

UE IN608N (CRYPTO): Attaque intégrale sur une version réduite d'un AES-128

Rapport IN608

Docherty Ronan, Ejjed Zakaria, Gago Jérémy, Guerin Raphaël, Thienard Rodolphe

10 Mai 2022

SOMMAIRE

1	<u>Introduction</u>	3
I	<u>Gestion des commandes et Makefile</u>	3
II	<u>Implémentation de l'AES-128</u>	3
2	SubOctet	4
3	DecaleLignes	4
4	MelangeColonnes	4
5	AjouteCleTour	5
6	Les Tours	5
7	Gestion des clé	5
7.1	Clé Maitre	5
7.2	Clé de Tour	6
8	Chiffrement CTR	6
9	L'AES-128	6
III	<u>Attaque Intégrale AES-128 sur 4 tours</u>	7

INTRODUCTION

Le but de ce Projet était de d'implémenter une version réduite d'un AES-128 avec un mode de chiffrement OFB et/ou CTR en C. Mais aussi et surtout réalisé l'attaque intégrale sur 4 tours de l'AES-128.

Première partie

Gestion des commandes et Makefile

Tout d'abord pour lancer le programme il vous suffit de taper `make` dans le terminal. La commande `make` vous affiche les différents arguments a mettre et les modes disponibles. Les arguments disponibles sont les suivant :

1. `-a` : qui permet de faire l'attaque.
2. `-e` : qui permet de faire l'encryptage et le décryptage d'un fichier.
3. `-out` : qui permet de nommer le fichier de sortie.
4. `-h` : qui permet d'afficher les aides.
5. `-nonce` : qui génère un nombre aléatoire pour le CTR.

Dans le `Makefile` il existe déjà des commandes types comme `make enc` qui effectue un encryptage sur le fichier `matrices.txt`. Nous gérons aussi les erreurs possibles d'arguments, ainsi si les arguments nécessaire ne sont pas présent un message d'erreur apparaîtra.

Deuxième partie

Implémentation de l'AES-128

Un tour d'AES-128 est composé de 4 fonctions :

1. `SubOctet` : Substitue les octets de la matrice d'état.
2. `DecaleLignes` : Décale les lignes de la matrice d'état.
3. `MelangeColonnes` : Mélanges les colonnes de la matrice d'état.
4. `AjouteCleTour` : Ajoute la clé de tour à la matrice d'état.

Nous commencerons donc par la fonction `SubOctet` puisque c'est la première fonction du tour.

SUBOCTET

La fonction `suboctet(int **matrix)` nous permet de substituer l'octet contenu dans une case de notre matrice, à l'aide de la table de substitution de l'AES, qui nous donnera un octet différent du précédent.

DECALELIGNES

La fonction `decale_lignes(int **matrix)`; permet de décaler les lignes de la matrice d'état en fonction de la ligne. Pour faire cela on crée une matrice (`int **`) temporaire qui stockera le décalage des lignes. Ces modifications seront recopiées dans la matrice d'état.

MELANGECOLONNES

La fonction `melange_colonnes(int **matrix)` permet, à l'aide de deux matrices (`operation_double` et `operation_triple`), d'effectuer certaines opérations pour donner de nouvelles valeurs aux lignes de chaque colonne de notre matrice. Les opérations sont les suivantes :

Avec $B_{x,y}$ l'octet contenu dans la ligne x et la colonne y de la matrice entrée en argument, B' étant la matrice résultant des opérations, $2 \star B_{x,y}$ correspondant à l'octet renvoyé par la case de `operation_double`, à la ligne égale à la première partie de l'octet renvoyé par $B_{x,y}$ et égale à la colonne de la deuxième partie de cet octet, idem pour $3 \star B_{x,y}$ mais cette fois dans la matrice `operation_triple`

1.
$$B'_{0,1} = (2 \star B_{0,1}) \oplus (3 \star B_{1,1}) \oplus B_{2,1} \oplus B_{3,1}$$

La première ligne prendra la valeur de : l'octet renvoyé par la case correspondant à l'octet de la ligne 0 de cette colonne dans `operation_double` XOR l'octet renvoyé par la case correspondant à l'octet de la ligne 1 dans `operation_triple` XOR l'octet de la ligne 2 XOR l'octet de la ligne 3.
2.
$$B'_{1,1} = B_{0,1} \oplus (2 \star B_{1,1}) \oplus (3 \star B_{2,1}) \oplus B_{3,1}$$

La seconde prendra la valeur de : l'octet de la ligne 0 XOR l'octet renvoyé par la case correspondant à l'octet de la ligne 1 dans `operation_double` XOR l'octet renvoyé par la case correspondant à l'octet de la ligne 2 dans `operation_triple` XOR l'octet de la ligne 3
3.
$$B'_{2,1} = B_{0,1} \oplus B_{1,1} \oplus (2 \star B_{2,1}) \oplus (3 \star B_{3,1})$$

La troisième prendra la valeur de : l'octet de la ligne 0 XOR l'octet de la

ligne 1 XOR l'octet renvoyé par la case correspondant à l'octet de la ligne 2 dans `operation_double` XOR l'octet renvoyé par la case correspondant à l'octet de la ligne 3 dans `operation_triple`

4. $B'_{3,1} = (3 \star B_{0,1}) \oplus B_{1,1} \oplus B_{2,1}(2 \star B_{3,1})$
 La dernière prendra la valeur de : l'octet renvoyé par la case correspondant à l'octet de la ligne 0 dans `operation_triple` XOR l'octet de la ligne 1 XOR l'octet de la ligne 2 XOR l'octet renvoyé par la case correspondant à l'octet de la ligne 3 dans `operation_double`

AJOUTECLETOUR

La fonction `addroundkey(int **matrix, int **key);` fait un XOR entre la matrice d'état courante et la matrice de la clé de tour.

