Algorithme AES
Advanced Encryption Standard

Saiida LAZAAR

Département Mathématiques Informatique
Université AbdelMalek Essaadi – ENSA de Tanger

Février 2019

Sommaire

Introduction

Ce cours présente les connaissances essentielles pour appréhender l'algorithme AES de chiffrement par blocs.
Il inclut aussi des notions de base sur le corps de Galois $GF(2^8)$ dans lequel de nombreuses opérations de chiffrement sont effectuées.

Un peu d'arithmétique

- L'addition dans $GF(2^8)$ correspond au XoR bit à bit. La multiplication et l'addition sur $GF(2^8)$ conduisent à un espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$: $GF(2^8) = \mathbb{Z}/2^8\mathbb{Z}$.

- Un élément de $GF(2^8)$ est un polynôme de degré ≤ 7 qui s'écrit sous forme polynômiale, binaire ou hexadécimale.

On a : $GF(2^8) = \mathbb{Z}/2^8\mathbb{Z}[x]/n(x), n(x) = x^8 + x^4 + x^3 + x + 1$.

- La multiplication de deux éléments de $GF(2^8)$ s'écrit sous forme polynômiale, on les multiplie ensuite et on cherche le reste de la division du résultat par $n(x)$.

L'octet $(b_7, b_6, \ldots b_0)$ correspond à : $\sum_{i=0}^{7} b_i \alpha^i \in GF(2^8), \alpha$ est une racine $n(x)$.

Présentation de AES

- En 1997, la sécurité de DES n'était plus garantie face à une recherche exhaustive de la clé ; 3DES était jugé trop lent.
- 15 propositions ont été présentées pour une nouvelle norme du gouvernement des USA, parmi les 5 finalistes, Rijndael fût choisi pour devenir AES.
- Serpent fût un finaliste AES mais 3 fois plus lent que AES, et difficile à implémenter.
- AES a été publié par le NIST (National Institute of Standards and Technology) (décembre 2001) ;
- AES est un nouveau standard qui a succedé à DES (Data Encryption Standard).

Critères de sélection de AES

Le NIST a défini trois critères pour choisir le nouveau standard :

- Sécurité
- Coût
- Implémentation (Performance)

AES ?

- AES est un algorithme de chiffrement symétrique, par blocs.
- AES opère avec un bloc de 128-bits.
- AES fonctionnes pour 3 type de clés : 128, 192, 256 bits.
- Pour chaque taille de clé, AES fonctionne selon 1 nombre de tour bien fixé : 10, 12 ou 14 tours.

AES ?

Version	Taille clé	Taille bloc	Nombre de tours
AES-128	128-bits	128	10
AES-192	192-bits	128	12
AES-256	256-bits	128	14

Description de AES

AES est un sytème de chiffrement itératif qui fonctionne selon des tours.

A chaque tour, on applique au bloc d'entrée une **substitution** non linéaire suivie d'une fonction (généralement linéaire) appelée **permutation**.

- On transforme le message de 128 bits en un tableau appelé STATE-Etat.

Le chiffrement découpe chaque bloc de 128 bits en 16 octets et chaque bloc est représenté sous forme d'une matrice carrée 4x4, les octets sont numérotés de 1 à 16 gauche à droite.

Fonctionement de AES

Le bloc initial de AES (1er tableau STATE) est à chiffrer : On l'additionne bit à bit avec une clé de tour initiale K_0. La clé de tour K_i est un bloc de 128 bits différent à chaque tour.

On applique ensuite de façon répétée quatre procédures :

- Transformation SubByte : Substitution des octets, elle applique sur chacun des 16 octets de l'état interne une S-Boîte qui a pour but de faire diparaitre les structures linéaires et algébriques du chiffrement (Assure une bonne confusion)
- Transformation ShiftRows : Effectue des rotations vers la gauche.
- Transformation MixColumns : Combine les 4 octets de chaque colonne de la matrice Etat avec une transformation linéaire pour assurer une bonne **diffusion**.
- Opération AddRoundKey

