**FICHE D’EXECICES SUR AES**

Exercice 1 : Question de cours

1 – a) Définir les sigles DES et AES

b) Donner les limites du DES

2- a) Quel est le type de chiffrement utilise par ces deux algorithmes

b) Le définir et citer un autre type de chiffrement

3- a) donner 4 forces de l’AES.

b) Quelle faille peut contenir AES à votre avis ?

4- Donnez les noms des différentes fonctions utilisées lors de l’algorithme du chiffrement de l’AES et faire ensuite un schéma illustrant le chiffrement de celui-ci.

5 – Quelles sont les différentes tailles de clé que l’on peut avoir ?

Exercice 2 : CORPS DE L’AES

Représentation : les mots de 8 bits correspondent à des mots de deux chiffres hexadécimaux et à des polynômes de de degré ≤ 7.

Exemple : On identifie

Dans le Corps A.E.S, On travaille dans le quotient [X]/R(X) où R[X] est le polynôme de Rinjdael (irréductible sur ) défini par

1. Montrer que l’addition correspond au « ou exclusif » sur les mots binaires
2. Calculer la transformation sur un mot de huit bits correspondant à la multiplication par {00}, {01} et {02}
3. En déduire une méthode efficace pour multiplier deux éléments du corps AES
4. Calculer par cet algorithme, {2A} x {37}
5. Calculer {38} x {3F}

Exercice 3

1. Expliquer le principe du Shift Row et du AddRoundKey.
2. Soient les tableaux représentant respectivement le message en cours de chiffrement et la clé a un tour quelconque. Effectuez un ShiftRow puis un AddRoundKey.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 61 | 62 | 4c | 75 |  | 53 | 61 | 72 | 61 |
| 6c | 69 | 65 | 6c | 68 | 65 | 73 | 74 |
| 64 | 6e | 62 | 74 | 6d | 69 | 67 | 6e |
| 70 | 61 | 61 | 4c | 6f | 6e | 6e | 65 |

Exercice 4

Nous cherchons à déchiffrer par force brute un message chiffré par AES. Nous considérons ici que nous avons un registre quantique de 64 qubits.

1. Combien d'opérations faites avec un registre classique de 64 bits pourrions-nous paralléliser avec un tel registre quantique ?

2. Supposons que l'ordinateur utilisé (64 bits) soit capable de briser le chiffrement DES en un jour.

Lors d'un déchiffrement d'AES-128, estimer le temps moyen pour déchiffrer le message avec un registre classique de 64 bits.

3. Même question avec un registre quantique de 64 qubits.

4. Estimer le temps pris pour déchiffrer le message par un registre de n qubits.

5. Quelle valeur de n serait suffisante pour briser le chiffrement AES-128 en un jour ?

6. Conclure

**REPONSES AUX EXERCICES**

Exercice 1

1 - a) DES signifie Data Encryption Standard, et AES signifie Advanced Encryption Standard. Ce sont deux algorithmes de chiffrement symétrique, c’est-à-dire qu’ils utilisent la même clé pour chiffrer et déchiffrer les données.

b) Les limites du DES sont sa faible taille de clé (56 bits), qui le rend vulnérable à une attaque par force brute, et sa structure basée sur un schéma de Feistel, qui le rend sensible à certaines attaques cryptanalytiques.

2 - a) Ces deux algorithmes utilisent un type de chiffrement par blocs, c’est-à-dire qu’ils découpent les données en blocs de taille fixe (64 bits pour le DES, 128 bits pour l’AES) et les transforment en blocs chiffrés à l’aide d’une clé et d’une fonction de chiffrement.

b) Un autre type de chiffrement est le chiffrement par flots, qui traite les données bit par bit à l’aide d’un générateur de bits pseudo-aléatoires et d’une opération de combinaison (souvent un XOR) avec la clé.

3 - a) Quatre forces de l’AES sont :

- Sa sécurité, qui repose sur une grande taille de clé (jusqu’à 256 bits), un nombre élevé de tours (jusqu’à 14), et une résistance aux attaques connues.

- Sa rapidité, qui s’explique par sa simplicité, son efficacité et son adaptabilité à différentes plateformes (logicielles ou matérielles).

- Sa flexibilité, qui lui permet de supporter différentes tailles de clé et de bloc, et de s’adapter à différents modes opératoires selon les besoins.

