Corrigé du *partiel SéCrypt - Info 3*

Les copies des transparents, et notes, de cours et de travaux dirigés sont autorisées. Veuillez justifier vos réponses de façon rigoureuse.

Exercice 1 : Relations d'ordre & treillis (Politique de sécurité)

1. La relation binaire suivante sur $E = \{0, 1, 2, 3, 4, 5\}$ est-elle une relation d'ordre ?

$$\begin{array}{rcll} 0 & \leq & x & \forall x \in \{0, 1, 2, 3, 5\} \ , \\ 1 & \leq & 3 & \\ 3 & \leq & 5 & \\ 1 & \leq & 5 & \\ 2 & \leq & 4 \ . & \end{array}$$

   Correction. Non ce n'est pas une relation d'ordre car elle n'est pas transitive : on a $0 \leq 2$, $2 \leq 4$ mais il manque $0 \leq 4$.

2. Si la relation précédente n'est pas une relation d'ordre, quelle information faut-il ajouter pour qu'elle le devienne ? **Correction.** Il suffit de rajouter $0 \leq 4$.

3. Avec l'information ajoutée (question précédente), la relation d'ordre obtenue est-elle totale ? **Correction.** Non ! Car il n'y a aucune relation entre 4 et 5.

4. On considère la relation binaire suivante sur $E = \{0, 1, 2, 3, 4, 5\}$.

$$\begin{array}{rcll} 0 & \leq & x & \forall x \in E \ , \\ 1 & \leq & 3 & \\ 3 & \leq & 5 & \\ 1 & \leq & 5 & \\ 2 & \leq & 4 \ . & \end{array}$$

   Correction. Calculer $\inf\{x, y\}$ pour tous $x, y \in E$.

$inf(l, c)$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	0	1	0	1
2	0	0	2	0	2	0
3	0	1	0	3	0	3
4	0	0	2	0	4	0
5	0	1	0	3	0	5

   où l est un élément pris sur une ligne, et c sur une colonne.

5. La relation introduite à la question précédente est-elle un treillis ? **Correction.** Non car $sup\{4, 5\}$ n'existe pas.

6. Dans le cas où la réponse à la question précédente est non, pouvez-vous ajouter une (ou des) information(s) afin d'en faire un treillis ? **Correction.** On peut rajouter $4 \leq 5$ par exemple.

7. On considère trois catégories `top secret`, `sensible`, `déclassée` ordonnées par la relation `top secret` $\geq$ `sensible` $\geq$ `déclassée`. On suppose que les niveaux d'habilitation des utilisateurs et les niveaux de classification des objets sont l'une de

ces catégories. Imaginez une politique de contrôle d'accès dans laquelle aucune fuite d'information n'est possible d'un niveau donné vers un niveau qui lui est inférieur. **Correction.** On suppose qu'un propriétaire d'un fichier peut lire dans un fichier de niveau de classification supérieur à son niveau d'habilitation et écrire dans un fichier de niveau de classification inférieur à son niveau d'habilitation. Ainsi si un utilisateur lit un fichier, il ne lui est pas possible de le recopier dans un fichier de niveau de classification inférieur puisqu'il n'aura pas le droit d'écriture !

Exercice 2 : Groupes pour la cryptographie

1. Expliquer en quelques mots l'importance des groupes en cryptographie ;
2. Soit $G = \{1, 2, 3, 4\}$ muni de l'opération $*$ donnée par la table de " multiplication " suivante

$*$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

   (a) G est-il un groupe ? **Correction.** Oui, puisqu'il s'agit de $\mathbb{Z}_5$ avec la multiplication.

   (b) L'opération $*$ est-elle commutative ? **Correction.** Oui : on le voit par la symétrie de la table de multiplication.

3. Soit $\mathbb{N}$ l'ensemble $\{0, 1, 2, \cdots\}$ des entiers naturels. Cet ensemble $\mathbb{N}$ avec la multiplication (usuelle) est-il un groupe ? **Correction.** Non : excepté 1, aucun élément n'a d'inverse. Même question avec l'addition (usuelle). **Correction.** Non, excepté 0, aucun élément n'a d'opposé.
4. On considère $\mathbb{Z}_{26}$ avec la multiplication modulo vingt-six. Cet ensemble est-il un groupe (pour la multiplication) ? (Indication : un élément quelconque de $\mathbb{Z}_{26}$ est-il inversible ?) **Correction.** Non : on a vu en td que pour qu'un élément de cet ensemble soit inversible il faut et il suffit qu'il soit premier avec 26. Ainsi, par exemple, 2 n'est pas inversible modulo 26.

