



# FIPS 197

## Introduction

Éléments importants

Structure du document

## Définitions

Glossaire des termes et des définitions

Paramètres, symboles et fonctions de l'algorithme

## Notation et conventions

Entrées et sorties

Octets

Tableaux d'octets

L'état intermédiaire de chiffrement (State)

Représentation de l'état intermédiaire comme un tableau de colonnes

Synthèse

## Concepts mathématiques

Addition

Multiplication

Cas général

Multiplication par  $x$

Polynômes à coefficients dans  $GF(2^8)$

# Introduction



Le rapport FIPS 197 décrit le standard AES (Advanced Encryption Standard), qui est un algorithme de chiffrement symétrique par blocs

## Éléments importants

L'algorithme AES est basé sur l'algorithme Rijndael

Il traite des blocs de données de 128 bits et utilise des clés de chiffrement de 128, 192 et 256 bits

L'algorithme Rijndael a été conçu pour gérer des tailles de blocs et de clés supplémentaires, mais ces options ne sont pas adoptées dans le standard AES

Les différentes versions d'AES sont désignées comme AES-128, AES-192 et AES-256, en fonction de la longueur de clé utilisée

## Structure du document

1. Définitions des termes, acronymes, paramètres, symboles et fonctions de l'algorithme
2. Notations et conventions utilisées dans la spécification de l'algorithme, y compris l'ordre et la numérotation des bits, octets et mots
3. Propriétés mathématiques utiles pour comprendre l'algorithme
4. Spécification de l'algorithme, couvrant l'expansion de la clé, le chiffrement et le déchiffrement
5. Questions liées à l'implémentation, telles que le support de la longueur de clé, les restrictions de clé et les tailles de blocs, de clés et de tours supplémentaires

Enfin, le rapport se termine par plusieurs annexes contenant des exemples détaillés pour l'expansion de la clé et le chiffrement, des exemples de vecteurs pour le chiffrement et le déchiffrement inverse, ainsi qu'une liste de références

## Définitions

Pour cette partie, on propose seulement une traduction de la norme, n'ayant pas d'éléments importants à y ajouter

## Glossaire des termes et des définitions

Voici les définitions utilisées tout au long de cette norme :

**AES** : Advanced Encryption Standard (Standard de chiffrement avancé).

**Transformation affine** : Une transformation consistant en une multiplication par une matrice suivie de l'addition d'un vecteur.

**Tableau (array)** : Une collection énumérée d'entités identiques (par exemple, un tableau d'octets).

**Bit** : Un chiffre binaire ayant une valeur de 0 ou 1.

**Bloc (block)** : Séquence de bits binaires qui constituent l'entrée, la sortie, l'état et la clé de tour. La longueur d'une séquence est le nombre de bits qu'elle contient. Les blocs sont également interprétés comme des tableaux d'octets.

**Octet** : Un groupe de huit bits traité soit comme une seule entité, soit comme un tableau de 8 bits individuels.

**Chiffrement (Cipher)** : Série de transformations qui convertit le texte en clair en texte chiffré à l'aide de la clé de chiffrement.

**Clé de chiffrement (Cipher Key)** : Clé cryptographique secrète utilisée par la routine d'expansion de clé pour générer un ensemble de clés de tour ; peut être représentée comme un tableau rectangulaire d'octets, ayant quatre rangées et Nk colonnes.

**Texte chiffré (Ciphertext)** : Données en sortie du chiffrement ou en entrée du déchiffrement inverse.

**Déchiffrement inverse (inverse Cipher)** : Série de transformations qui convertit le texte chiffré en texte en clair à l'aide de la clé de chiffrement.

**Expansion de clé** : Routine utilisée pour générer une série de clés de tour à partir de la clé de chiffrement.

**Texte en clair** : Données en entrée du chiffrement ou en sortie du déchiffrement inverse.

**Rijndael** : Algorithme cryptographique spécifié dans ce standard de chiffrement avancé (AES).

**Clé de tour (Round key)** : Les clés de tour sont des valeurs dérivées de la clé de chiffrement à l'aide de la routine d'expansion de clé ; elles sont appliquées à l'état dans le chiffrement et le déchiffrement inverse.

**État (State)** : Résultat intermédiaire du chiffrement pouvant être représenté comme un tableau rectangulaire d'octets, ayant quatre rangées et Nb colonnes.