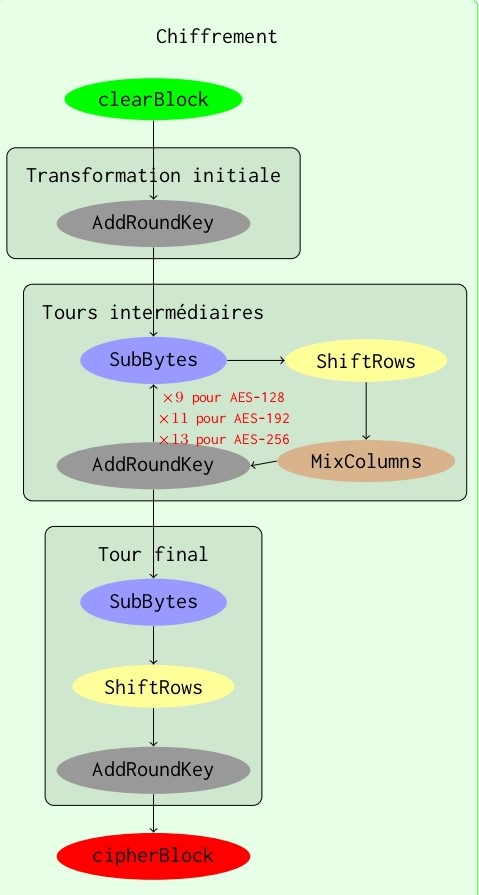
- Sa standardisation, qui le rend libre d’utilisation, sans restriction ni brevet, et qui facilite son interopérabilité et sa diffusion.

b) Une faille potentielle de l’AES pourrait sa mauvaise implémentation, car le code est assez sensible et ainsi, on aura un mauvais chiffrement du message.

4 - Les différentes fonctions utilisées lors de l’algorithme du chiffrement de l’AES sont :

* KeyGenerator : on génère toutes les clés à partir de la clé initiale
* AddRoundKey : on fait un XOR entre le bloc de données à chiffrer et la sous clé initiale du tour
* Sub-byte : remplacement de chaque bit du bloc de données à chiffrer par un autre bloc de bytes en utilisant la table S-Box
* ShiftRow : on décale circulairement vers la gauche les bytes de chaque ligne de la matrice qui représente le bloc de donnée. Le décalage varie selon le numéro de la ligne
* MixColumn : on fait une transition linéaire sur chaque colonne de la matrice en utilisant une multiplication matricielle dans un corps fini

**Schéma du chiffrement :**



5 - Les différentes tailles de clé qu’on peut avoir sont :

* 128 bits
* 192 bits
* 256 bits

Exercice 2 :

1. Montrons que l’addition correspond ou « ou exclusif » pour les mots binaires

Pour cela, faisons une table de vérité pour l’addition + et pour le ou exclusif XOR

* On sait que si a = b= 0, on a a+b = 0
* Si a et b sont différents on a a+b = 1
* Si a = b = 1 on a résultat a+b = 0 et retenue = 1.

On sait que XOR entre deux bits, retourne 0 si les deux bits sont identiques et 1 sinon

On a donc

|  |  |  |  |
| --- | --- | --- | --- |
| a | b | a+b | a XOR b |
| 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 |

1. Soit un mot A de huit bits, défini par A ={xy} = avec . Calculons la transformation sur un mot de huit bits, correspondant à la multiplication par :

* {00} : {00} correspondant au polynôme nul, la multiplication de A par {00} donne {00}
* {01} : ce mot correspond au polynôme 1, ainsi la multiplication de A par {01} donne toujours A
* {02} : ce mot correspond au polynôme X. On effectue donc la multiplication de A par X en faisant attention a ce que le degré du polynôme résultat ne dépasse pas 7. Si c’est le cas, on réduit le résultat a l’aide du polynôme irréductible de Galois défini par : en faisant une division euclidienne du résultat de la multiplication par le polynôme irréductible de Galois. Le résultat final est le reste de cette division

1. Déduisons une méthode efficace pour multiplier deux éléments du corps.

* On représente les éléments du corps comme des polynômes de degré inférieur ou égal à 7 à coefficients dans Z/2Z c’est-à-dire valent 0 ou 1.
* On effectue la multiplication des polynômes en utilisant les règles habituelles, mais en prenant les coefficients modulo 2. Donc lorsqu’on fait le regroupement et la réduction, on récupère le reste de la division euclidienne du coefficient par 2.
* Si le degré du polynôme résultant est supérieur a 7, on réduit le résultat modulo le polynôme irréductible , qui est utilisé pour définir le corps A.E.S. Pour cela, on effectue la division euclidienne du résultat par le polynôme irréductible et on prend le reste.
* On convertit le reste en notation hexadécimale pour obtenir l’élément du corps A.E.S. Par exemple.