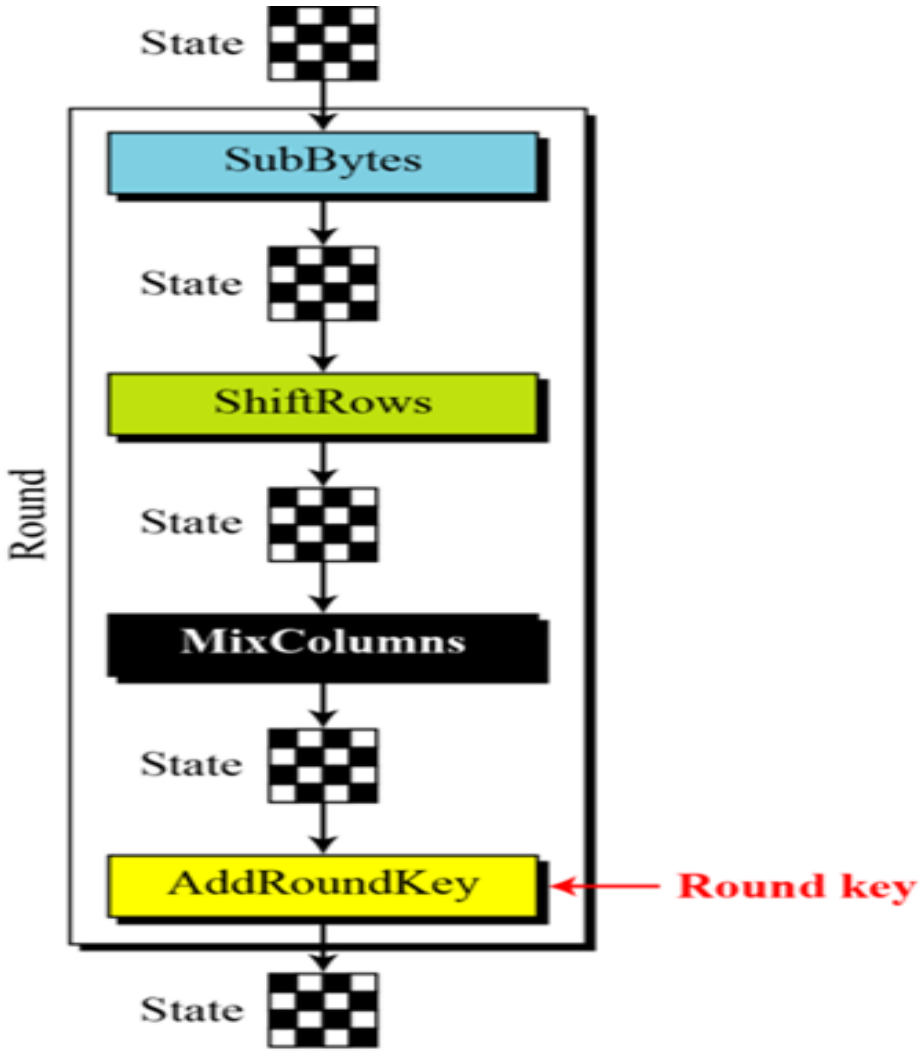

FIGURE – Fonctionnement de AES

Opérations dans AES

AES Utilise les transformations suivantes :

- SubBytes : Substitution
- ShiftRows : Permutation
- MixColumns : Mélange des colonnes
- AddRoundKey : Addition des clés

1ère transformation de AES : First State

- Le message de AES est une suite de 16 octets :

$$M = a_0 a_1 \dots a_{15} \text{ où } a_i \in GF(2^8).$$

- Le message est copié dans un tableau appelé **STATE** de 4 lignes et 4 colonnes.

- Le tableau est transformé en un tableau de 4 - 32 bits :

$$W_0 W_1 W_2 W_3.$$

où W_i : word composé de 4 octets de $GF(2^8)$, $W_0 = a_0 a_1 a_2 a_3$. ($a_i = (b_7, b_6, \dots b_0)$ correspond à $\sum_{i=0}^{7} b_i \alpha^i \in GF(2^8), \alpha$ est une racine $n(x)$.)

1ère transformation de AES : First State

a_0	a_4	a_8	a_12
a_1	a_5	a_9	a_13
a_2	a_6	a_10	a_14
a_3	a_7	a_11	a_15

Exempe : First State

Exemple :

Texte en clair : AESUSESAMATRIXZZ

Conversion : 00041214120412000C00131108231919

00	12	0C	08
04	04	00	23
12	12	13	19
14	00	11	19

ShiftRows

Cette transformation est basée sur une permutation circulaire.