**S-box** : Table de substitution non linéaire utilisée dans plusieurs transformations de substitution d'octets et dans la routine d'expansion de clé pour effectuer une substitution un-à-un d'une valeur d'octet.

**Mot (Word)** : Un groupe de 32 bits traité soit comme une seule entité, soit comme un tableau de 4 octets.

## Paramètres, symboles et fonctions de l'algorithme

Les paramètres, symboles et fonctions suivants sont utilisés tout au long de cette norme :

**AddRoundKey()** : Transformation dans le chiffrement et le déchiffrement inverse où une clé de tour est ajoutée à l'état à l'aide d'une opération XOR. La longueur d'une clé de tour est égale à la taille de l'état (c'est-à-dire, pour  $Nb = 4$ , la longueur de la clé de tour est égale à 128 bits/16 octets).

**MixColumns()** : Transformation dans le chiffrement qui prend toutes les colonnes de l'état et mélange leurs données (indépendamment les unes des autres) pour produire de nouvelles colonnes.

**InvMixColumns()** : Transformation dans le déchiffrement inverse qui est l'inverse de MixColumns().

**ShiftRows()** : Transformation dans le chiffrement qui traite l'état en décalant cycliquement les trois dernières rangées de l'état avec des décalages différents.

**InvShiftRows()** : Transformation dans le déchiffrement inverse qui est l'inverse de ShiftRows().

**SubBytes()** : Transformation dans le chiffrement qui traite l'état à l'aide d'une table de substitution non linéaire d'octets (S-box) qui opère sur chacun des octets de l'état indépendamment.

**InvSubBytes()** : Transformation dans le déchiffrement inverse qui est l'inverse de SubBytes().

**K** : Clé de chiffrement.

**Nb** : Nombre de colonnes (mots de 32 bits) composant l'état. Pour cette norme,  $Nb = 4$ .

**Nk** : Nombre de mots de 32 bits composant la clé de chiffrement. Pour cette norme,  $Nk = 4, 6$  ou  $8$ .

**Nr** : Nombre de tours, qui est une fonction de  $Nk$  et  $Nb$  (qui est fixé). Pour cette norme,  $Nr = 10, 12$  ou  $14$ .

`Rcon[]` : Le tableau de mots constants de tour.

`RotWord()` : Fonction utilisée dans la routine d'expansion de clé qui prend un mot de quatre octets et effectue une permutation cyclique.

`SubWord()` : Fonction utilisée dans la routine d'expansion de clé qui prend un mot d'entrée de quatre octets et applique une S-box à chacun des quatre octets pour produire un mot de sortie.

`XOR` : Opération OU exclusif.

`⊕` : Opération OU exclusif.

`⊗` : Multiplication de deux polynômes (chacun de degré < 4) modulo  $x^4 + 1$ .

`•` : Multiplication dans un corps fini.

# Notation et conventions

## Entrées et sorties

L'algorithme AES utilise des séquences de 128 bits pour les entrées et sorties, appelées blocs, et une clé de chiffrement de 128, 192 ou 256 bits. Aucune autre longueur n'est autorisée par cette norme. Les bits dans les séquences sont numérotés de 0 à un de moins que la longueur de la séquence et sont appelés indices, qui se situent dans des plages spécifiques en fonction de la longueur du bloc et de la clé.

## Octets

L'unité de base pour le traitement dans l'algorithme AES est un octet (`byte`), composé de huit bits traités comme une seule entité. Les séquences d'entrée, de sortie et de clé de chiffrement sont traitées comme des tableaux d'octets, en divisant ces séquences en groupes de huit bits contigus. Les octets dans le tableau sont référencés par  $a_n$  ou  $a[n]$ , où  $n$  varie en fonction de la longueur de la clé et du bloc.

Les valeurs des octets dans l'algorithme AES sont présentées comme la concaténation de leurs valeurs de bits individuelles, et sont interprétées comme des éléments de corps fini à l'aide d'une représentation polynomiale. Par exemple,  $\{01100011\}$  identifie l'élément de corps fini  $x^6 + x^5 + x + 1$ .

Il est également pratique d'utiliser la notation hexadécimale pour représenter les valeurs des octets, chaque groupe de quatre bits étant représenté par un seul caractère. Ainsi, l'élément  $\{01100011\}$  peut être représenté par  $\{63\}$ .

