AES INES

INES (Intelligent Network Encryption System) est une technologie de cryptographie symétrique polymorphe.

Genèse

Les travaux de Riemann sur la distribution des nombres premiers constituent le point de départ de nos travaux : « les zéros non triviaux de la fonction Zeta sont distribués sur la droite complexe de valeur réelle ½ ».

La machine Enigma (version marine) et les travaux d'Alan Turing sur les automates à états finis sont l'autre source d'inspiration.

Notre démarche a été d'imaginer une machine Enigma dont les rotors tournent de façon aléatoire, capable de résister à toute forme de déchiffrement s'appuyant notamment sur la force brute et les statistiques.

Pour développer INES, le choix a été fait de repartir des fondamentaux ; les travaux de l'école allemande de mathématiques (Göttingen).

Clés de protection

Les clés mises en œuvre s'appuient sur des ensembles aléatoirement distribués, chaque ensemble étant composé de nombres premiers eux-mêmes aléatoirement distribués au sein de l'ensemble ; ce que l'on peut résumer par des ensembles aléatoires, au contenu aléatoirement distribué.

La taille des clés dépend de la relation entre la cardinalité de l'espace d'origine et la cardinalité de l'espace cible.

En l'état actuel **la taille des clefs va de 8.192 bits (force 1) à 262.144 bits (force 4).**

Le mécanisme mis en œuvre est le suivant :

- L'utilisateur impose une clé privée
- L'IA générative fabrique un nonce à partir de cette clé privée
- Ce nonce est exploité par l'IA générative pour fabriquer les ensembles aléatoires aléatoirement distribués.

A noter que :

- La même clé privée ne générera jamais le même nonce.
- En mode polymorphe, à partir d'un nonce inchangé, les ensembles aléatoires aléatoirement distribués sont regénérés (et différents) pour chaque paquet.

Plusieurs fonctions de hachage sont disponibles pour application dynamique à partir de la clef privée en fonction de sa longueur.

Poupées gigognes

Plusieurs passes cryptographiques peuvent être appliquées en série sur un même fichier ou flux.
Un chiffrement de type F(G(H)) sera décodé par application inverse $H^{-1}(G^{-1}(F^{-1}))$.

Implémentation

- 3 modes (@Profil) sont disponibles pour répondre à des besoins différents : RAW, MUX_MONO, MUX_POLY.
- Pour chaque mode, 4 forces (@Level) sont disponibles : BASIC, STANDARD, MEDIUM, HIGH

Mode (Profil)	Usage
RAW	• Chiffrement de fichier. • La signature est dissociée des données.
MUX	• Chiffrement de fichier ou de flux IP. • Un multiplex est généré composé d'un canal de signalisation et d'un canal de données. L'overhead du canal de signalisation est de 1%. **MUX Monomorphe :** le contexte cryptographique est conservé sur l'ensemble de la session. En mode flux, la latence mesurée sur le réseau est de 15 ms. **MUX Polymorphe :** le contexte cryptographique aléatoire est recalculé pour chaque paquet.

Cloud Souverain

La modélisation, les études et les développements ont été réalisés en France.

Nous ne nous appuyons sur aucune technologie tierce.

Les données de l'entreprise sont hébergées en France.

Le fondateur et les collaborateurs de l'entreprise sont français.

Qui sommes-nous ?

JLME a été créée par Jean-Luc Morizur en septembre 2018.

Elle a une double activité : éditeur de solutions et bureau d'études