AES ou Rinjdael

AES est un Algorithme de cryptographie à clé symétrique. Son chiffrement est rapide, ce qui le rend parfaitement adapté pour les applications, les microprogrammes et le matériel qui exigent une faible latence ou un haut débit, comme les pare-feu et les routeurs.
Il est utilisé dans de nombreux protocoles, tel SSL/TLS, ainsi que dans les applications et les périphériques récents qui utilisent le chiffrement.

Fonctionnement général

AES comprend trois algorithmes de chiffrement par blocs : AES-128, AES-192 et AES-256.

Chaque code chiffre et déchiffre les données par blocs de 128 bits au moyen de clés cryptographiques de 128, 192 et 256 bits, respectivement

Les codes symétriques ou à clé secrète utilisent la même clé pour le chiffrement et le déchiffrement. L'expéditeur et le destinataire doivent donc connaître et utiliser la même clé secrète.
Un tour comprend plusieurs étapes de traitement : la substitution, la transposition et la combinaison du texte en clair en entrée avant sa transformation finale en cryptogramme.
Il faut 10 tours pour une clé de 128 bits, 12 pour une clé de 192 bits et 14 pour une clé de 256 bits.

Fondé sur des entrées permutés selon une table définie au préalable, l'algorithme offre des tailles de blocs et de clés qui sont des multiples de 32 (compris entre 128 et 256 bits). Ces différentes opérations sont répétées plusieurs fois et définissent un «tour». A chaque tour, une **clé unique** est calculée à partir de la clé de cryptage et incorporée dans les calculs. L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait donc entre 128, 192 ou 256 bits.

Fonctionnement plus technique

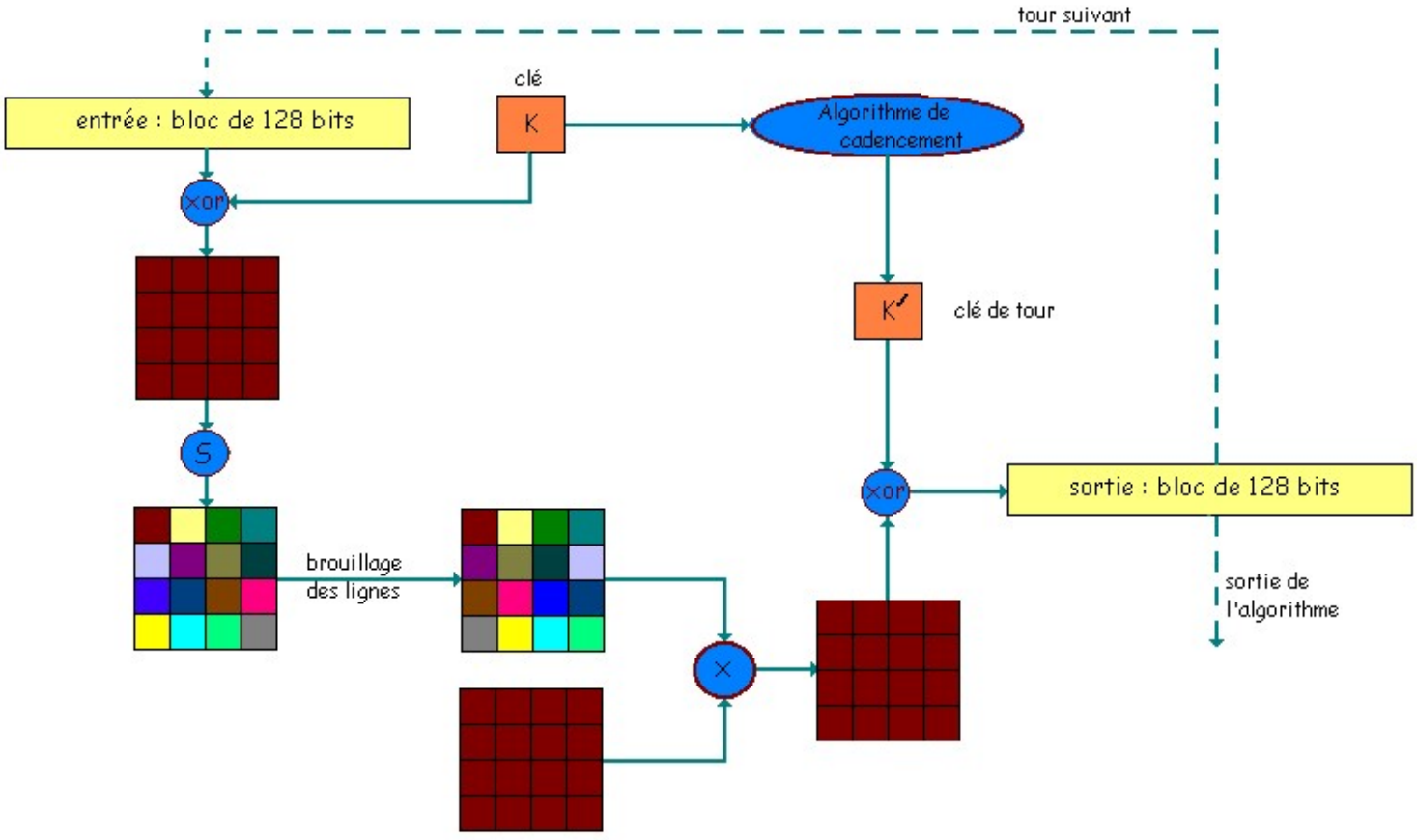
5 étapes :

1. Les 16 octets en entrée sont permutés selon une table définie au préalable.
2. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne.
3. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(2^8) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.
4. Finalement, un XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire.

Expliqué autrement :

1. Addition de la clé secrète (par un ou exclusif).
2. Transformation non linéaire d'octets : les 128 bits sont répartis en 16 blocs de 8 bits (8 bits=un octet), eux-même dispatchés dans un tableau 4×4. Chaque octet est transformé par une fonction non linéaire S. S peut être simplement vue comme une substitution sur les entiers compris entre 1 et 256. En particulier, elle peut être implantée sur ordinateur par un simple tableau.
3. Décalage de lignes : les 3 dernières lignes sont décalées cycliquement vers la gauche : la 2ème ligne est décalée d'une colonne, la 3ème ligne de 2 colonnes, et la 4ème ligne de 3 colonnes.
4. Brouillage des colonnes : Chaque colonne est transformée par combinaisons linéaires des différents éléments de la colonne (ce qui revient à multiplier la matrice 4×4 par une autre matrice 4×4). Les calculs sur les octets de 8 bits sont réalisés dans le corps à 2^8 éléments.
5. Addition de la clé de tour : A chaque tour, une clé de tour est générée à partir de la clé secrète par un sous-algorithme (dit de cadencement). Cette clé de tour est ajoutée par un ou exclusif au dernier bloc obtenu.

Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.



SOURCES :

https://www.boxcryptor.com/fr/encryption/
http://www.lemagit.fr/definition/AES-Advanced-Encryption-Standard
http://fracademic.com/dic.nsf/frwiki/1568194
http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/aes
http://www.bibmath.net/crypto/moderne/images/aes.gif
https://www.securiteinfo.com/cryptographie/aes.shtml

vidéo :
https://www.youtube.com/watch?v=2y_tidbY-Lw