HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Enzo Allemano

08/05/2022

Duc Alexandre
Fortunato Filipe

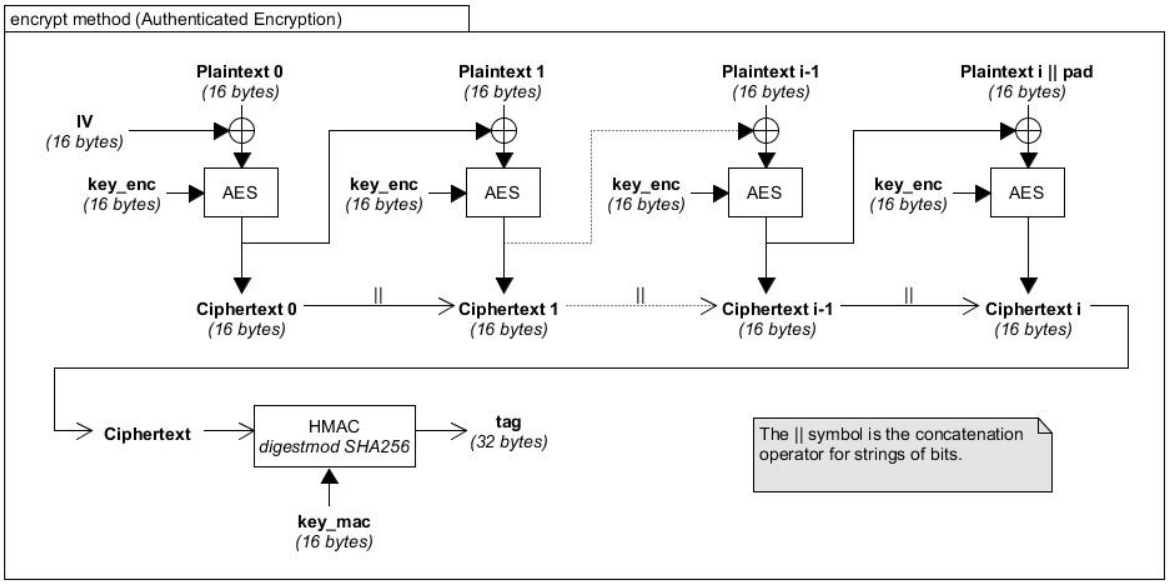
Cryptographie

Rapport laboratoire 2:
Cryptographie symétrique

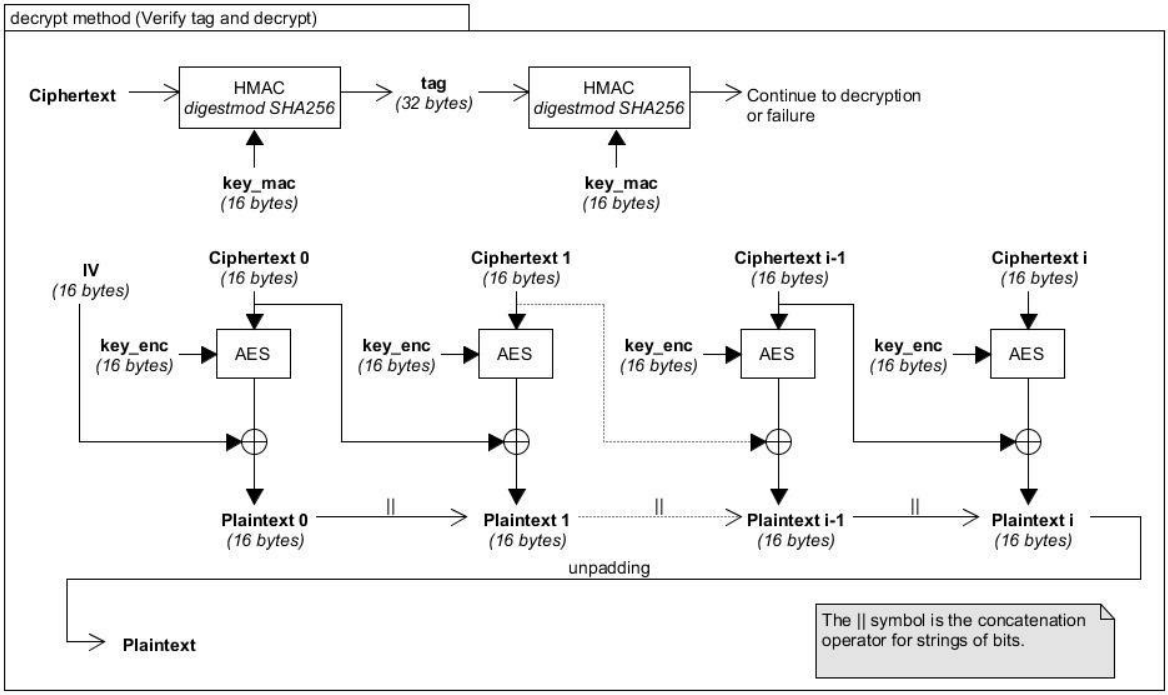
Chiffrement Authentifié

Description de l'implémentation

Chiffrement authentifié



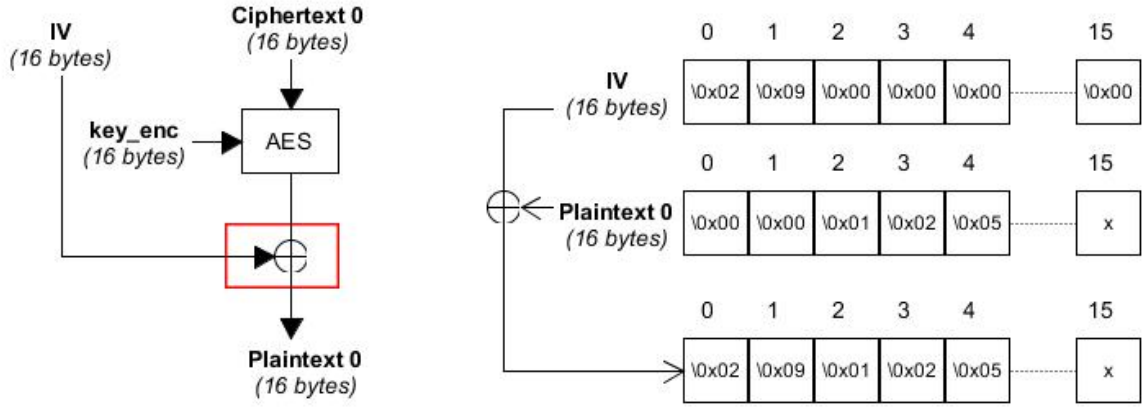
Vérification du tag et déchiffrement



Analyse de l'attaquant

Puisque l'IV est toujours passé en clair, l'attaquant peut le modifier. Cela ne pose pas de problème lors du passage dans le HMAC car on ne tient pas compte de l'IV. Le tag est donc validé, on va donc enchaîner avec le déchiffrement.

De ce fait, un XOR est effectué entre l'IV et le résultat du chiffrement AES. La manière la plus simple de démontrer une attaque est de changer les deux premiers « 0 » du montant du texte clair de la manière suivante :



Maintenant le montant du virement sera de 29'125 CHF.- et non plus de 125.- CHF.-

On pourrait évidement aussi modifier les prochains chiffres du montant à virer en faisant correspondre le résultat du XOR au code ASCII du chiffre désiré.

Correction du chiffrement

Puisque que le problème se trouve dans la modification de l'IV, une solution serait de passer l'IV dans le HMAC. Ainsi, la modification de celui-ci ne serait plus possible puisque il devrait être intègre pour pouvoir valider le tag.

Un Nouveau Système de Chiffrement

Implémentation du déchiffrement

Dans la fonction de chiffrement on trouve : (m étant le message clair)

