Cours 420-202-RE **Traitement de données orienté objet** **Hiver 2019** **Cégep Limoilou** **Département d'Informatique**	**Tp 5 mandat 1 de 4 (1 semaine pour cette partie)** **10% pour les 4 mandats** **Cryptographie - Le chiffre de Hill**

OBJECTIFS

- Utiliser et manipuler des structures de données sur disque et en mémoire;
- Trouver une solution informatique à un problème;
- Utiliser les méthodes appropriées des classes de l'API de Java;
- Livrer un code documenté et testé.

ACTIVITÉ À RÉALISER

Le Tp 5 consiste à utiliser une solution mathématique pour programmer une application de cryptographie. La cryptographie est un moyen de protéger le caractère confidentiel d'une information privée. Les méthodes cryptographiques modernes permettent le chiffrement, le déchiffrement et la signature numérique. Le chiffrement est la transformation des données dans une certaine forme illisible. Son but est d'assurer la sécurité en maintenant l'information cachée aux gens à qui l'information n'est pas adressée. Le déchiffrement est l'inverse du chiffrement; c'est la transformation des données chiffrées dans une forme intelligible.

Il existe principalement deux méthodes cryptographiques. Dans le cas de la cryptographie à clé secrète, la même clé est utilisée pour chiffrer et déchiffrer les données. Dans le cas de la cryptographie à clé publique, il existe deux clés différentes, ce qui a été chiffré à l'aide de l'une ne peut être déchiffré qu'à l'aide de l'autre.

Sans la clé, les données codées ne peuvent être transformées en un texte clair compréhensible qu'en utilisant des techniques de « force brute », c'est-à-dire en essayant toutes les variantes possibles de la clé et en vérifiant si le texte clair qui en résulte a un sens.

Un type de code, difficile à déchiffrer, se sert d'une matrice pour coder un message. Le récepteur du message le décode en employant l'inverse de la matrice (l'inverse de Hill). La première matrice s'appelle la **matrice de codage** et son inverse s'appelle la **matrice de décodage**.

Dans les différents mandats du travail, vous allez écrire un programme qui permet de chiffrer et de déchiffrer un message en utilisant des matrices de codage et de décodage. Vous allez tenter de « craquer » le déchiffrement et ensuite vous allez appliquer, si vous avez le désir, une amélioration en ajoutant un algorithme additionnel avant d'encoder votre message avec votre matrice.

Ce travail doit être réalisé en équipe de 2 et se déroule sur 4 séances de laboratoires.

CONTRAINTES IMPORTANTES :

- On veut absolument que les algorithmes pour produire toutes les possibilités de matrices et pour générer le déterminant d'une matrice soient récursifs.
- On veut absolument que vous utilisiez une variété de structures de données appropriées à la résolution de votre problème (utilisez 3 ou 4 structures de données différentes).

MANDAT 1 :

Documentation et recherche :

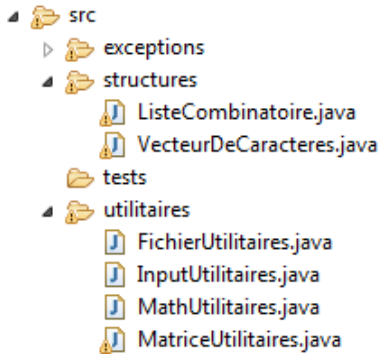
- Commencez par vous documenter sur le sujet pour bien saisir et comprendre le problème. Voici quelques références qui pourraient vous être utiles.
  - Les documents disponibles dans le dossier du travail sur Léa.
  - http://aix1.uottawa.ca/~jkhoury/cryptographyf.htm
  - http://fr.wikipedia.org/wiki/Chiffre_de_Hill

- http://www.bluebit.gr/matrix-calculator/
- http://bts-ig.numeriques.net/cours-exercices-corriges/produit/index.php#fin

- Envisagez vos solutions et notez vos idées tout en essayant de prévoir une solution plus vaste que votre application (par exemple produire des matrices avec des chiffres différents que ceux demandés, travailler avec un modulo autre que 27, etc.)
- Identifiez vos ressources documentaires et les principaux algorithmes que vous envisagez pour résoudre ce problème.

Dans un premier temps, nous allons nous intéresser aux classes sous-jacentes nous permettant de résoudre le problème principal :

- Maintenant que vous avez commencé à vous documenter sur le sujet et que vous commencez à mieux comprendre le problème, vous allez réaliser le code de certaines classes **qui nous fournira les méthodes essentielles de base pour résoudre le problème d'encryption du chiffrement de Hill**.
- À partir du code fourni sur le réseau vous devez, dans un nouveau projet Java en UTF-8 et selon la « JavaDoc », compléter les différentes méthodes. Il faut bien comprendre que les utilitaires et structures de données que vous allez développer dans ce mandat sont vus comme un « framework » et seront utilisés dans les prochains mandats du même travail.
- Ne pas développer les méthodes qui comportent la référence « MANDAT 2 » dans leur notice « TODO ».
- Complétez la JavaDoc pour les méthodes qui n'en ont pas…
- Il faut aussi produire les classes **de tests JUnit** pour chacune des classes dont vous allez compléter le code dans ce mandat. Il est conseillé de produire les tests au fur et à mesure que vous développez vos méthodes.
- **Testez correctement car c'est la base de votre solution globale, vous devez avoir confiance en votre code.**
- Voici les différents packages et classes qui vous sont fournis.



Échéancier :

- Vous avez une semaine pour réaliser le travail demandé par ce mandat.
- Il n'y a rien à remettre pour ce mandat, vous devez simplement avoir terminé et testé correctement votre code.