Exercice 3 : Le carré de Polybe

On considère un carré 5×5. On choisit un mot qui n'a que des lettres distinctes (c'est-à-dire qu'une lettre n'apparaît qu'au plus une fois dans ce mot ; par exemple, " mot " et contre-exemple : " chiffrement " où il y a deux " f " et deux " e ") et qui ne contient pas la lettre " j ". Pour chiffrer un message (écrit sans accents, sans ponctuation ni espaces et en majuscules), on commence par placer dans l'ordre (de la gauche vers la droite et de haut en bas) la clef secrète dans le tableau en commençant par la case $(1, 1)$ (première ligne et première colonne). On complète ensuite ce carré en inscrivant les lettres de l'alphabet (dans l'ordre alphabétique) qui n'apparaissent **pas** dans le mot choisit comme clef, en omettant la lettre " J ". Le cryptogramme est obtenu de la façon suivante : on considère un message dans lequel la lettre " J " n'apparaît pas. On chiffre chaque lettre du texte clair par les coordonnées notée "ij" (i : numéro de la ligne, j : numéro de la colonne, i=1,..., 5 et j=1,..., 5) de la case (dans le carré) dans laquelle la lettre apparaît.

1. Soit le mot clef " POLYBE ".
   (a) Construire le carré 5×5 comme indiqué dans l'énoncé. **Correction.**

	1	2	3	4	5
1	P	O	L	Y	B
2	E	A	C	D	F
3	G	H	I	K	M
4	N	Q	R	S	T
5	U	V	W	X	Z

   (b) Chiffrer le message " CENOMESTGRECBIENSUR". **Correction.** C=23 E=21 N=41 O=12 M=35 E=21 S=44 T=45 G=31 R=43 E=21 C=23 B=15 I=33 E=21 N=41 S=44 U=51 R=43, et donc on a le chiffré 23214112352144453143212315332141445143.

2. Déchiffer le cryptogramme suivant obtenu avec la clef " CRYPTO ".
   231222522152215145225225551512215152254122232143432512251421434525232142112151122232251421511241224551341525.
   Correction. Le carré est ici

	1	2	3	4	5
1	C	R	Y	P	T
2	O	A	B	D	E
3	F	G	H	I	K
4	L	M	N	Q	S
5	U	V	W	X	Z

   On a alors
   23=B 12=R 22=A 52=V 21=O 52=V 21=O 51=U 45=S 22=A 52=V 25=E 55=Z 15=T 12=R 21=O 51=U 52=V 25=E 41=L 22=A 23=B 21=O 43=N 43=N 25=E 12=R 25=E 14=P 21=O 43=N 45=S 25=E 23=B 21=O 42=N 11=C 21=O 51=U 12=R
   22=A 32=G 25=E 14=P 21=O 51=U 12=R 41=L 22=A 45=S 51=U 34=I 15=T 25=E, et donc
   BRAVO VOUS AVEZ TROUVÉ LA BONNE RÉPONSE BON COURAGE POUR LA SUITE.

Exercice 4 : Système cryptographique produit

Une des notions introduites par Shannon en 1949 est l'idée de combiner des systèmes cryptographiques en formant leur " produit ". Cette idée joue un rôle fondamental dans la conception des systèmes cryptographiques actuels tels le DES.
Supposons que l'on ait deux procédés de chiffrement S_1 et S_2. On suppose que les ensembles de message clairs et de chiffrés de S_i, $i = 1, 2$ sont tous identiques. On note $\mathcal{K}^{(i)}$ l'espace des clefs du système S_i $(i = 1, 2)$ et pour $K \in \mathcal{K}^{(i)}$, on note $D_K^{(i)}$ et $E_K^{(i)}$ les fonctions de déchiffrement et de chiffrement de $S^{(i)}$ $(i = 1, 2)$. On définit le système **produit** $S_1 \times S_2$ par la règle de chiffrement

$$E_{K_1,K_2}(x) := E_{K_2}^{(2)}(E_{K_1}^{(1)}(x))$$

pour x un message clair, $K_i \in \mathcal{K}^{(i)}$. Il résulte que l'espace des clefs de $S_1 \times S_2$ n'est rien d'autre que le produit cartésien $\mathcal{K}^{(1)} \times \mathcal{K}^{(2)}$.