Certaines opérations de corps fini impliquent un bit supplémentaire ( $b_8$ ) à gauche d'un octet de 8 bits. Lorsque ce bit supplémentaire est présent, il apparaît comme '{01}' immédiatement avant l'octet de 8 bits.

En résumé, dans l'algorithme AES, l'unité de base est un octet, composé de huit bits. Les séquences d'entrée, de sortie et de clé de chiffrement sont traitées comme des tableaux d'octets. Les valeurs des octets sont interprétées comme des éléments de corps fini à l'aide d'une représentation polynomiale. La notation hexadécimale est souvent utilisée pour représenter les valeurs des octets, facilitant ainsi la représentation.

## Tableaux d'octets

Les octets sont constitués de groupes de 8 bits consécutifs de la séquence d'entrée. Par exemple,  $a_0$  contient les bits 0 à 7,  $a_1$  contient les bits 8 à 15, et ainsi de suite. La même logique s'applique aux clés de 192 et 256 bits. La formule générale pour obtenir l'octet  $a_n$  est :

$$a_n = \text{input}_{8n}, \text{input}_{8n+1}, \dots, \text{input}_{8n+7}$$

Input bit sequence	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	...
Byte number									0							1								2	...
Bit numbers in byte	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	...

La figure 2 montre comment les bits à l'intérieur de chaque octet sont numérotés, en considérant les sections 3.2 et 3.3 ensemble.

## L'état intermédiaire de chiffrement (State)

On explique ici le fonctionnement interne de l'algorithme AES avec un tableau à deux dimensions appelé "State"

Le tableau *State* est composé de quatre rangées d'octets, chacune contenant  $Nb$  octets, où  $Nb$  est la longueur du bloc divisée par 32. Pour cette norme,  $Nb = 4$ .

Chaque octet individuel dans le tableau *State* possède deux indices : le numéro de ligne  $r$  avec ( $0 \leq r < 4$ ) et le numéro de colonne  $c$  avec ( $0 \leq c < Nb$ ). Ainsi, un octet individuel du tableau *State* peut être référencé sous la forme  $s_{r,c}$  ou  $s[r, c]$ .

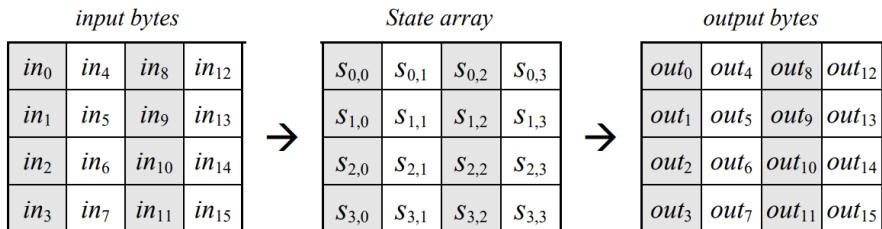


Figure 3. State array input and output.

Au début de l'algorithme, les octets d'entrée sont copiés dans le tableau *State* comme illustré dans la figure 3. Les opérations de chiffrement ou de déchiffrement sont ensuite effectuées sur ce tableau *State*, puis sa valeur finale est copiée dans les octets de sortie.

L'entrée est copiée dans le tableau *State* selon le schéma suivant :

$$s[r, c] = in[r + 4c] \text{ pour } 0 \leq r < 4 \text{ et } 0 \leq c < Nb,$$

À la fin du chiffrement ou du déchiffrement, le tableau *State* est copié dans le tableau de sortie *out* de la manière suivante :

$$out[r + 4c] = s[r, c] \text{ pour } 0 \leq r < 4 \text{ et } 0 \leq c < Nb.$$

En bref, l'algorithme AES fonctionne en interne en utilisant un tableau à deux dimensions appelé *State*. Le tableau est composé de 4 rangées et de  $Nb$  colonnes d'octets. Les opérations de chiffrement et de déchiffrement sont effectuées sur le tableau *State*. Les octets d'entrée sont d'abord copiés dans le tableau *State*, puis les opérations sont réalisées, et enfin, le contenu du tableau *State* est copié dans les octets de sortie.