Chaque ligne du tableau STATE subit une permutation circulaire vers la gauche.

- Permutation de 0 cran pour la ligne 0.
- Permutation de 1 cran pour la ligne 1.
- Permutation de 2 crans pour la ligne 2.

ShiftRows

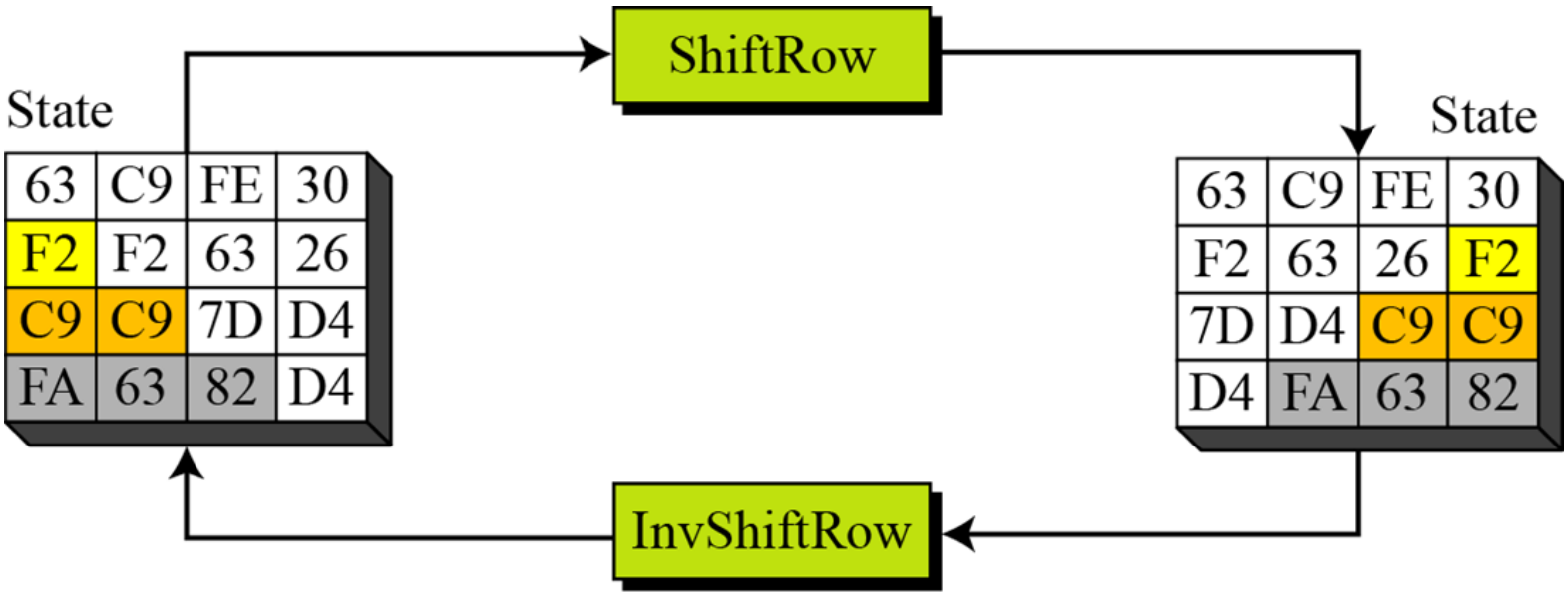

FIGURE – source

MixColumns

Elle combine les 4 octets de chaque colonne de la matrice Etat avec une transformation linéaire.

- Chaque colonne est lue comme un polynôme de degré 3 sur $GF(2^8)$ multiplié modulo $x^4 + 1$ par le polynôme :

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}.$$

- Il s'agit d'opérations dans : $GF(2^8)[x]/(x^4 + 1)$.

- Ici, la colonne $s_j = (s_{0,j}, s_{1,j}, s_{2,j}, s_{3,j})$ de STATE est identifiée avec le polynôme : $s_{0,j} + s_{1,j}x + s_{2,j}x^2 + s_{3,j}x^3 \in GF(2^8)[x]$.

AddRoundKey

Le tableau obtenu est remis en ligne de 16 octets (suite de 128 bits).

Cette suite est additionnée bit à bit mod 2 (XoR) avec la clé de tour, qui est à 128 bits.

