Le standard d'encryption avancée - Block Ciphers "Different Modes"

BICS- Sean ACHTATOU

University Of Luxembourg

E-mail : sean.achtatou@hotmail.be

1.INTRODUCTION

Ce projet académique permet d'ouvrir les yeux, aux personnes, concernant la perception de la sécurité informatique réel existante sur le net. En effet, ce projet met en œuvre la sécurité ou l'insécurité que l'on peut obtenir avec l'une des applications de Cryptage les plus connus au monde : l'Advanced Encryptions Standard [Le standard d'encryptions avancé]. Ce projet s'intéressera particulièrement à l'algorithme d'Encryptage existant du Standard d'Encryptions Avancé et en analysera chaque partie de manière individuelle pour en connaitre quelle sont leurs fonctions premières. Ces dernières seront les suivantes : Il y aura en tout premier lieu l'Initial Round [Le tour initial] donc la fonction est d'effectuer un AddRoundKey ; puis sera suivi des Rounds[Tours] dans les différentes fonctions tels que SubBytes, ShiftRows, MixColumns et AddRoundKey seront analysés ; et cette partie se terminera avec le Last Round [Dernier Round] étant similaire aux Tours pour les fonctions mais sans celle du MixColumns. Cette méthode d'analyse sera également utilisée autour des trois modes pour le standard d'encryptions avancée existant sur lesquels ce projet s'intéressera : Il y aura en premier lieu le mode ECB[ElectronicBook] utilisant des Blocks de cryptage Indépendant ; puis sera suivi par l'analyse du mode CBC[CypherBlockCipher] utilisant des Blocks Dépendant et un Initialisation Vector [Vecteur d'initialisation] ; et se terminera par le mode CTR[Counter] ayant la particularité d'utiliser un Compteur.

2.Sommaire

Après l'analyse précise de chaque fonction du standard d'encryptions avancé et des trois différents modes énoncés plus tôt, il y aura une comparaison de ces derniers entres eux ce qui permettra par la suite de se faire une idée concernant l'efficacité du mode, et par conséquence lesquels serait le plus apte à encrypter les données de la manière la plus sécurisée possible. Pour que cette tache soit atteinte, il y aura un travail pratique d'implémentation de l'algorithme en lui-même sur un langage de programmation, ici ce projet se basera sur le Python pour sa simplicité et sa lecture des lignes de code très compréhensibles. Lors des différents résultats, il y aura une rapide constatation que le mode ECB n'est pas très recommandé. En effet il y aura l'apparition de répétitions constantes de certaines lettres des données dans l'encryptage de ce dernier permettant une lecture facile et rapide des données même après cryptage. Tandis qu'au contraire, les deux autres modes CBC et CTR apporteront des résultats plus que satisfaisant sur la méthode de cryptage utilisés. Pour renforcés les résultats obtenus, le projet s'appuiera également sur l'utilisation d'images qui seront elles-mêmes encryptées. Il y aura cela dit des exceptions existantes pour chaque mode, permettant l'apport d'une sécurité plus haute, ou moindre.

3.Conclusion

Le projet se conclura par une efficacité plus que satisfaisante, pour obtenir une sécurité d'Encryption des données correctes, pour les modes CBC et CTR, tandis que le mode ECB sera considérer principalement comme un mode à délaisser. Mais comme toute application implémentée, il existe toujours des failles de sécurités, et aucun programme ne peut être considéré comme sécurisé a 100%.