Sécurité Appliquée
Evaluation de TP

Jean-François COUCHOT
couchot[arobase]femto-st[point]fr

8 mars 2024

Tous les supports de TD/TP et de CM sont autorisés. Aucune communication n'est autorisée entre vous et une autre personne.

1 Prérequis

Chaque étudiant·e doit s'inscrire sur l'espace moodle
https://moodle.univ-fcomte.fr/course/view.php?id=2714
avec la clef écrite au tableau.

2 A réaliser

1. Générer une clef publique et une clef privé de 2048 bits pour RSA. Les sauvegarder respectivement sous les noms `mpubkey.pem` et `mprivkey.pem`.
2. Calculer l'empreinte selon l'algorithme sha256 du jeu de données propriétaires. Cette empreinte sera stockée au moyen d'un fichier `footprint.json`.
3. Générer la signature associée à ce fichier et à la clé privée. On pourra s'inspirer du code de signature de pycryptodome. Cette signature sera enrigistrée aussi au moyen d'un fichier `signature.json`.
4. Construire le code permettant de vérifier la validité du document vis à vis de la signature.
5. Déposer sur moodle :
   — le programme de construction de l'empreinte et de la signature ;
   — le programme de vérification de la validité du document ;
   — la clef publique `mpubkey.pem` ;
   — les deux fichiers json `footprint.json` et `signature.json`.