AES Encryption

The AES contains of 4 main functions:

قبل ما نتعرف على الـ functions لازم نعرف ان بالبداية بنحول block الى (Matrix) state حيث ان البلوك عبارة عن **text** كل عنصر فيها يحتوي على **8 bits** ، فلما نحولها لمصفوفة نقدر بعدها نستخدم الـ 4 functions الأساسية.

1. AddRoundKey():

لمّا نستخدم Add round key معناها حجم الـ **key** مساوي لحجم الـ state معناها بنعمل لها **XOR** بعد ما احول العناصر فيها من **hexadecimal** الى**Binary**

فـ AddRoundKey () بالتفصيل معناها اجيب الـ Key اللي بعطيك هو و تعملي عملية الـ **XOR** مع اول عنصر في المصفوفة.

Example:

Text	A	E	S	U	S	E	S	A	M	A	T	R	I	X	Z	Z
Hexadecimal	00	04	12	14	12	04	12	00	0C	00	13	11	08	23	19	19

$$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix}$$ State

key بيكون نفس حجم المسج المطلوب ، في حال كان الـ key بـ hexa بحوله للباينري و ابدا اشفره مع كل عنصر بالمصفوفة ، و بعد ما اخلص تشفير احول من باينري الى هيكسا و تطلع لي مسج مختلفة بعد التشفير.

Good Luck ☺

2. **Substitute bytes:**

يشبه S-box ، بمسك كل عنصر و بشوف تقاطعهم بالجدول زي مثلا **00**
تقاطعها بالجدول **63** و استبدلها بالقيمة الجديدة، نشوف العنصر الثاني **12** اشوف الجدول و
اشوف القيمة كم طلعت لي؟**C9** و هكذا

	0	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
40	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Good Luck ☺

3. Shift rows:

هي عملية للإزاحة بعض العناصر بِآلية معينة كالتالي:

القيم تتكون من اربع صفوف و أعمدة، الاستراتيجية المُتعبة هي:

١/ اول صف ثابت ما يتغير.

٢/ ثاني صف نُزيح اول عنصر و نضيفه باخر الصف.

٣/ ثالث صف نُزيح اول عنصرين و نعمل عليهم عملية الازاحة.

٤/ الصف الاخير نُزيح الثلاث عناصر و العنصر الأخير في المقدمة.

Example:

Input

F0	89	9B	BB
J4	C9	A2	Q8
78	8B	56	E4
32	C8	AC	DF

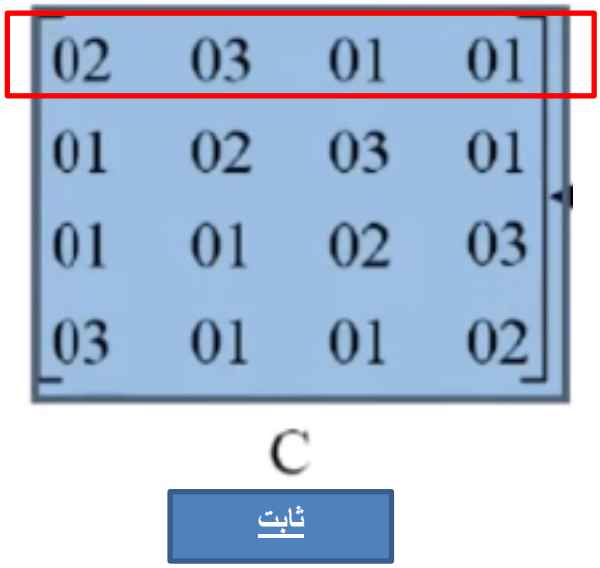
Output

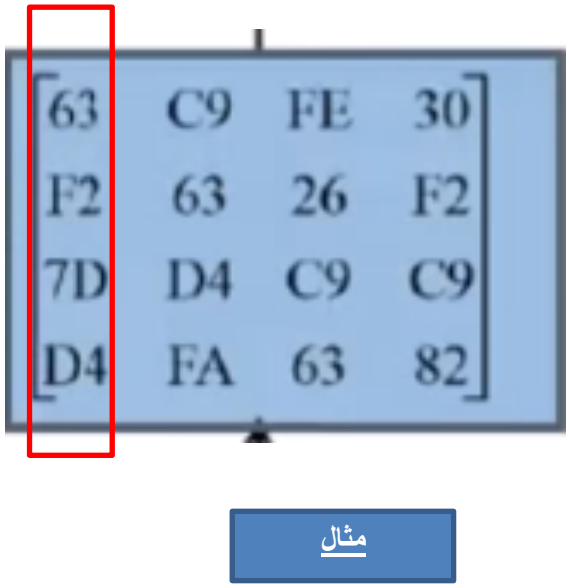
F0	**89**	**9B**	**BB**
C9	A2	Q8	**J4**
56	E4	**78**	**8B**
DF	**32**	**C8**	**AC**

Good Luck ☺

4. Mix Columns:

عبارة عن مصفوفة ثابتة تقريبا و نضربها بمصفوفة أخرى.
هذا الجدول ثابت بصير انا اعطيك مصفوفة ثانية تضربين الصف في الجدول الثابت بالعامود من المصفوفة اللي انا بعطيك هي و هكذا.





اخذ الصف الاول و **نضربه** بالعامود الاول:

63 * 02 + F2 * 03 + 7D* 01 + D4 * 01

* طبعا بحولهم للـ Binary لانهم Hexadecimal

ببدأ اقسم ، بأخذ **63 * 02**

63 = 01100011
01100011

ايش بنسوي؟
بشوف انا ضربتها ب 02
فبحذف اخر خانة اللي هي صفر و اضيف صفر اخر خانة
بتصير كذا

11000110

طيب نبغا نشوف في حال كانت اول خانة 1؟ نشوف و نكمل

11000110 + F2 * 03 + 7D* 01 + D4 * 01

F2*03 نقسمها لقسمين

(F2 * 02 + F2 * 01)

{
F2= 11110010
ولسه فيه خطوة زيادة بحيث انو 11100100 نسوي
XOR with 1B
1B= 00011011
11100100 XOR
00011011
————--
11111111
}

{
11110010
لانها مضروبة بـ 01
فالقيم تبقى زي ماهي
}

بعمل لهم XOR

11111111 =(F2*02)
11110010 =(F2*01)
————————
00001101 =final result

Good Luck ☺

11000110 + 00001101 + 7D* 01 + D4 * 01
11000110 + 00001101 + 01111101 + 11010100

عملية الجمع اللي بينهم هي عملية XOR اصلا
فبسوي العملية بينهم بالترتيب

11000110 + 00001101 + 01111101 + 11010100

01111101
11010100

10101001

11000110 + 00001101 + 10101001

00001101
10101001

10100100

11000110 + 10100100

10100100
11000110

01100010

final result = 01100010

و بعد ما نحولها لـ decimal يطلع **62** ، و هكذا نكمل باقي على العناصر.

Good Luck ☺