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 ?

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

2. Si la relation précédente n'est pas une relation d'ordre, quelle information faut-il ajouter pour qu'elle le devienne ?
3. Avec l'information ajoutée (question précédente), la relation d'ordre obtenue est-elle totale ?
4. On considère la relation binaire suivante sur $E = \{0, 1, 2, 3, 4, 5\}$.

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

   Calculer $\inf\{x, y\}$ pour tous $x, y \in E$.
5. La relation introduite à la question précédente est-elle un treillis ?
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 ?
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.

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 ?

(b) L'opération $*$ est-elle commutative ?

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 ? Même question avec l'addition (usuelle).
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 ?)

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 ;
   (b) Chiffrer le message " CENOMESTGRECBIENSUR".
2. Déchiffer le cryptogramme suivant obtenu avec la clef " CRYPTO ".
   231222522152215145225225551512215152254122232143432512251421434525232142112151122232251421511241224551341525.

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 ;

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 ;
3. Déduire de la définition de la règle de chiffrement, la méthode de déchiffrement de $S_1 \times S_2$;
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 $K_2 \in \mathcal{K}^{(2)}$;

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).

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 $y \in \mathcal{C}$;
2. La confidentialité parfaite est-elle assurée par ce cryptosystème ?

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.)

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 ;
2. Calculer l'inverse dans $\mathbb{Z}_{30}$ des éléments trouvés à la question précédente ;
3. On définit 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 ;
   (b) Décrire la fonction de déchiffrement D_a pour $a \in \mathcal{K}$;
   (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