```
A*(m+IV)
```

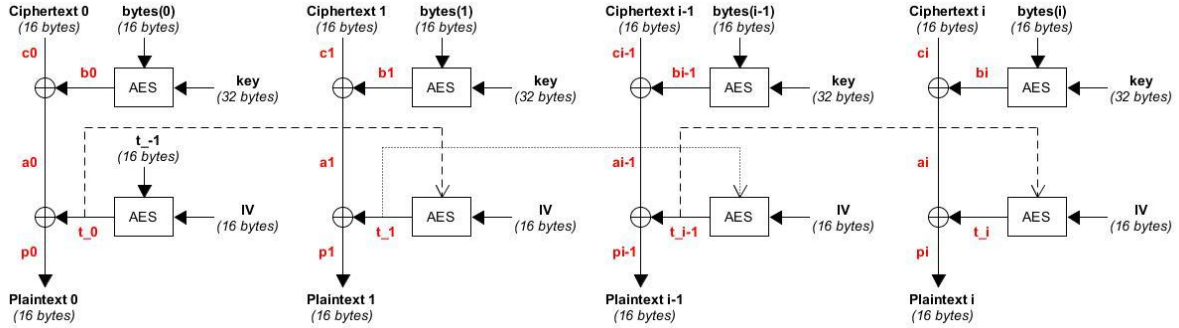
Pour calculer m, il suffit de retourner la fonction de cette manière (c étant le message chiffré) :

```
A.inverse()*(c) + IV
```

On a donc le résultat de la multiplication entre la matrice A inversée et le message chiffré, XORée avec l'IV.

Mode Opératoire

Description du déchiffrement



Analyse de l'attaquant

Connaissance de l'attaquant :

- Un message m3
- Son équivalent chiffré c3
- L'IV est également connu puisque on estime qu'il est toujours transmis en clair (IV3)
- Un message chiffré c3chall
- L'IV avec le quel il a été chiffré (IV3chall)

Le message c3 et c3chall ont été chiffré avec la même clé.

A l'aide de m3, c3 et IV3 on peut trouver :

$$a0 = p0 \oplus t\_0$$

$$b0 = a0 \oplus c0$$

Une fois que le variable `b0` correspondante au premier bloc est trouvée, on répète l'opération pour tout les prochains bloc. (jusqu'à trouver bi)

En effet, cette variable b nous est très utile, elle représente en fait le résultat du chiffrement AES avec la clé inconnue. Cette variable reste la même pour chaque bloc de chiffrement. Ainsi, une fois toute les variables b récupérées, il nous est possible de déchiffrer le message chiffré bloc par bloc.

Durant le déchiffrement de c3chall, il faut également recalculer la variable t_i correspondante à chaque bloc. Ceci n'est pas un problèmes puisque l'on connait IV3chall.

Cette fois ci en prenant c3chall = c et IV3chall :

$$a0 = b0 \oplus c0$$

$$p0 = a0 \oplus t\_0$$

On a donc déchiffré le premier bloc de c3chall.