## Représentation de l'état intermédiaire comme un tableau de colonnes

Il est expliqué que les quatre octets de chaque colonne du tableau "State" forment des mots (words) de 32 bits, où le numéro de rangée  $r$  sert d'indice pour les quatre octets de chaque mot. Ainsi, l'état peut être interprété comme un tableau unidimensionnel de mots de 32 bits (colonnes),  $w_0 \dots w_3$ , où le numéro de colonne  $c$  fournit un indice pour ce tableau. Par exemple, en se basant sur la figure 3, le *State* peut être considéré comme un tableau de quatre mots, comme suit :

$$w_0 = s_{0,0} s_{1,0} s_{2,0} s_{3,0}$$

$$w_1 = s_{0,1}s_{1,1}s_{2,1}s_{3,1}$$

$$w_2 = s_{0,2}s_{1,2}s_{2,2}s_{3,2}$$

$$w_3 = s_{0,3}s_{1,3}s_{2,3}s_{3,3}$$

## Synthèse

La section sur les notations et conventions d'AES aborde plusieurs aspects clés du fonctionnement de l'algorithme AES :

- 1** Les entrées et sorties de l'algorithme AES sont des séquences de 128 bits, et la clé de chiffrement peut être de 128, 192 ou 256 bits. Les bits sont numérotés de 0 à un nombre inférieur à la longueur de la séquence
- 2** L'unité de base pour le traitement dans l'algorithme AES est un octet, qui est une séquence de huit bits traitée comme une seule entité. Les octets sont représentés en notation hexadécimale pour plus de commodité
- 3** Les séquences de bits sont traitées comme des tableaux d'octets, en divisant les séquences en groupes de huit bits contigus. Les tableaux sont indexés par des nombres entiers dans des plages spécifiques en fonction de la longueur de la clé
- 4** L'algorithme AES effectue des opérations sur un tableau bidimensionnel d'octets appelé *State*. Le tableau *State* est composé de quatre rangées d'octets, chacune contenant un nombre d'octets  $Nb$ , où  $Nb$  est la longueur du bloc divisée par 32. Les octets individuels dans le tableau *State* sont référencés par deux indices, le numéro de rangée  $r$  et le numéro de colonne  $c$
- 5** Les quatre octets de chaque colonne du tableau *State* forment des mots (*words*) de 32 bits, où le numéro de rangée  $r$  sert d'indice pour les quatre octets de chaque mot. L'état peut être interprété comme un tableau unidimensionnel de mots de 32 bits (colonnes)

Ces conventions et notations sont essentielles pour comprendre le fonctionnement de l'algorithme AES et faciliter la mise en œuvre de cet algorithme de chiffrement.

# Concepts mathématiques

## Addition



On réalise une opération d'addition entre les polynômes grâce à l'opération XOR

Table de vérité du XOR (ou exclusif) :

a	b	a XOR b
0	0	0
0	1	1
1	0	1
1	1	0

L'addition est une opération effectuée dans le cadre de la transformation `AddRoundKey`, qui a lieu à chaque tour de l'algorithme, à la fois lors du chiffrement et du déchiffrement. L'addition dans AES est définie comme l'opération "ou exclusif" (XOR) bit à bit sur les octets (bytes) des données en entrée.

L'addition XOR est une opération commutative, ce qui signifie que l'ordre dans lequel les bits sont ajoutés n'a pas d'importance. Elle est également associative, ce qui signifie que l'ordre dans lequel les bits sont ajoutés peut être modifié sans changer le résultat final.

Il est important de noter que l'opération XOR est sa propre inverse, c'est-à-dire que si  $A \text{ XOR } B = C$ , alors  $A = C \text{ XOR } B$  et  $B = A \text{ XOR } C$ . Cette propriété est utile pour le déchiffrement dans AES, car elle permet de retrouver facilement l'état précédent à partir de l'état chiffré, en utilisant simplement l'opération XOR avec la même clé de tour.

## Multiplication

### Cas général

La multiplication est utilisée principalement dans la transformation **MixColumns**, qui a lieu lors de chaque tour de l'algorithme, à l'exception du dernier, lors du processus de chiffrement. Elle est également utilisée dans la transformation inverse **InvMixColumns** lors du déchiffrement.

Dans AES, la multiplication est définie comme une opération sur les éléments d'un corps fini appelé GF(2<sup>8</sup>), ou corps de Galois de 2<sup>8</sup> éléments.