LES TOURS

Pour les tours d'AES nous avons une fonction `turn(int matrix, int key)`, qui effectue les fonctions précédemment cité (dans le même ordre), nous avons ensuite une fonction `last_turn(int matrix, int key)` qui effectue les même fonctions que `turn` à part la fonction `melange_colonne` et enfin `aes(int matrix, int extended_key, int turns)` qui effectue un nombre défini de fois la fonction `turn` et qui termine par une itération de `last_turn`, dans notre cas 10 tour.

GESTION DES CLÉ

L'AES-128 utilise 2 clés différentes :

1. - **La clé Maitre**
2. - **La clé de Tour**

La clé Maitre est donnée par l'utilisateur en entrée et doit faire 128 bits. La clé de tour quand a elle n'est pas donné en entrée mais utilise la clé maitre pour être créer et change à chaque tour qu'effectue l'AES.

7.1 Clé Maitre

Comme dit précédemment la clé maitre est la clé principale de l'AES-128. Cette clé est donnée par l'utilisateur et doit obligatoirement faire 128 bits. Cette clé est utilisé pour la création des clé de Tour. La clé Maitre étant donné en argument

elle est de type `char*`, nous avons donc créé une fonction qui convertit les `char*` en matrices (en `int **`) `str_to_matrix(char *key)`.

7.2 Clé de Tour

Pour générer la clé de Tour nous avons besoin d'étendre la clé de maitre de 128 bits à 1408 bits. Puis chaque portion de 128 bits de la clé maitre étendue deviens une clé de tour. Comme il y a dix tours il y a 10 clé de tour, plus une pour le dernier tour. La clé de tour est donc générée chaque tour par la fonction `key_extension(int **master_key, int **extended_key)` qui à partir de la clé maitre effectue un SubOctet sur la RotationOctet d'une clé tampon puis un XOR avec les constantes Rcon. L'action RotationOctet est effectuée dans `rotation_left(int *tampon)` et les constantes Rcon dans un variable du même nom.

CHIFFREMENT CTR

Pour faire le chiffrement CTR nous utilisons une fonction `counter_mode(int matrix, int extended_key, int **plaintext, int turns)` qui après avoir fait les tours d'AES sur une matrice, XOR cette matrice avec une autre matrice contenant 16 bits de texte clair. Cette fonction est ensuite utilisée dans la fonction

`loop_ctr(struct chained_matrixchained, int matrix, int extended_key, int turns)` qui quant à elle, nous place au début d'une liste chaînée(ici le message clair) et effectue la fonction `counter_mode` avec les bouts de 16 bits de texte clair, autant de fois qu'il y'a de bouts.

L'AES-128

Après avoir tapé la commande :

```
./$(BIN) "aes128 clemaitre" "azertyuiopqsdfgh"
-e test.txt -out sortie.txt
```

le programme va effectuer l'encryptage du fichier `test.txt` avec la clé maitre `"aes128 clemaitre"` en utilisant la nonce `azertyuiopqsdfgh` pour le chiffrement CTR et `sortie.txt` comme fichier de sortie d'encryptage.

Mais comment cela se passe dans le code ?

Tous d'abord la fonction `commande` comprend que l'on veut encrypter (`-e`) le fichier `test.txt` avec la clé maitre `"aes128 clemaitre"` et la nonce `"azertyuiopqsdfgh"`. A ce moment là le programme doit récupérer le message à encrypter et le transformer en matrices. Pour cela on utilise : `init_plaintext(FILE *file, char *filename)`

qui justement transforme le message en une liste chaînée (`struct init_matrix`) contenant toutes les matrices créées. Si jamais le message contient un nombre non multiple de 16, la fonction se charge de remplir la matrice non pleine pour pouvoir effectuer correctement l'AES. On lance ensuite la fonction :

`aes_128(struct init_matrix *init, int **master_key, int **nonce)` qui effectue l'AES-128 complet utilisant les différentes fonctions expliquées précédemment.

Tout d'abord `aes_128` crée la clé de tour avec la fonction `key_extension` puis lance la fonction :

`loop_ctr(struct chained_matrix *chained, int **matrix, int **extended_key, int turns)` qui s'occupe de faire l'AES avec ces 10 tours et fait le chiffrement

CTR du résultat. Une fois cela fait `aes_128` se termine et renvoie la liste chaînée de matrices contenant le chiffré du message clair. On peut donc écrire le chiffré dans le

fichier de sortie avec `write_to_file(struct init_matrix *init, char *outfile)`.

Troisième partie

Attaque Intégrale AES-128 sur 4 tours