Présentation générale de l'algorithme AES

L'AES (Advanced Encryption Standard) est, comme son nom l'indique, un standard de cryptage symétrique destiné à remplacer le DES (Data Encryption Standard) qui est devenu trop faible au regard des attaques actuelles.

Historiquement, le développement de l'AES a été instigué par le NIST (National Institue of Standards and Technology).

Il est également approuvé par la NSA (National Security Agency) pour l'encryption des informations dites très sensibles.

Cet algorithme suit les spécifications suivantes :

- L'AES est un standard, donc libre d'utilisation, sans restriction d'usage ni brevet.
- C'est un algorithme de type symétrique
- C'est un algorithme de chiffrement par blocs
- Il supporte différentes combinaisons [longueur de clé]-[longueur de bloc] : 128-128, 192-128 et 256-128 bits (en fait, l'AES supporte également des tailles de blocs variables, mais cela n'est pas retenu dans le standard)

En termes décimaux, ces différentes tailles possibles signifient concrètement que:

3.4 x 1038 clés de 128-bit possibles

6.2 x 1057 clés de 192-bit possibles

1.1 x 1077 clés de 256-bit possibles

Pour avoir un ordre d'idée, les clés DES ont une longueur de 56 bits (64 bits au total dont 8 pour les contrôles de parité), ce qui signifie qu'il y a approximativement 7.2 x 1016 clés différentes possibles.

Cela nous donne un ordre de 1021 fois plus de clés 128 bits pour l'AES que de clés 56 bits pour le DES. En supposant que l'on puisse construire une machine qui pourrait cracker une clé DES en une seconde (donc qui puisse calculer 255 clés par seconde), alors cela prendrait environ 149 mille milliards d'années pour cracker une clé AES.

Caractéristiques et points forts de l'AES

Le choix de cet algorithme répond à de nombreux critères plus généraux dont nous pouvons citer les suivants :

- Sécurité ou l'effort nécessaire pour une éventuelle cryptanalyse
- Puissance de calcul qui entraine une grande rapidité de traitement
- Besoins en ressources et mémoire très faibles
- Flexibilité d'implémentation, cela inclut une grande variété de plateformes et d'applications ainsi que des tailles de clés et de blocs supplémentaires
- Compatibilité hardware et software, il est possible d'implémenter l'AES aussi bien sous forme logicielle que matérielle
- Simplicité, le design de l'AES est relativement simple

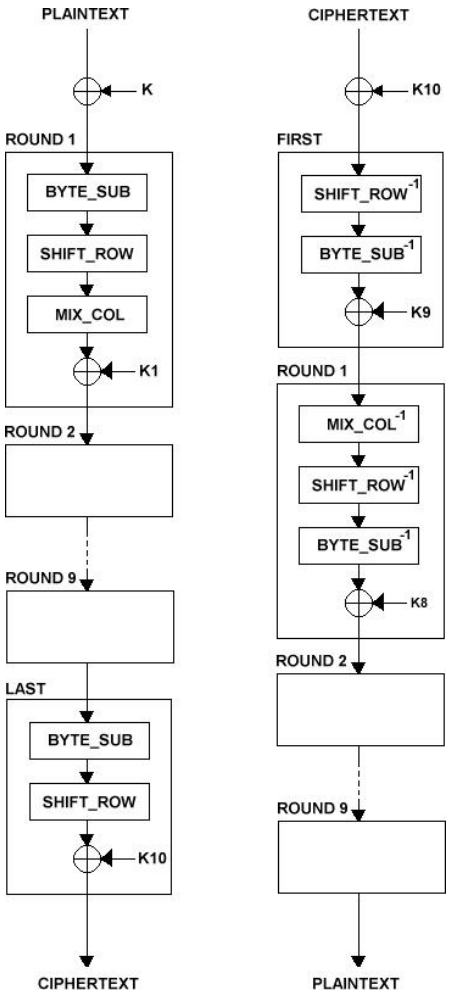
Si l'on se réfère à ces critères, on constate que l'AES est également un candidat particulièrement approprié pour les implémentations embarquées qui suivent des règles beaucoup plus strictes en matière de ressources, puissance de calcul, taille mémoire, etc...

C'est sans doute cela qui a poussé le monde de la 3G (3ème génération de mobiles) à adopter cet algorithme pour son schéma d'authentification.

Détails techniques

L'AES opère sur des blocs de 128 bits qu'il transforme en blocs cryptés de 128 bits par une séquence de N opérations ou « rounds », à partir d'une clé de 128, 192 ou 256 bits. Suivant la taille de celle-ci, le nombre de rounds diffère : respectivement 10, 12 et 14 rounds.

Le schéma suivant décrit succinctement le déroulement du chiffrement :



BYTE_SUB (Byte Substitution) est une fonction non-linéaire opérant indépendamment sur chaque bloc à partir d'une table dite de substitution.