1. Calculons {2A} x {37}

On a {2A} = 00101010 =

Et {37} = 00110111 =

On a donc Res = {2A} x {37}

=

On remarque que deg (Res) > 7, donc il faut réduire Res en faisant la division euclidienne de Res par le polynôme de Galois, et on récupère le reste

Ainsi on a :

Res =

Donc le résultat final est donné par le reste de cette division

D’où **{2A} x {37} =**

1. Calculons {38} x {3F}

On a {38} = 00111000 = et {3F} = 00111111 =

Res = . Comme deg (Res) > 7, on réduit Res a l’aide du polynôme de Galois, et on obtient :

Res =

Ainsi le résultat final est donné par le reste de cette division :

D’où **{38} x {3F} = = 10011111 = {9F**

Exercice 3

1. Principes de fonctionnement :

* Le Shift Row consiste à effectuer un décalage circulaire des bytes de chaque ligne du bloc à chiffrer, selon un offset variable. Par exemple, si le bloc est de 128 bits, il est divisé en 4 lignes de 4 bytes chacune. La première ligne n’est pas décalée, la deuxième ligne est décalée d’une byte vers la gauche, la troisième ligne est décalée de deux bytes vers la gauche, et la quatrième ligne est décalée de trois bytes vers la gauche
* Le AddRoundKey consiste à ajouter par ou exclusif (XOR) le bloc à chiffrer avec une sous-clé, qui est dérivée de la clé principale par une fonction de génération de clés. Il y a une sous-clé différente pour chaque tour de l’algorithme, et le nombre de tours dépend de la taille de la clé principale

1. Effectuons un ShiftRow ensuite un AddRoundKey

ShiftRow

|  |  |  |  |
| --- | --- | --- | --- |
| 61 | 62 | 4c | 75 |
| 69 | 65 | 6c | 6c |
| 62 | 74 | 64 | 6e |
| 4c | 70 | 61 | 61 |

AddRoundKey

|  |  |  |  |
| --- | --- | --- | --- |
| 32 | 03 | 3E | 14 |
| 01 | 00 | 1F | 18 |
| 0F | 1D | 03 | 00 |
| 23 | 1F | 0E | 04 |

Pour faire XOR, on rentre d’abord en binaire, et ensuite reconvertit le résultat en hexadécimal. Pour la case (1,1), on a :

61 XOR 53= 01100001 XOR 01010011

Donc 0 1 1 0 0 0 0 1

^ 0 1 0 1 0 0 1 1

0 0 1 1 0 0 1 0 = 32

62 XOR 61 = 01100010 XOR 01100001

Donc 0 1 1 0 0 0 1 0

^ 0 1 1 0 0 0 0 1

0 0 0 0 0 0 1 1 = 03 et on fait de même pour les autres cases du tableau

Exercice 4

1. On peut paralléliser 2⁶⁴ opérations

2. Le DES utilise des clés de 54 bits. L’AES-128 bits utilise des clés de 128 bits. On suppose donc que l'ordinateur puisse faire 2⁵⁴ en un jour.

Pour déchiffrer un message chiffré par AES-128 bits, il faut pouvoir tester les 2¹²⁸ clés. Cet ordinateur le ferait donc en t = 2¹²⁸ / 2⁵⁴ = 2⁷⁴ jours.

3. Avec un registre quantique de 64 bits, on ferait ces opérations 2⁶⁴ fois plus vite. Donc, l'ordinateur le ferait en 2⁷⁴ / 2⁶⁴ = 2¹⁰ = 1024 jours. Soit plus de 2 ans.

4. Pour déchiffrer un message avec un registre de n qubits, il faudrait 2¹²⁸ / (2⁵⁴ \* 2^n) =

2^ (74 - n)

5. Pour le faire en un jour, il faudrait que 2^ (74 - n) = 1. Donc n = 74 qubits.

6. Cela serait très difficile avec les technologies actuelles car, les ordinateurs quantiques les plus performants aujourd'hui n'atteignent pas ce standard de 74 bits. De plus, notre hypothèse de départ est de pouvoir briser le chiffrement DES en un jour ce qui n'est pas évident.