Organigramme global

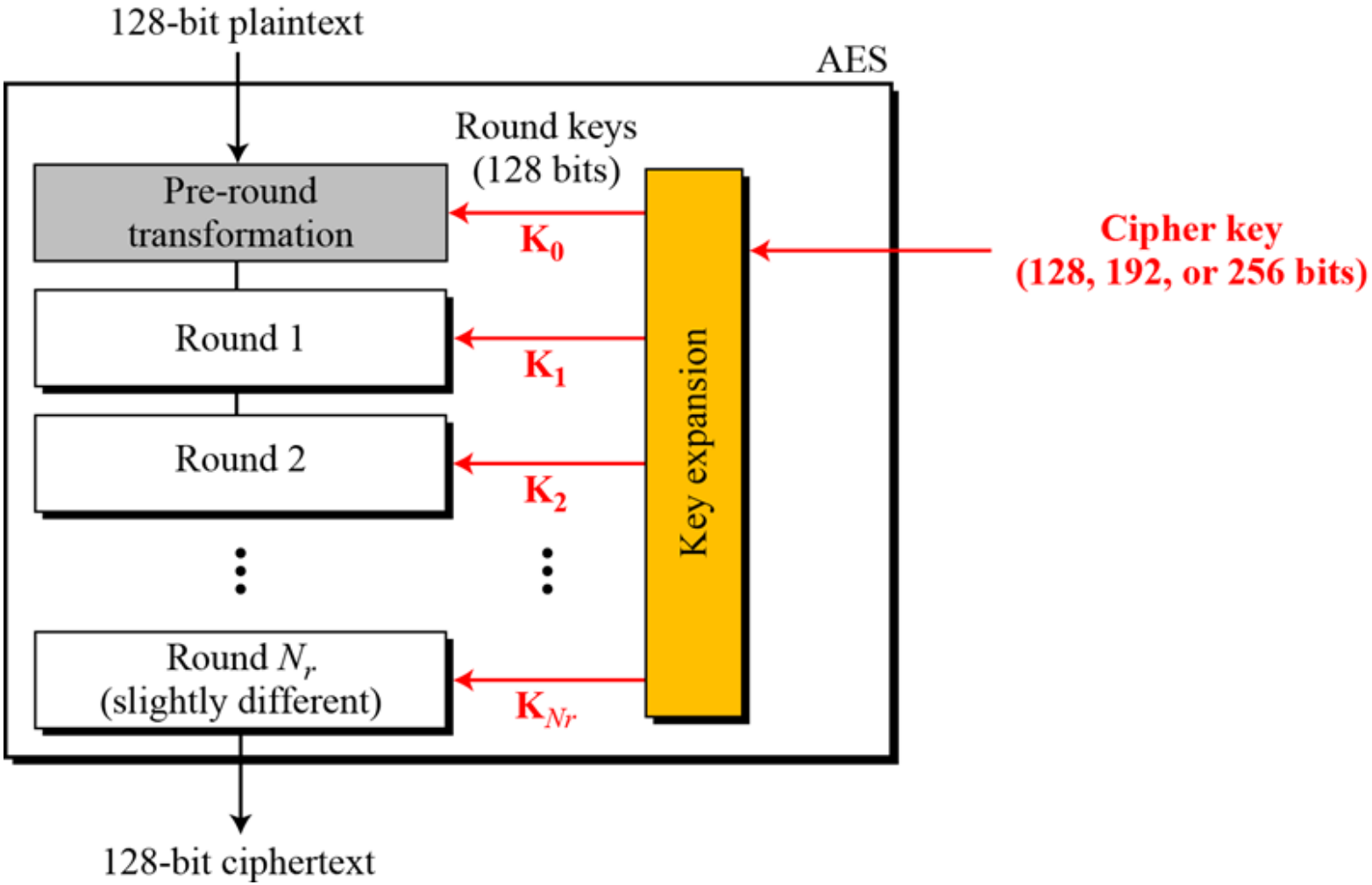

FIGURE – Fonctionnement des tours et sous-clés

Biblio

- Damien Vergnaud. Exercices et problèmes de cryptographie. Edt. Dunod 2015.

- Niel Ferguson and Bruce Schneier. Cryptographie en pratique. Edt. Vuibert 2003.