SHIFT_ROW est une fonction opérant des décalages (typiquement elle prend l'entrée en 4 morceaux de 4 octets et opère des décalages vers la gauche de 0, 1, 2 et 3 octets pour les morceaux 1, 2, 3 et 4 respectivement).

MIX_COL est une fonction qui transforme chaque octet d'entrée en une combinaison linéaire d'octets d'entrée et qui peut être exprimée mathématiquement par un produit matriciel.

Le signe + entouré d'un cercle désigne l'opération de OU exclusif (XOR).

Kn est la n ème sous-clé calculée par un algorithme à partir de la clé principale K.

Le déchiffrement consiste à appliquer les opérations inverses, dans l'ordre inverse et avec des sous-clés également dans l'ordre inverse.

Attaques par dictionnaires

Nous allons comparer l'AES au 3DES qui est son concurrent le plus direct (le DES n'étant pratiquement plus utilisé dans sa forme simple). Le 3DES est, comme son nom l'indique, l'enchainement de 3 DES simples dans l'ordre DES, DES-1, DES. Il est évident à prime abord que chaque opération utilise une clé distincte, car sans cela les 2 premières s'annuleraient (DES, DES-1). Mais en pratique, on n'utilise que 2 clés différentes (que l'on alterne) car l'utilisation d'une troisième clé ne rajoute aucune sécurité.

En effet, l'attaque la plus courante contre le triple DES consiste à créer des dictionnaires multiples de façon à scinder le schéma en 2 parties et diminuer ainsi d'autant le nombre de possibilités à tester :

- La première partie conduit à l'élaboration d'un dictionnaire dont la taille est définie par le calcul suivant: le premier DES utilise une clé de 56 bits, il y a donc 256 cas possibles. C'est pareil pour le deuxième DES, sauf que qu'il faut le multiplier au premier cas, soit un total de 2112 possibilités.
- La seconde partie ne comporte qu'un seul DES, donc 256 possibilités pour la clé. Il suffit ensuite de faire correspondre ces 2 dictionnaires pour trouver la valeur qui est commune aux 2, nous donnant ainsi la bonne combinaison de clés.

En ce qui concerne l'AES, c'est un algorithme qui ne présente qu'une seule étape, donc le calcul est simple : comme cité précédemment, il y 2128 clés possibles (dans la version minimale où la clé ne fait "que" 128 bits de long). C'est directement la force de l'algorithme.

Attaques par cryptanalyse différentielle

L'attaquant choisit des textes clairs présentant une différence fixe, calcule les chiffrés (en ayant accès au système) et leurs différences puis assigne des probabilités à certains types de clés. Plus le nombre d'essais augmente, plus la probabilité de découvrir la bonne clé ne devient forte.

Dans le cas du DES simple, cette attaque nécessite 247 textes clairs et 247 chiffrements pour retrouver la clé. Néanmoins, les textes clairs doivent être soigneusement choisis.

L'AES est lui résistant à ce type d'attaque.

Attaques par cryptanalyse linéaire

L'attaquant utilise des approximations linéaires pour décrire les opérations conduisant au résultat chiffré. Comme précédemment, plus le nombre d'essais augmente, plus la probabilité de découvrir la bonne clé augmente.

Cette attaque est actuellement la plus performante puisqu'elle ne nécessite que 243 textes clairs et 243 chiffrements pour retrouver une clé DES (simple).

L'AES est lui résistant à ce type d'attaque.

Conclusion

En conclusion, l'AES est plus sûr que le 3DES car il présente, entre autres, une plus grande résistance aux attaques par dictionnaires de clés. Les autres attaques ne sont pas applicables dans son cas.

Schéma illustrant la création d'un trousseau de clés sécurisé :