1. Expliquer, en français, le fonctionnement de cette méthode de chiffrement. **Correction.** On commence par chiffrer le message avec les règles de S_1 puis on chiffre le résultat obtenu avec les méthode de S_2.
2. Donner le nombre de clefs de $S_1 \times S_2$ en fonction des nombres de clefs de S_1 et de S_2. **Correction.** C'est le nombre de clef de S_1 multiplié par le nombre de clefs de S_2 (cardinal de $S_1 \times S_2$).
3. Déduire de la définition de la règle de chiffrement, la méthode de déchiffrement de $S_1 \times S_2$. **Correction.** On commence par déchiffrer avec les règles de S_2 puis on déchiffre avec celle de S_1
4. Montrer (en utilisant la propriété de déchiffrement vue en cours) que l'on a

   $$D^{(1)}_{K_1}(D^{(2)}_{K_2}(y)) = x$$

   quel que soit le message clair x et son chiffré $y = E_{K_1,K_2}(x)$, et quelles que soient les clefs $K_1 \in \mathcal{K}^{(1)}$ et $K_2 \in \mathcal{K}^{(2)}$. **Correction.**

   $$\begin{aligned} D^{(1)}_{K_1}(D^{(2)}_{K_2}(y)) &= D^{(1)}_{K_1}(D^{(2)}_{K_2}(E_{K_1,K_2}(x)) \\ &= D^{(1)}_{K_1}(D^{(2)}_{K_2}(E^{(2)}_{K_2}(E^{(1)}_{K_1}(x))) \\ &= D^{(1)}_{K_1}(D^{(2)}_{K_2}(E^{(2)}_{K_2}(E^{(1)}_{K_1}(x)))) \\ &= D^{(1)}_{K_1}(E^{(1)}_{K_1}(x)) \\ &= x\ . \end{aligned}$$

5. Montrer que le procédé de chiffrement affine (vu en TD) peut être décrit comme un procédé produit $S_1 \times S_2$ (où l'un des facteurs S_i est le procédé de chiffrement par décalage, tandis que l'autre facteur est un procédé que vous devrez imaginer). **Correction.** On définit $E^{(2)}_b(x) = x + b \mod 26$ et $E^{(1)}_a(x) = ax \mod 26$ pour a inversible dans $\mathbb{Z}_{26}$ et alors $E_{(a,b)}(x) = E^{(2)}_b(E^{(1)}_a(x))$.

Exercice 5 : Confidentialité parfaite

Soit un système cryptographique dans lequel $\mathcal{P} = \{a, b, c\}$, $\mathcal{K} = \{K_1, K_2, K_3\}$ et $\mathcal{C} = \{1, 2, 3, 4\}$. Supposons que la règle de chiffrement soit défini par la table suivante

	a	b	c
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

On suppose que la probabilité $\mathsf{P}_\mathcal{K}$ est la probabilité uniforme, et, $\mathsf{P}_\mathcal{P}(a) = \frac{1}{2}$, $\mathsf{P}_\mathcal{P}(b) = \frac{1}{3}$ et $\mathsf{P}_\mathcal{P}(c) = \frac{1}{6}$.

1. Calculer les probabilités conditionnelles $\mathsf{P}(x|y)$ pour tout $x \in \mathcal{P}$ et $y \in \mathcal{C}$. **Correction.** On utilise les formules vue au chapitre IV : on commence par calculer $\mathsf{P}_\mathcal{C}(y)$.
   - $y = 1 : C_1 = \{K \in \mathcal{K} : \exists x \in \mathcal{P},\ E_K(x) = 1\} = \{K_1, K_3\}$. Donc $\mathsf{P}_\mathcal{C}(1) = \mathsf{P}_\mathcal{K}(K_1)\mathsf{P}_\mathcal{P}(\underbrace{D_{K_1}(1)}_{=a}) + \mathsf{P}_\mathcal{K}(K_3)\mathsf{P}_\mathcal{P}(\underbrace{D_{K_3}(1)}_{=c}) = \frac{1}{3}(\frac{1}{2} + \frac{1}{6}) = \frac{2}{9}$;
   - $y = 2 : C_2 = \{K_1, K_2\}$, donc $\mathsf{P}_\mathcal{C}(2) = \frac{1}{3}(\frac{1}{2} + \frac{1}{3}) = \frac{5}{18}$;
   - $y = 3 : C_3 = \{K_1, K_2, K_3\}$, donc $\mathsf{P}_\mathcal{C}(3) = \frac{1}{3}$;

– $y = 4 : C_4 = \{K_2, K_3\}$, donc $\mathsf{P}_{\mathcal{C}}(4) = \frac{1}{3}(\frac{1}{3} + \frac{1}{6}) = \frac{2}{9}$.

