Cryptographie AES et les portes XOR

Le « Advanced Encryption Standard » est un processus de standardisation lancé en 1997 pour demander aux cryptologues de concevoir un nouvel algorithme de chiffrement par bloc destiné au gouvernement des États-Unis. Le but était de remplacer le Data Encryption Standard (DES). Ce dernier étant vulnérable à un grand nombre d'attaques et utilisant une clé de seulement 56 bits, la sécurité n'était plus garantie puisqu'une recherche exhaustive des clés était désormais envisageable.

La cryptographie XOR seule n'est pas suffisante pour sécuriser des communications (même si elle est bien plus difficile à déchiffrer qu'un chiffrement Vigenere). Le XOR est donc une étape, dans le processus de cryptographie AES.

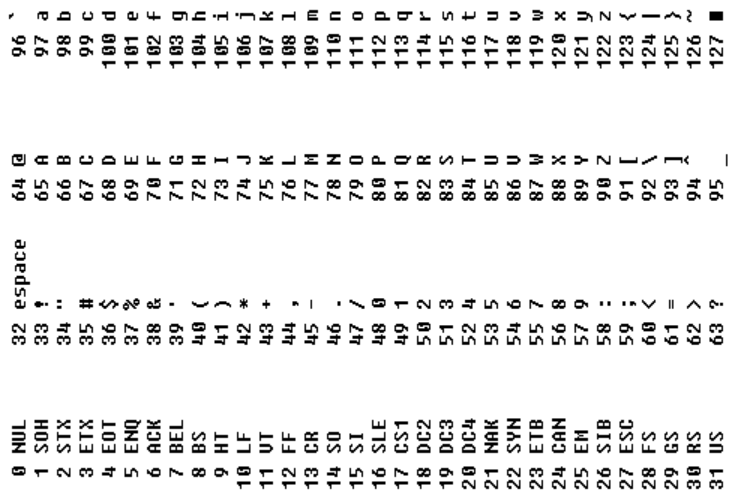
I. Appliquer un XOR sur une chaine de caractère :

La première étape de la cryptographie AES consiste à appliquer sur le message, converti en bianire, une porte logique XOR. Nous utiliserons pour chaque lettre la même clé pour simplifier. Le message crypté est appelé « Cipher »

Texte	N	S	I	F	O	R	E	V	E	R
ASCII										
Binaire										
Clé	01010010	01010010	01010010	01010010	01010010	01010010	01010010	01010010	01010010	01010010
Cipher										

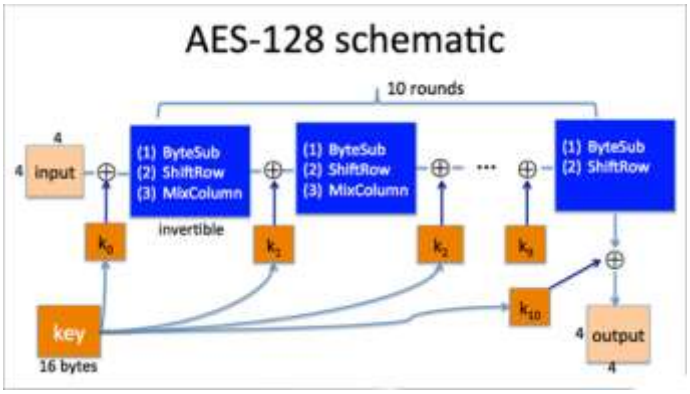
II. Décrypter une chaine binaire de 3 caractères avec XOR :

Cipher	00000001	00100111	00111100
Clé	01010010	01010010	01010010
Binaire			
ASCII / lettre			