**Corps fini** : ensemble fini d'éléments avec des opérations d'addition, de soustraction, de multiplication et de division. Dans le cas de GF(2<sup>8</sup>), les éléments sont des polynômes de degré inférieur à 8 avec des coefficients binaires (0 ou 1), et les opérations sont définies modulo un polynôme irréductible de degré 8.

La multiplication dans le champ de Galois GF(2<sup>8</sup>) est réalisée en utilisant une multiplication polynomiale. Chaque octet est considéré comme un polynôme de degré 7 dont les coefficients sont soit 0, soit 1. La multiplication de deux octets est alors réalisée en multipliant les deux polynômes correspondants, puis en réduisant le résultat modulo un polynôme irréductible de degré 8.

La réduction modulo un polynôme irréductible de degré 8 permet de ramener le résultat de la multiplication à un octet de 8 bits.

**Polynôme irréductible** :  $x^8 + x^4 + x^3 + x + 1$

En résumé, cette opération est réalisée en multipliant deux octets considérés comme des polynômes, puis en réduisant le résultat modulo un polynôme irréductible de degré 8.

## Multiplication par $x$

La multiplication par  $x$  dans GF(2<sup>8</sup>) est effectuée en multipliant un élément (représenté par un polynôme) par le polynôme  $x$ , puis en réduisant le résultat modulo le polynôme irréductible défini pour AES, qui est  $x^8 + x^4 + x^3 + x + 1$ .

En termes d'opérations sur les octets, la multiplication par  $x$  peut être réalisée en effectuant un décalage vers la gauche de l'octet, puis en effectuant une opération XOR avec le polynôme irréductible (sous forme d'octet) si le bit le plus à gauche (bit de poids fort) de l'octet initial est 1. Cette opération XOR est effectuée pour garantir que le résultat reste un polynôme de degré inférieur à 8.

Exemple :

1. Supposons que l'élément à multiplier par  $x$  soit représenté par l'octet  $A = 10011011$ .

2. On effectue un décalage vers la gauche : 00110110.
3. Comme le bit le plus à gauche de A est 1, on effectue un XOR avec le polynôme irréductible (sous forme d'octet) :  $00110110 \oplus 00011011 = 00101101$ .

Cette multiplication par  $x$  est utilisée à plusieurs reprises dans l'algorithme AES, notamment dans les transformations `MixColumns`, `InvMixColumns` et la génération des tables de substitution pour la transformation `SubBytes`.

## Polynômes à coefficients dans $\text{GF}(2^8)$

Dans cette section, il est expliqué que les polynômes à coefficients dans  $\text{GF}(2^8)$  sont des polynômes dont les coefficients sont des éléments du corps fini  $\text{GF}(2^8)$ . Les opérations d'addition, de soustraction, de multiplication et de division sur ces polynômes sont définies en utilisant les opérations correspondantes dans  $\text{GF}(2^8)$ . Par exemple, pour additionner deux polynômes à coefficients dans  $\text{GF}(2^8)$ , on additionne les coefficients correspondants en utilisant l'opération XOR, qui est l'addition dans  $\text{GF}(2^8)$ .

Un aspect important de cette section est la représentation des données et des clés de l'algorithme AES sous forme de polynômes à coefficients dans  $\text{GF}(2^8)$ . Le bloc de données (State) et la clé de chiffrement sont représentés sous forme de matrices  $4 \times 4$  d'octets, où chaque octet correspond à un élément de  $\text{GF}(2^8)$ . Chaque colonne de la matrice d'état peut être interprétée comme un polynôme de degré 3 avec des coefficients dans  $\text{GF}(2^8)$ , et chaque colonne de la matrice de clé peut être interprétée comme un polynôme de degré 3 avec des coefficients dans  $\text{GF}(2^8)$ .

Dans la transformation `MixColumns`, chaque colonne de la matrice d'état est traitée comme un polynôme de degré 3 sur  $\text{GF}(2^8)$ , et est multipliée par un polynôme fixe  $a(x) = 3x^3 + x^2 + x + 2$ . Cette multiplication a pour effet de mélanger les octets dans les colonnes de la matrice d'état, renforçant ainsi la diffusion des données dans le processus de chiffrement. Lors du déchiffrement, la transformation `InvMixColumns` utilise la multiplication par le polynôme inverse de  $c(x)$ , c'est-à-dire  $a^{-1}(x) = 11x^3 + x^2 + 9x + 14$ .