TD6 - Cryptage – RSA en Java

Ce TD a pour objectif de vous faire découvrir les fonctions de codage asymétrique (ou a clés publiques et privées). Vous travaillerez sur l'algorithme RSA au travers du langage Java.

Les objets pour le cryptage RSA en java

1 - Les packages sécurité de Java

Java.security.*
Javax.crypto.*

2 – Générateur de clé privée

La classe KeyPairGenerator : Cette classe génère une paire de clés

Les méthodes
getInstance("RSA") : active le générateur de clé RSA
initialize() : initialise la longueur des clés
genKeyPair() : génère les clés
getPrivate() et getPublic() : permettent de récupérer les clés

Exemple

```
// génération des clés RSA
KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");
keyGen.initialize(1024);
KeyPair keypair = keyGen.genKeyPair();
PrivateKey clePrivee = keypair.getPrivate();
PublicKey clePublique = keypair.getPublic();
```

3 – Cryptage et décryptage des données

Classe Cipher : Cette classe encapsule le cryptage et le décyptage de données.

Les méthodes
Cipher.getInstance() : permet d'obtenir une instance particulière d'un algorithme
Cipher.init() : défini le mode d'utilisation (Cryptage ou Décryptage) et la clé.
Cipher.doFinal() : crypte et renvoi le texte codé

Exemple

```
Cipher cipher = Cipher.getInstance("RSA");
// Codage RSA
 cipher.init(Cipher.ENCRYPT_MODE, clePublique);
 byte[] cipherText = cipher.doFinal("Texte");
 System.out.println("cipher: " + new String(cipherText));
// décodage RSA
 cipher.init(Cipher.DECRYPT_MODE, clePrivee);
 byte[] plainText = cipher.doFinal(cipherText);
 System.out.println("plain : " + new String(plainText));
```

Travail à faire

Exercice 1 : Codage RSA

Créer une application qui :

1. Génère un couple de clés RSA et les affiche.
2. Code et décode un message de votre choix

Exercice 2 : Une application plus sophistiquée

En reprenant le 1er TD sur le cryptage et en vous aidant de la question précédente, créer une application qui sécurise le transfert de données.

Variables globales
Clé secrète DES
Clé publique RSA
Clé privée RSA
Message codé

Partie 1 de l'application : Codage
2 - Création d'une clé secrète DES
3 - Codage de la clé secrète avec la clé publique RSA
5 - Lecture d'un fichier texte à coder
6 - Codage du fichier avec la clé secrète DES

Partie 2 de l'application : Décodage
1 - Création d'un couple de clés RSA
4 - Décodage de la clé secrète avec la clé privée RSA
7 - Décodage et écriture du fichier codé, avec la clé secrète DES

Remarques :

1 - Pour simplifier, les parties 1 (codage) et 2 (décodage) seront deux tâches, lancées par l'application principale qui se partagent les clés DES, RSA et le message codé.

2 - Il ne faut pas oublier de bien synchroniser ces tâches, avec des sémaphores par exemple.