On calcule ensuite toutes les probabilités conditionnelles $\mathsf{P}(y|x)$:

– $y = 1, x = a : D_{a,1} = \{K_1\}$, donc $\mathsf{P}(1|a) = \frac{1}{3}$;
– $y = 1, x = b : D_{b,1} = \emptyset$, donc $\mathsf{P}(1|b) = 0$;
– $y = 1, x = c : D_{c,1} = \{K_3\}$, donc $\mathsf{P}(1|c) = \frac{1}{3}$;
– $y = 2, x = a : D_{a,2} = \{K_2\}$,donc $\mathsf{P}(2|a) = \frac{1}{3}$;
– $y = 2, x = b : D_{b,2} = \{K_1\}$, donc $\mathsf{P}(2|b) = \frac{1}{3}$;
– $y = 2, x = c : D_{c,2} = \emptyset$, donc $\mathsf{P}(2|c) = 0$;
– $y = 3, x = a : D_{a,3} = \{K_3\}$, donc $\mathsf{P}(3|a) = \frac{1}{3}$;
– $y = 3, x = b : D_{b,3} = \{K_2\}$, donc $\mathsf{P}(3|b) = \frac{1}{3}$;
– $y = 3, x = c : D_{c,3} = \{K_1\}$, donc $\mathsf{P}(3|c) = \frac{1}{3}$;
– $y = 4, x = a : D_{a,4} = \emptyset$, donc $\mathsf{P}(4|a) = 0$;
– $y = 4, x = b : D_{b,4} = \{K_3\}$, donc $\mathsf{P}(4|b) = \frac{1}{3}$;
– $y = 4, x = c : D_{c,4} = \{K_2\}$, donc $\mathsf{P}(4|c) = \frac{1}{3}$.

Enfin on calcule les proba $\mathsf{P}(x|y) = \dfrac{\mathsf{P}_{\mathcal{P}}(x)\mathsf{P}(y|x)}{\mathsf{P}_{\mathcal{C}}(y)}$:

– $x = a, y = 1 : \mathsf{P}(a|1) = \frac{\frac{1}{2}\frac{1}{3}}{\frac{2}{9}} = \frac{3}{4}$;
– $x = a, y = 2 : \mathsf{P}(a|2) = \frac{\frac{1}{2}\frac{1}{3}}{\frac{5}{18}} = \frac{3}{5}$;
– $x = a, y = 3 : \mathsf{P}(a|3) = \frac{\frac{1}{2}\frac{1}{3}}{\frac{1}{3}} = \frac{1}{2}$;
– $x = a, y = 4 : \mathsf{P}(a|4) = \frac{\frac{1}{2}0}{\frac{2}{9}} = 0$;
– $x = b, y = 1 : \mathsf{P}(b|1) = \frac{\frac{1}{3}0}{\frac{2}{9}} = 0$;
– $x = b, y = 2 : \mathsf{P}(b|2) = \frac{\frac{1}{3}\frac{1}{3}}{\frac{5}{18}} = \frac{2}{5}$;
– $x = b, y = 3 : \mathsf{P}(b|3) = \frac{\frac{1}{3}\frac{1}{3}}{\frac{1}{3}} = \frac{1}{3}$;
– $x = b, y = 4 : \mathsf{P}(b|4) = \frac{\frac{1}{3}\frac{1}{3}}{\frac{2}{9}} = \frac{1}{2}$;
– $x = c, y = 1 : \mathsf{P}(c|1) = \frac{\frac{1}{6}\frac{1}{3}}{\frac{2}{9}} = \frac{1}{4}$;
– $x = c, y = 2 : \mathsf{P}(c|2) = \frac{\frac{1}{6}0}{\frac{5}{18}} = 0$;
– $x = c, y = 3 : \mathsf{P}(c|3) = \frac{\frac{1}{6}\frac{1}{3}}{\frac{1}{3}} = \frac{1}{6}$;
– $x = c, y = 4 : \mathsf{P}(c|4) = \frac{\frac{1}{6}\frac{1}{3}}{\frac{2}{9}} = \frac{1}{4}$.

2. La confidentialité parfaite est-elle assurée par ce cryptosystème ? **Correction.** À l'évidence non : par exemple, $\mathsf{P}_{\mathcal{P}}(a) = \frac{1}{2}$ alors que $\mathsf{P}(a|1) = \frac{3}{4}$.

