**Final SR50**

**UTBM-Automne 2017**

rana.abdallah@utbm.fr

**Exercice 1**

Considérons un pare-feu dont le filtrage est fondé sur les paquets SYN.

On souhaite que l’échange de fichiers via FTP ( 192.168.2.1) sur le réseau interne puisse recevoir et envoyer des fichiers de et vers Internet. Ecrire les règles de filtrage du pare-feu dans le tableau suivant.



**Exercice 2**

Voici un message non chiffré de 128 bits :

|  |  |  |  |
| --- | --- | --- | --- |
| BD | 27 | 51 | 96 |
| 94 | EE | 3F | 08 |
| 77 | D6 | 32 | 64 |
| 8C | 89 | 17 | FB |

Utiliser le chiffrement AES pour chiffrer ce message en citant les différentes étapes.

La clé utilisée pour ce chiffrement est : *K = 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C.*

**Annexe**

****

 S-Box

La matrice utilisée dans l’étape MixColumns est :

|  |  |  |  |
| --- | --- | --- | --- |
| 02 | 03 | 01 | 01 |
| 01 | 02 | 03 | 01 |
| 01 | 01 | 02 | 03 |
| 03 | 01 | 01 | 02 |

Pour la partie MixColumns, remplir le vide dans le tableau :

|  |  |  |  |
| --- | --- | --- | --- |
| A0 | 3B |  | 5B |
| 40 | 9A | 12 |  |
| 05 | 93 |  | CE |
|  | B1 | F8 | 84 |

Le message chiffré obtenu est:

|  |  |  |  |
| --- | --- | --- | --- |
| 8B | 45 | AE |  |
| 68 | 34 |  | 83 |
| AE |  | F7 | 46 |
|  | 7E | B7 | B8 |

 Bonne Chance