

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 chaîne de caractère :

La première étape de la cryptographie AES consiste à appliquer sur le message, converti en binaire, 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										

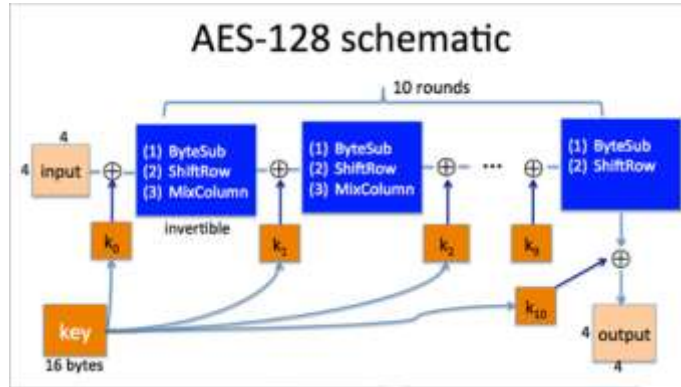
II. Décrypter une chaîne binaire de 3 caractères avec XOR :

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

96	97	a	98	b	99	c	100	d	101	e	102	f	103	g	104	h	105	i	106	j	107	k	108	l	109	m	110	n	111	o	112	p	113	q	114	r	115	s	116	t	117	u	118	v	119	w	120	x	121	y	122	z	123	{	124		125	}	126	~	127	■	
64	@	65	A	66	B	67	C	68	D	69	E	70	F	71	G	72	H	73	I	74	J	75	K	76	L	77	M	78	N	79	O	80	P	81	Q	82	R	83	S	84	T	85	U	86	V	87	W	88	X	89	Y	90	Z	91	[92	\	93]	94	^	95	_
32	espace	33	?	34	"	35	#	36	\$	37	%	38	&	39	.	40	(41)	42	*	43	+	44	,	45	-	46	.	47	/	48	0	49	1	50	2	51	3	52	4	53	5	54	6	55	7	56	8	57	9	58	:	59	;	60	<	61	=	62	>	63	?
0	NUL	1	SOH	2	STX	3	ETX	4	EOT	5	ENQ	6	ACK	7	BEL	8	BS	9	HT	10	LF	11	VT	12	FF	13	CR	14	SO	15	SI	16	SLE	17	CSI	18	DC2	19	DC3	20	DC4	21	NAK	22	SYN	23	ETB	24	CAN	25	EM	26	STB	27	ESC	28	FS	29	GS	30	RS	31	US

III. Les étapes suivantes :

On découpe la chaîne 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 ?

Etape A

Next I shift the rows to the left
Hiiii yaahl

c9	fb	92	f5
af	da	aa	6b
d4	c9	d7	43
f2	b6	59	6a

...and then wrap them around the other side

c9	fb	92	f5
da	aa	6b	af
d7	43	d4	c9
6a	f2	b6	59

Denotes 'permutation'

Etape B

At the end of each round, I apply the next round key with an xor

41	b9	e0	8b
6e	83	95	a9
18	da	8b	38
99	00	65	d0

$d0 \oplus c7 = 17$

e1	c1	e1	c1
21	10	52	19
86	b4	fd	b8
f2	ca	9e	c7

$a0$ 78 01 4a
4f 93 c7 b0
9e 6e 76 80
6b ca fb 17

Denotes XOR

Etape C

I use confusion (Big Idea #1) to obscure the relationship of each byte. I put each byte into a substitution box (sbox), which will map it to a different byte:

12	63	74	77
1b	7a	62	05
19	12	0d	64
04	79	15	58

$58 \rightarrow \text{sbox} \rightarrow 6a$

c9	fb	92	f5
af	da	aa	6b
d4	c9	d7	43
f2	b6	59	6a

Denotes 'confusion'

Etape D

I take each column and mix up the bits in it.

c9	fb	92	f5
da	aa	6b	af
d7	43	d4	c9
6a	f2	b6	59

41	b9	e0	8b
6e	83	95	a9
18	da	8b	38
99	00	65	d0

Denotes ShiftRow

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 ?