TP2 – Cryptographie en Java

Exercice 1:

1. Écrire un programme qui chiffre un texte lu à l'entrée standard selon l'algorithme *DES*, ensuite le déchiffre avec la même clé et affiche le résultat.
2. Modifier le programme de sorte que le texte chiffré soit placé dans un fichier, puis lors du déchiffrement le texte soit d'abord lu du fichier puis déchiffré.

Exercice 2: Écrire un programme qui chiffre un texte lu à l'entrée standard selon l'algorithme *RSA* du provider *BouncyCastle* (`"BC"`), ensuite le déchiffre et affiche le résultat. Le texte chiffré sera placé dans un fichier puis, au moment du déchiffrement, lu du fichier chiffré.

Exercice 3:

1. Écrire un programme qui crée une clé *DES* qu'il utilise pour chiffrer un texte, remet le texte chiffré dans un autre fichier et la clé de chiffrement dans un troisième fichier.
2. Écrire un deuxième programme qui recupère la clé de chiffrement et déchiffre le texte crypté par le premier programme (qui sera lu dans le fichier chiffré).
3. (Et bien-sûr) Vérifier les deux programmes !

Exercice 4: Modifier les deux programmes de l'exo précédent de sorte que le texte clair (donc à chiffrer) soit en fait le contenu d'un fichier. Votre programme doit gérer les fichiers de taille quelconque – se rappeler de l'emploi de `update()` et `doFinal()` !
