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. Construire un code pemrettant de créer une clé AES à l'aide d'un générateur de nombres pseudo-alatoires sur 16 octets. Enregistrer celle-ci sous le nom `myaeskey.txt`.
2. Récupérer la clef publique au format PEM. Utiliser cette clé publique pour chiffrer avec RSA la clé générée précédement. Enregistrer ce chiffré sous le nom `rsaaeskey.txt`.
3. Chiffrer le fichier contenant des données sensibles avec la clé enregistrée sous `myaeskey.txt` en utilisant AES et le mode GCM. Enregistrer le chiffré et les informations complémentaires sous le nom `cipheraes.json`.
4. Développer le code permettant à votre prof de déchiffrer ce message chiffré `cipheraes.json` en connaissant `rsaaeskey.txt` et la clé privée associée à la clé publique de la question 2.
5. Déposer sur moodle :
   — le programme de génération de clé symétrique pour AES, de chiffrement de cette clé selon RSA et du chiffrement du fichier sensible selon AES (GCM).
   — le programme de déchiffrement du chiffré de ce fichier sensible ;
   — les fichiers `rsaaeskey.txt`, `cipheraes.json`.