

# Explications fiche 2

---

Le but de ces deux applications est de réaliser la signature d'un fichier quelconque à partir d'une clé privée puis de vérifier cette signature à partir d'une clé publique.

## Procédure à suivre

1. Compilation
  - **javac -encoding utf-8 \*.java**
2. Génération des deux clés
  - **java GenerationClesRSA privee.bin publique.bin**
3. Génération de la signature d'un fichier (ici, le fichier ReadMe.md)
  - **java SignatureFichier privee.bin ReadMe.md signature.bin**
4. Vérification de la signature
  - **java VerificationSignature ReadMe.md signature.bin publique.bin**
  - ==> Normalement, affichage de 'Fichier OK'
  - **Modifiez ce fichier (ajoutez un espace) puis relancez :**
  - ==> Normalement, affichage de 'Fichier invalide'