $MAC = MDC + N \neq 0$

1

10

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.

la clé secrète de la partie 1 doit être transmise sur un canal sûr, suivant le modèle de Shannon.
les clés d'Even / Mansour sont transmise par le chiffrement de la partie 1.

1

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

1

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

0

1