

# Sujet 6

## Chiffrage Partiel de Fichiers

### 1 Objectif.

Il est des situations où il n'est pas nécessaire (ou même souhaitable) de chiffrer intégralement un fichier. Il peut n'être utile que de chiffrer une partie de celui-ci. Il vous est demandé de concevoir une application *Java* qui permettra à l'utilisateur de sélectionner un bloc d'un *fichier texte* (par exemple en spécifiant le numéro de ligne de départ et le nombre de lignes constituant ce bloc) et de ne chiffrer que ce bloc. Cette même application devra permettre à un utilisateur possédant la clé de lire l'intégralité du fichier et à un utilisateur ne possédant pas la clé de lire la partie apparaissant en clair.

### 2 Structure de l'application.

Votre application devra être accessible depuis une interface graphique permettant la sélection du fichier, la saisie de la spécification du bloc à crypter, la saisie du mot de passe d'où sera dérivée la clé de chiffrement. Favoriser l'usage des composants graphiques *swing*.

**aide.** Vous pouvez segmenter le fichier en plusieurs sous-fichiers. Si par exemple le fichier fait 1000 lignes et si les lignes 100 à 199 doivent n'être lisibles que par des personnes autorisées, vous pourrez le segmenter en trois sous-fichiers comportant les lignes 1 à 99 *en clair* les lignes 100 à 199 cryptées et les lignes 200 à 1000 en clair.