Examen du vendredi 7 janvier 2022, de 9h à 11h.
Sont autorisés : une calculatrice et résumé de cours manuscrit format A4 recto-verso.
Autres documents et portables interdits.
Le sujet comporte 2 pages. Le barême est indicatif.

1. BASES (5 POINTS)

La base 45 est un système d'encodage utilisé par certaines applications, par exemple les QR codes du passe sanitaire. On écrit un nombre en base 45 avec les caractères suivants :
`0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ␣$%*./:"+-`
Ainsi `;1A` en base 45 correspond à l'entier $44 \times 45^2 + 1 \times 45 + 10$ en base 10.

(1) Déterminer la représentation en base 45 de 65535.

(2) En déduire n le nombre maximal de caractères qui sont nécessaires pour représenter 2 octets en base 45. Peut-on obtenir le code `$00` ?

(3) On décide de représenter 2 octets par n caractères en base 45, en ajoutant des 0 au début si nécessaire. Voici un extrait de 6 caractères d'un QR code `6BF0D;` Quels sont les octets correspondants ?

(4) On suppose qu'on dispose d'une fonction `num` qui prend en argument un caractère d'écriture en base 45 et renvoie un entier entre 0 et 44. Donner au choix en langage naturel ou en C ou en Python un algorithme prenant en entrée une chaine de caractère représentant un QR code en base 45 et renvoyant un tableau (ou une liste) d'octets. On testera la validité de la chaine de caractères.

2. CRYPTOGRAPHIE DE HILL (6 POINTS)

Soit $p = 31$ et la matrice à coefficients dans $\mathbb{Z}/p\mathbb{Z}$

$$A = \begin{pmatrix} 1 & 5 \\ 5 & 4 \end{pmatrix} \ [31]$$

(1) Un agent secret de nom de code BOND utilise la cryptographie de Hill pour envoyer des messages, en codant les caractères de A à Z par les entiers de 0 à 25, puis les caractères `+-*/^` par les entiers 26 à 30. Déterminer les 2 vecteurs de $(\mathbb{Z}/p\mathbb{Z})^2$ correspondant à son nom de code, puis les 2 vecteurs cryptés correspondant.

(2) Montrer que A est inversible et calculer son inverse. Vérifiez en décryptant les 2 vecteurs de la question précédente.

(3) Montrer que le nombre de matrices de cryptage possible est inférieur à 31^4. Est-ce suffisant pour assurer la sécurité des échanges ?

(4) Un espion du camp adverse intercepte un message de BOND. On suppose que BOND termine son message par les deux vecteurs de son nom de code crypté. L'espion du camp adverse peut-il en déduire la matrice A ?

(5) Peut-on améliorer la sécurité en prenant une valeur de p plus grande, par exemple $p = 65537$ ou un nombre premier beaucoup plus grand de 1024 bits ?

3. SECRET COMMUN (9 POINTS)

On présente une méthode permettant à deux personnes, Alice et Bob, de créer un secret commun sans avoir besoin de se rencontrer. Pour expliquer cette méthode, on commence par travailler dans $\mathbb{Z}/19\mathbb{Z}$. Puis on travaillera dans $\mathbb{Z}/p\mathbb{Z}$ pour un entier premier p.

3.1. **Exemple jouet.** Alice et Bob choisissent donc de travailler dans $\mathbb{Z}/19\mathbb{Z}$ et d'utiliser $g = 2$ qui est un générateur de $\mathbb{Z}/19\mathbb{Z}^*$. Alice choisit un entier secret a puis calcule le reste A de la division de g^a par 19 et l'envoie à Bob. Bob choisit un entier secret b puis calcule le reste B de la division de g^b par 19 et l'envoie à Alice. Alice calcule alors le reste de B^a par 19, Bob calcule le reste de A^b par 19, ces nombres sont identiques, c'est leur secret commun.

(1) Alice choisit $a = 7$ et Bob choisit $b = 13$. Donner A et B puis vérifier que $A^b = B^a \pmod{19}$.

(2) Que se passe-t-il si Alice choisit $a = 25$? À quelle valeur maximale pour a et b Alice et Bob peuvent-ils se restreindre ?

(3) Vérifier que 2 est bien un générateur de $\mathbb{Z}/19\mathbb{Z}^*$. Déterminer la table de toutes les puissances de 2 dans $\mathbb{Z}/19\mathbb{Z}$.

(4) Alice et Bob choisissent deux autres entiers a et b et s'envoient $A = 4$ et $B = 17$. En utilisant la table, déterminer les valeurs de a et b. Quelle est la valeur du secret commun ?

3.2. **Sécurité.** On a vu qu'une personne qui connait les entiers A et B (par exemple en espionnant les échanges entre Alice et Bob) pouvait calculer le secret commun si on travaille dans $\mathbb{Z}/19\mathbb{Z}$. Pour espérer sécuriser le secret commun, il faut travailler dans $\mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier plus grand.

(1) Commençons par essayer avec $p = 65537$ et $g = 3$.
   (a) Quel est l'ordre de $\mathbb{Z}/p\mathbb{Z}^*$? Vérifier que 3 est un générateur de $\mathbb{Z}/p\mathbb{Z}^*$.
   (b) Si Alice choisit $a = 12345$, combien doit-elle effectuer de multiplications pour calculer A par l'algorithme de la puissance rapide ?
   (c) À quelle valeur maximale pour a et b Alice et Bob peuvent-ils se restreindre ?
   (d) Quelle est la taille de la table des puissances de 3 modulo p ? Comparez avec la question (b). La sécurité du secret commun vous semble-t-elle suffisante ?

(2) On prend maintenant un nombre premier dont l'écriture en base 2 comporte exactement 1024 bits, et tel que $g = 2$ est un générateur de $\mathbb{Z}/p\mathbb{Z}^*$. La sécurité du secret commun vous semble-t-elle suffisante ?