FALLET Nathan
LAMIDEL Arthur
MAKALOU Shérif

Mise en place du TIPE

Dernière modification :
7 février 2021

INTRODUCTION DU SUJET ET DU PROJET

Pour ce TIPE, nous allons nous intéresser aux algorithmes de cryptographie (en lien avec la prévention et la protection des données), et plus précisément à AES (encryption symétrique) et à RSA (encryption asymétrique).

PARTIE INFORMATIQUE DU TIPE

Nous allons essayer d'implémenter un algorithme (soit simplifié, soit proche de la réalité) d'encryption symétrique et asymétrique (représentant chacun le fonctionnement d'AES et RSA)

PARTIE MATHÉMATIQUE DU TIPE

Les algorithmes d'encryption que nous allons implémenter se basent sur des notions mathématiques tel que de la manipulation de matrices ou de nombres premiers très grands.

SCHÉMAS REPRÉSENTANTS LE FONCTIONNEMENT DES ALGORITHMES

Pas de schéma pour cette fois, mais la prochaine version contiendra un schéma pour chaque algorithme que nous étudierons, montrant tout ce qu'il se passera entre les données qui entrent et celles qui sortent.

PARAMÈTRES FIXES ET PARAMÈTRES VARIABLES

Pour les paramètres fixes, il y aura la clé d'encryption symétrique, et le couple clé publique/clé privée pour l'encryption asymétrique.
Pour les paramètres variables, il y aura le contenu à chiffrer/déchiffrer, qui peut être du texte représenté en binaire en ASCII, ou du contenu binaire quelconque, le but étant de montrer que le contenu est bien le même avant chiffrement et après déchiffrement.