CC1 Mat309, 10 octobre 2022, 15h15-16h45

Calculatrices et documents interdits. Les réponses doivent être justifiées.

Exercice 1. (~ 8 points)

1. Déchiffrer le message crypté

QZZMITQAIJTM

exprimant l'opinion de César concernant une possible défaîte de son armée face à un certain village gaulois.

Son message a été intercepté et décrypté par ses adversaires. Utilisez le même chiffrage pour lui transmettre l'avis d'Astérix:

FACILE

2. Décryptez le message (crypté en permutant les lettres de l'alphabet) se terminant par les deux mots "James Bond" que 007 a envoyé à un collègue:

STO OTS RIU YTOZ, XQSRI YTOZ

Est-ce qu'on a assez de données pour crypter la réponse

BEAU NOM

en utilisant le même cryptage?

Cryptez cette réponse en mettant * pour d'éventuelles lettres indéterminées.

3. (Question peut-être plus difficile, à garder pour la fin?) On numérote les lettres de l'alphabet de 0 (correspondant à A) à 25 (correspondant à Z) et on utilise un entier binaire $b_{12}b_{11}b_{10}\dots b_1b_0$ (représentant $\sum_{i=0}^{12} b_i 2^i$) pour représenter la permutation qui échange la lettre numérotée i avec la lettre numérotée $i+13$ si $b_i = 1$ et qui ne les échange pas si $b_i = 0$.

Par exemple, si la clé se termine par $\cdots 101$, on échange A avec N, on laisse B et O inchangés, on échange C avec P.

(a) Combien y a-t-il de telles clés? (En comptant le chiffrage identité qui laisse le message en clair.)

(b) Trouver l'écriture binaire de 5719 et utiliser cette clé pour chiffrer votre avis 'MERDIQUE' sur les questions de ce CC.

(c) Montrer que le déchiffrement est du même type que le chiffrement pour cette méthode de chiffrage et décrire la clé de déchiffrement qui correspond à un entier binaire n.

(d) Quels entiers binaires correspondent à un chiffrement de César?

Tourner, SVP

Exercice 2. ($\sim$ 3 points)

1. Donner l'expression binaire de l'entier décimal 777.
2. Donner l'expression hexadécimale (base 16) de l'entier binaire

$$1011011101111$$

en utilisant les lettres a, b, c, d, e, f pour représenter les chiffres $10, 11, 12, 13, 14, 15$.

3. Donner l'expression ternaire (en base 3) de l'entier binaire 1110011.

Exercice 3. ($\sim$ 5 points)

1. Donner la table d'addition des entiers ≤ 4 en base 5.
2. L'écriture en base 5 de deux entiers A et B est donnée par 321 et 243. Donner l'écriture en base 5 de la somme $S = A + B$ en faisant les calculs en base 5. Les calculs en base 5 font partie de la réponse.
3. Écrire la table de multiplication des entiers naturels ≤ 4 en base 5.
4. Donner l'écriture en base 5 du produit AB en effectuant les calculs en base 5. Les calculs en base 5 font partie de la réponse.
5. Donner l'écriture en base 10 de l'entier dont l'écriture en base 5 est 200103.

Exercice 4. ($\sim$ 4 points)

1. Calculez le pgcd de 15994 et de 132 par un algorithme de votre choix qui n'utilise pas la factorisation en donnant les résultats intermédiaires.
2. Diviser 15994 et 132 par leur pgcd et vérifier que les deux nombres obtenus sont premiers entre eux.
3. Calculer une relation de Bézout pour les deux entiers $34, 21$.