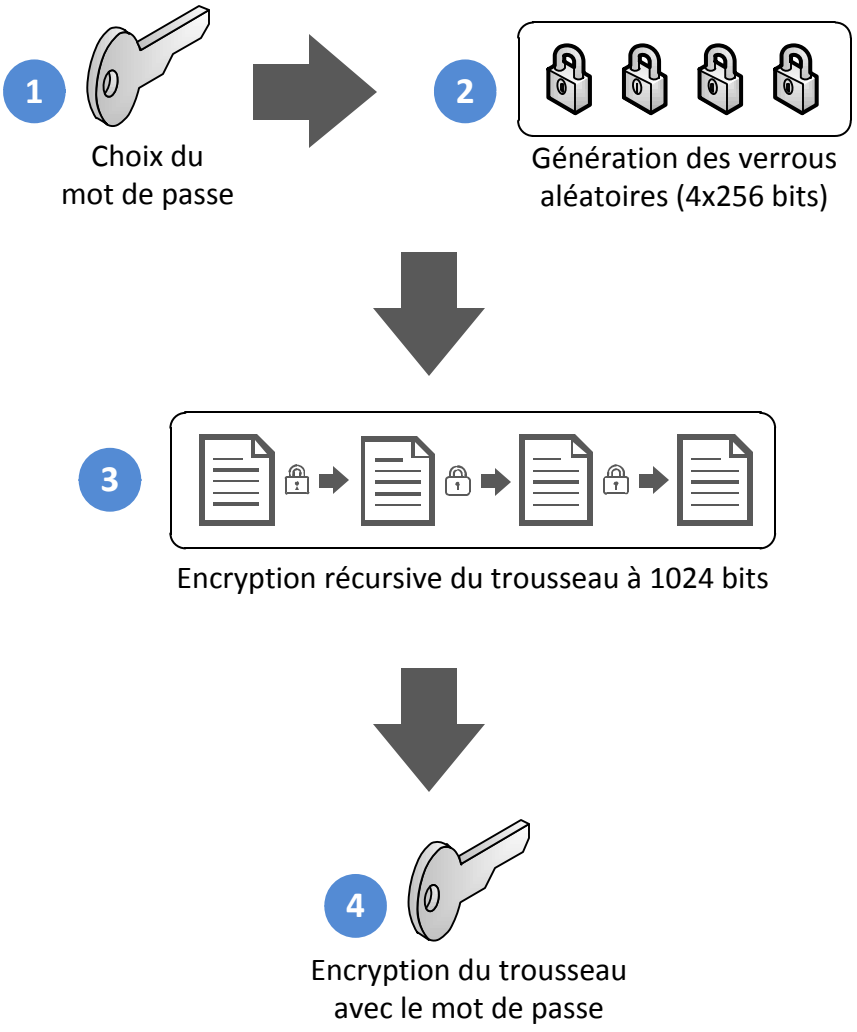
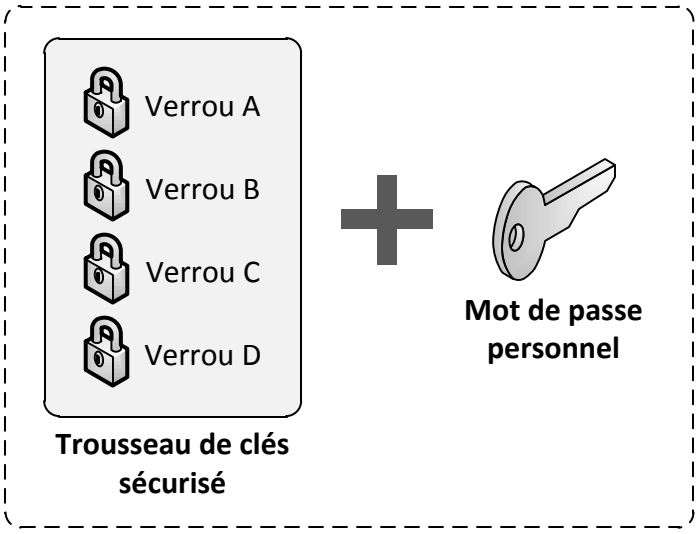
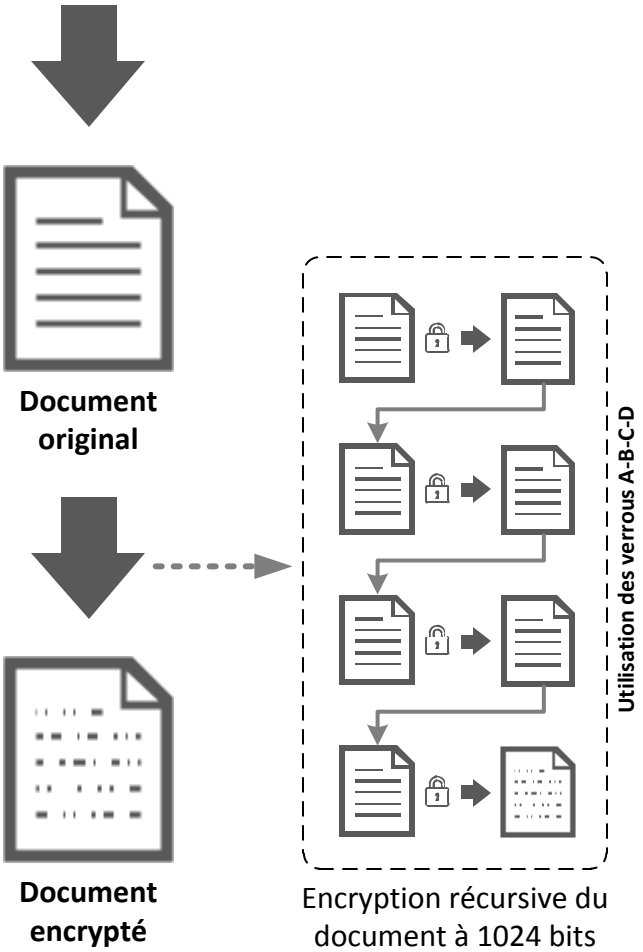


Schéma illustrant l'encryption d'un document à 1024 bits :



Mécanisme d'encryption
Le trousseau de clés est également encrypté
à 1024 bits et à l'aide du mot de passe



Encryption récursive du
document à 1024 bits