Exercice 6 : Structure de Feistel généralisée

Soient X, K deux ensembles finis. Soit les applications

$$B : X \times X \to X$$

telle que $B(x', B(x, x')) = x$ quels que soient $x, x' \in X$ et

$$f : X \times K \to X \ .$$

Soit enfin l'application

$$\begin{array}{rccl} \mathcal{F} : & (X \times X) \times K & \to & X \times X \\ & ((x_1, x_2), k) & \mapsto & (x_2, B(x_1, f(x_2, k))) \ . \end{array}$$

Montrer que quel que soit $k \in K$ fixé, la fonction $(x_1, x_2) \mapsto (x_2, B(x_1, f(x_2, k)))$ est inversible. (Inspirez-vous de la démonstration vue en cours du fait qu'une structure de Feistel est inversible.) **Correction.** On récupère la partie gauche du résultat de $(x'_1, x'_2) = \mathcal{F}((x_1, x_2), k)$, c'est-à-dire $x'_1 = x_2$. On calcule $f(x_2, k)$ (puisque l'on dispose de f, de k et maintenant de x_2), puis on calcule $B(f(x_2, k), x'_2) = x_1$ d'après la propriété de B et le fait que $x'_2 = B(x_1, f(x_2, k))$.

Exercice 7 : Procédé de chiffrement multiplicatif

On considère l'anneau $\mathbb{Z}_{30} = \{0, 1, 2, \cdots, 29\}$ des entiers modulo 30. Rappelons qu'un élément $a \in \mathbb{Z}_{30}$ est inversible (c'est-à-dire qu'il existe $b \in \mathbb{Z}_{30}$ tel que $ab = 1 \mod 30$; dans la suite vous noterez " a^{-1} " l'inverse de a) si, et seulement si, $pgcd(a, 30) = 1$ (c'est-à-dire le seul multiple commun entre a et 30 est 1).

1. Énumérer tous les éléments de $\mathbb{Z}_{30}$ qui sont inversibles. **Correction.** $30 = 2 \times 15 = 2 \times 3 \times 5$, donc tous les éléments de $\mathbb{Z}_{30}$ non divisibles par 2, 3 et 5 est premier avec 30. Il s'agit donc de
   1, 7, 11, 13, 17, 19, 23, 29.
2. Calculer l'inverse dans $\mathbb{Z}_{30}$ des éléments trouvés à la question précédente. **Correction**

a	a^{-1}
1	1
7	13
11	11
13	7
17	23
19	19
23	17
29	29

3. On défini le procédé de chiffrement **multiplicatif** sur $\mathbb{Z}_{30}$ de la façon suivante : les messages clairs et chiffrés sont des éléments de $\mathbb{Z}_{30}$ et l'espace des clefs est donné par $\mathcal{K} := \{a \in \mathbb{Z}_{30} : pgcd(a, 30) = 1\}$. La fonction de chiffrement est donné par $E_a(x) := ax \mod 30$ avec $a \in \mathcal{K}$.
   (a) Calculer le nombre de clefs possibles. **Correction.** C'est exactement les éléments de $\mathbb{Z}_{30}$ qui sont premiers avec 30 : il y en a huit.
   (b) Décrire la fonction de déchiffrement D_a pour $a \in \mathcal{K}$. **Correction.**
   (c) On suppose que les letters sont codées comme d'habitude par $A \leftrightarrow 0$, ..., $Z \leftrightarrow 25$, puis À$\leftrightarrow 26$, Ê$\leftrightarrow 27$, É$\leftrightarrow 28$ et le caractère blanc (l'espace) $\leftrightarrow 29$. Chiffrer le message suivant avec la clef $a = 13$ (vous donnerez le résultat sous la forme du texte corresponant à la suite de nombres) :

      SI VOUS EN ÊTES LÀ ALORS VOUS AVEZ PRESQUE TERMINÉ LE PARTIEL

Correction.

lettre	*code*	$E_{13}(code)$	*lettre*
A	0	0	A
B	1	13	N
C	2	26	À
D	3	9	J
E	4	22	W
F	5	5	F
G	6	18	S
H	7	1	B
I	8	14	O
J	9	27	Ê
K	10	10	K
L	11	23	X
M	12	6	S
N	13	19	T
O	14	2	C
P	15	15	P
Q	16	28	É
R	17	11	L
S	18	24	Y
T	19	7	H
U	20	20	U
V	21	3	D
W	22	16	Q
X	23	29	(espace)
Y	24	12	M
Z	25	25	Z
À	26	8	I
Ê	27	21	V
É	28	4	E
(espace)	29	17	R

On obtient finalement le texte chiffré suivant :

YORDCUYRWTVHWRXIRAXCLYRDCUYRADWZRPLWYÉUWRHWLSOTERX
WRALHOWX