Université de Lille 1 SCIENCES ET TECHNOLOGIES

L1 - SESI - 2014/2015

Arithmétique et Cryptographie

DS 1 - Durée 1h30

Toutes les réponses doivent être justifiées et vous soignerez votre rédaction. Le barème est indicatif.
Les documents et appareils électroniques (calculatrices, téléphones portables, etc...) sont interdits.
Notez le numéro de votre groupe sur la copie.

Exercice 1. (4 points)

On considère le chiffrement de César, avec une clé k. Les lettres chiffrées sont les lettres majuscules avec la correspondance habituelle $A \leftrightarrow 0$, $B \leftrightarrow 1, \ldots, Z \leftrightarrow 25$.

1. Écrire l'application mathématique C_k correspondant à ce chiffrement. On précisera en particulier quels sont les ensembles de départ et d'arrivée.
2. Quelle est la taille de l'espace des clés ?
3. Quelle est l'application de déchiffrement ?
4. Déchiffrer le message "ZHTLKP", chiffré par une clé dont on sait $0 \leqslant k \leqslant 10$.

Exercice 2. (4 points)

On considère le chiffrement de Vigenère, avec une clé de longueur 3 : (n_1, n_2, n_3). Les lettres chiffrées sont les lettres majuscules avec la correspondance habituelle $A \leftrightarrow 0$, $B \leftrightarrow 1, \ldots, Z \leftrightarrow 25$.

1. Écrire l'application mathématique C_{n_1,n_2,n_3} correspondant à ce chiffrement. On précisera en particulier quels sont les ensembles de départ et d'arrivée.
2. Quelle est la taille de l'espace des clés ?
3. Quelle est l'application de déchiffrement ?
4. Déchiffrer le message "MEJTSKM", chiffré par la clé $(8, 10, 7)$.

Exercice 3. (4 points)

1. **Question de cours.** Énoncer le théorème de Bézout sous la forme d'une équivalence, pour deux entiers a et b premiers entre eux.
2. Soit $a \in \mathbb{Z}$. Montrer que a et $a + 1$ sont premiers entre eux en considérant un diviseur d commun.
3. Soit $a \in \mathbb{Z}$. Montrer que a et $a + 1$ sont premiers entre eux en utilisant le théorème de Bézout.

Exercice 4. (4 points)

1. Calculer le pgcd de $a = 1810$ et de $b = 178$ par l'algorithme d'Euclide.
2. Trouver deux entiers u, v tels que $au + bv = \text{pgcd}(a, b)$.
3. Quel est l'inverse de a modulo b ?

Exercice 5. (4 points)

On propose l'algorithme suivant pour le calcul du pgcd de deux entiers a et b.

— **Étape 1.** Si a et b sont tous les deux pairs, alors $\text{pgcd}(a, b) = 2 \cdot \text{pgcd}(a/2, b/2)$.
— **Étape 2**
  — Si a est pair et b impair, alors $\text{pgcd}(a, b) = \text{pgcd}(a/2, b)$.
  — Si a est impair et b pair,alors $\text{pgcd}(a, b) = \text{pgcd}(a, b/2)$.
— **Étape 3**
  — Si a et b sont tous les deux impairs, et $a \geqslant b$ alors $\text{pgcd}(a, b) = \text{pgcd}((a - b)/2, b)$.
  — Si a et b sont tous les deux impairs,et $a \leqslant b$ alors $\text{pgcd}(a, b) = \text{pgcd}((b - a)/2, a)$.

L'algorithme consiste à répéter les étapes 1,2,3 jusqu'à obtenir une forme $\text{pgcd}(0, b)$ (ou $\text{pgcd}(a, 0)$) pour lequel on sait $\text{pgcd}(0, b) = b$ (ou $\text{pgcd}(a, 0) = 0$).

Questions.

1. Appliquer l'algorithme avec $a = 60$, $b = 18$.
2. Montrer que chacune des assertions des étapes 1, 2, 3 est vraie.
3. Pourquoi l'algorithme se termine ?
4. Quel est l'avantage de cet algorithme par rapport à l'algorithme classique d'Euclide ? (En particulier vous vous interrogerez sur comment un ordinateur vérifie qu'un entier est pair ou impair et comment il divise un entier pair par 2.)