Guilhem COULY

Rapport Cryptographie
Différences entre ECB et CBC

Différences entre ECB et CBC:

Fonctionnement du mode ECB:

Le mode ECB fonctionne en divisant le message en bloc de taille fixe. Ensuite il chiffre chacun de ces blocs indépendamment à l'aide de la clé de chiffrement générée précédemment.

Fonctionnement du mode CBC:

Le mode CBC fonctionne quasiment de la même manière cependant on se sert d'un vecteur d'initialisation afin de modifier le premier bloc. Ensuite pour chiffrer chaque bloc on utilise le bloc précédent.

Différences entre ECB et CBC

La différence repose principalement sur le chiffrement. Avec CBC on se sert des blocs précédents pour chiffrer le message ce qui permet de ne pas obtenir le même chiffrement pour 2 blocs identiques. Avec ECB si des blocs sont similaires nous obtiendrons le même résultat lors du chiffrement. On peut donc remarquer des répétitions.

Failles:

ECB

Avec ECB il est possible d'identifier des valeurs grâce aux répétitions dans le message chiffré.

CBC

Avec CBC nous sommes plus sensible aux répétitions mais il est possible de connaître le message en clair si le padding est mal géré (padding oracle)

GCM:

Comme AES en mode CTR (Counter Mode), AES-GCM chiffre les blocs de texte avec un compteur unique pour chaque bloc.

GCM utilise un nonce (IV de 12 octets recommandé) pour éviter les répétitions. Il génère ensuite une suite de chiffres pseudo-aléatoires via AES qui est XORée avec le texte en clair. Cela empêche donc toute analyse des motifs présents dans les données.

Ce qui assure la confidentialité et l’intégrité des données est lié au Tag.

GCM intègre un tag qui permet de détecter si une modification à eu lieu. Si le tag n’est pas validé lors de la vérification, le message sera rejeté