SAE3.04 Cryptographie

Les As de la Crypto

Deux membres du cercle des cryptographes disparus Alan et Blaise décident de mettre à profit leur connaissance afin de développer une nouvelle méthode de communication sécurisée.

Ils mettent au défi leurs camarades de venir à bout de leur solution. Pour cela ils mettent à leur disposition une trace d'échange réseau et leur donne comme date limite le **vendredi 14 décembre 2024 à minuit** afin de déchiffrer les messages contenus dans cette trace.

Consignes

Vous conserverez les même groupes que pour la première partie de la SAE.

La trace réseau vous sera remis via Celene à la suite de la première partie de la SAE.

L'évaluation de cette deuxième partie portera sur:

- un rapport au format pdf présentant les solutions que vous aurez mises en place,
- le code qui vous aura servi à déchiffrer les messages,
- une soutenance qui sera organisée en fin de période (une communication ultérieure précisera les modalités de soutenance)

Précisions pour le rapport

En vous appuyant sur votre cours, il faudra retrouver l'algorithme cryptographique utilisé ainsi que le mode d'opération. Il faudra également fournir une explication succincte de son fonctionnement. Si la méthode de chiffrement ou le mode d'opération est une variante d'algorithmes connus, il faudra expliciter clairement la différence par rapport à l'existant.

Vous devrez préciser les différentes étapes qui vous ont amené à trouver la solution. Faites le lien avec votre implémentation.

Enfin, il vous faudra expliquer en quoi Alan et Blaise ont été imprudents dans leurs communications et quelles précautions auraient-ils du prendre.