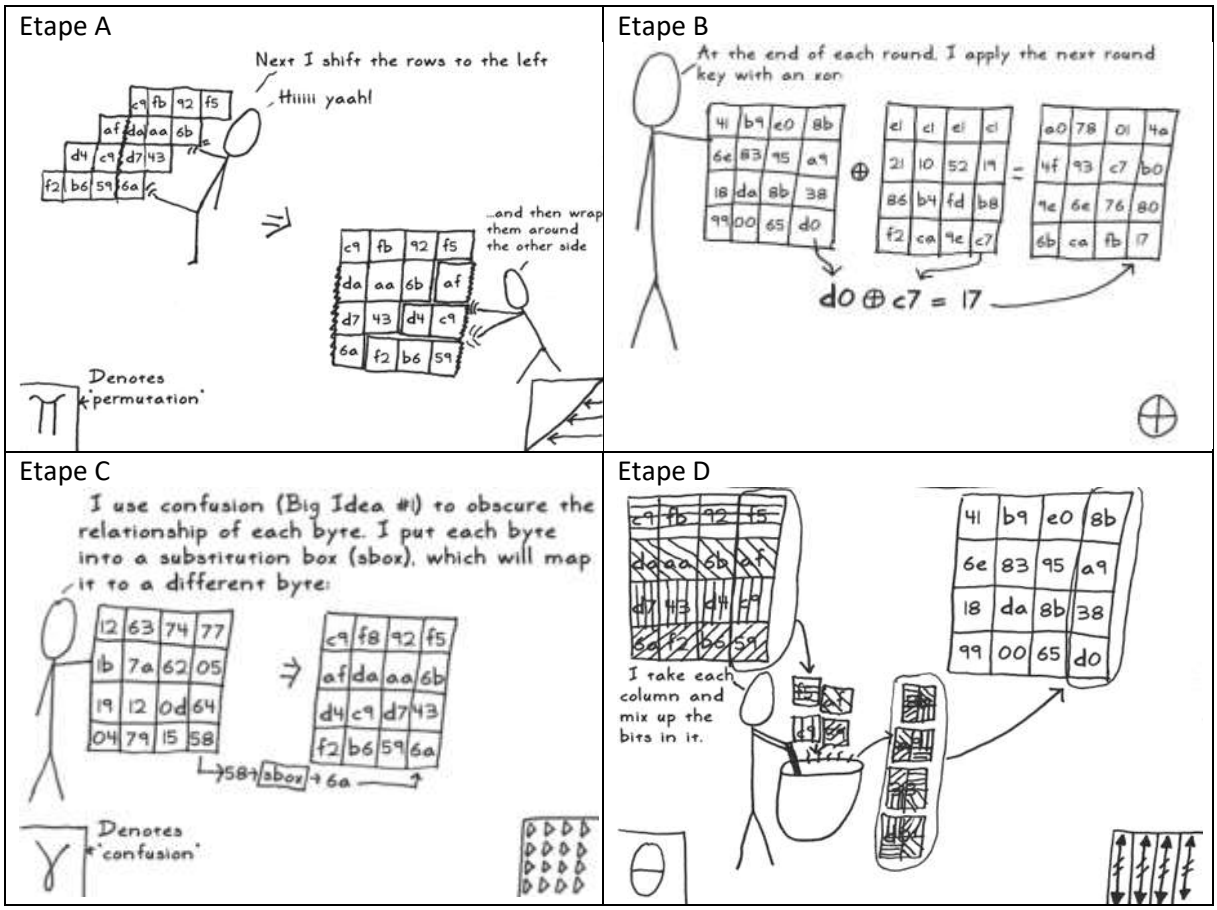
III. Les étapes suivantes :

On découpe la chaine obtenue au I. en plaçant chaque chiffre dans un tableau 4x4. Le + entouré par un cercle symbolise la porte XOR dans le schéma suivant :



Note : dans les vidéos et les illustrations suivantes, nous allons manipuler, non pas des nombres binaires, ***mais des nombres hexadécimaux****, dans le seul but d'être plus concis.*

1. En regardant la vidéo 2 proposée et l'illustration ci-dessus, nommez et remettre dans l'ordre les 4 opérations suivantes représentées sous forme de BD.
2. Combien de fois exécute-t-on ces étapes ?



3. A quel moment utilise-t-on des portes XOR ?

4. Décrire en des termes simples ce qui se passe dans l'étape A ?

5. Décrire en des termes simples ce qui se passe dans l'étape B ?

6. Dans cette étape B, on voit $d0 \oplus c7 = 17$. Prouvez que cette relation est vraie en passant par une notation binaire et en effectuant une porte logique XOR.

7. Décrire en des termes simples ce qui se passe dans l'étape C ?

8. Décrire en des termes simples ce qui se passe dans l'étape D ?

9. Quel est l'objectif recherché de toutes ces étapes ?