Ecole Polytechnique de Tunisie
1A, 2019

Mini-Projet POO: Initiation à la cryptographie en Java

On tiendra compte de la qualité du code et de la présentation du travail
A rendre le 21 Avril 2019 et à présenter lundi 22 Avril 2019

A Rendre

Ce travail peut s'effectuer en binôme et on demandera deux livrables : un document décrivant le diagramme de classe ainsi que le code développé. Le code doit être lisible et maintenable en ajoutant des commentaires concis et clairs et en respectant les conventions d'écriture de code Java.

Enoncé

Partie 1 :

On propose d'implémenter et d'utiliser un protocole de chiffrement simple d'un texte. Il consiste à modifier un caractère donné par un autre. On appelle clé tout couple (car1, car2) où car2 est le caractère substituant et car1 le caractère substitué. Par exemple, si clé=('O', 'Z'), on remplace O par Z dans le mot à crypter. Ainsi, dans cet exemple, le mot « BONJOUR » est chiffré en « BZNJZUR ». Pour déchiffrer le texte, il suffit d'effectuer la substitution dans le sens inverse (dans l'exemple, on remplace Z par O).

1. Ecrire la classe Crypto qui contient au moins deux méthodes publiques statiques :
   a. **public static String chiffrer(String texte, Cle cle)** qui prend un texte en entrée et retourne le mot chiffré selon la clé cle donnée. La classe Cle permet de définir les deux caractères de substitution de la clé.
   b. **public static String dechiffrer(String mot, Cle cle)** qui prend un texte chiffré et retourne un texte déchiffré selon la clé de chiffrement en paramètre.

2. Ecrire une application Java de test qui demande à l'utilisateur de saisir un texte et elle lui affiche sa version chiffrée. Il faudra considérer tous les cas particuliers (chaine vide, erreur de saisie, etc.).

3. Ecrire la classe Crypto2 en considérant une clé plus longue formée de 2 chaines de caractères (ch1, ch2) où ch1 et ch2 sont de même longueur. Pour le chiffrement, le ième caractère de ch1 est remplacé par le ième caractère de ch2. Ajouter l'application de Test qui permet de tester les méthodes de Crypto2.
4. Il est évident qu'il est facile de "casser" la clé en étudiant l'occurrence des caractères dans le texte. Par exemple, on sait que le caractère "E" est le plus utilisé dans la langue française. En vous basant sur cette remarque, proposer un programme Java qui permet de déchiffrer des textes français chiffrés en se basant sur l'occurrence des caractères.

On demande que le code soit dans un paquetage crypto et l'ensemble des tests dans un autre paquetage test.

Le code doit être lisible et maintenable en ajoutant les commentaires et en respectant les conventions d'écriture de code Java.

Partie2 :

On considère une méthode de chiffrement plus robuste basée sur AES – Advanced Encryption Standard qui est un algorithme de chiffrement symétrique.

AES peut utiliser des longueurs de clés différentes 128-, 192- and 256-bits selon le niveau de sécurité désiré.

Proposer une nouvelle version de Crypto qu'on appelle Crypto3 implémentant les méthodes chiffrer et déchiffrer comme suit :

a. **public static String chiffrer(String texte, Cle cle)** qui prend un texte en entrée et retourne le mot chiffré selon la clé donnée en paramètre.
b. **public static String dechiffrer(String mot, Cle cle)** qui prend un texte chiffré et retourne un texte déchiffré selon la clé de chiffrement en paramètre.

Ecrire une application Java qui permet de tester le chiffrement et le déchiffrement de textes en utilisant trois longueurs de clés différentes.

Comparer le temps d'exécution de ces deux opérations en variant la taille du texte à chiffrer et la taille de la clé. Quelle conclusion en tirer ?