جامعة المنارة
كلية الهندسة
قسم المعلوماتية

Information System Security
أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

الجلسة الخامسة

MU-EPP-FM-005 Issue date 17November2025 issue no:1 https://manara.edu.sy

المسألة الأولى

بفرض لدينا خوارزمية AES إذا علمت أن النص الصريح هو **be good all time**

وأن الخوارزمية تستخدم المفتاح **how are you?123** المطلوب:

١.احسب قيم التهيئة لهذه الخوارزمية

٢. نفذ الجولة الأولية

المحرف	أسكي
b	1100010
e	1100101
space	0100000
g	1100111
o	1101111
d	1100100
a	1100001
i	1101001
t	1110100
m	1101101
l	1101100

الحل:١.حساب قيم التهيئة لهذه الخوارزمية

تهيئة النص الصريح:

١. المدخلات من جدول الأسكي :

استخدام جدول الأسكي

	000	001	010	011	100	101	110	111
0000	NULL	DLE		0	@	P		p
0001	SOH	DC1	!	1	A	Q	a	q
0010	STX	DC2	"	2	B	R	b	r
0011	ETX	DC3	#	3	C	S	c	s
0100	EDT	DC4	$	4	D	T	d	t
0101	ENQ	NAK	%	5	E	U	e	u
0110	ACK	SYN	&	6	F	V	f	v
0111	BEL	ETB	'	7	G	W	g	w
1000	BS	CAN	(	8	H	X	h	x
1001	HT	EM	)	9	I	Y	i	y
1010	LF	SUB	*	:	J	Z	j	z
1011	VT	ESC	+	;	K	[	k	{
1100	FF	FS	,	<	L	\	l	|
1101	CR	GS	-	=	M	]	m	}
1110	SO	RS	.	>	N	^	n	~
1111	SI	US	/	?	O		o	DEL

٢. كتابة النص الصريح بالست عشري (hex)

b	e		g	o	o	d		a	l	l		t	i	m	e
62	65	20	67	6f	6f	64	20	61	6c	6c	20	74	69	6d	65

٣. نكتب قيم النص الصريح على شكل مصفوفة 4x4

State=	62	6f	61	74
	65	6f	6c	69
	20	64	6c	6d
	67	20	20	65

تهيئة مفتاح الدخل:

١. المدخلات من جدول الأسكي :

المحرف	أسكي
h	1101000
o	1101111
space	0100000
w	1110111
a	1100001
y	1111001
a	1100001
?	011111
1	0110001
2	0110010
3	0110011
r	1110010

٢. كتابة المفتاح بالست عشري (hex)

h	o	w		a	r	e		y	o	u	?		1	2	9
68	6f	77	20	61	72	65	20	79	6f	75	3f	20	31	32	33

استخدام جدول الأسكي

	000	001	010	011	100	101	110	111
0000	NULL	DLE		0	@	P		p
0001	SOH	DC1	!	1	A	Q	a	q
0010	STX	DC2	"	2	B	R	b	r
0011	ETX	DC3	#	3	C	S	c	s
0100	EDT	DC4	$	4	D	T	d	t
0101	ENQ	NAK	%	5	E	U	e	u
0110	ACK	SYN	&	6	F	V	f	v
0111	BEL	ETB	'	7	G	W	g	w
1000	BS	CAN	(	8	H	X	h	x
1001	HT	EM	)	9	I	Y	i	y
1010	LF	SUB	*	:	J	Z	j	z
1011	VT	ESC	+	;	K	[	k	{
1100	FF	FS	,	<	L	\	l	|
1101	CR	GS	-	=	M	]	m	}
1110	SO	RS	.	>	N	^	n	~
1111	SI	US	/	?	O	_	o	DEL

٣. نكتب قيم المفتاح على شكل مصفوفة 4x4

K=

68	61	79	20
6F	72	6F	31
77	65	75	32
20	20	3F	33

2. تنفيذ الجولة الأولية:

إضافة المفتاح الأولي:

addRoundKey=State $\oplus$ K =$State$

62	6f	61	74
65	6f	6c	69
20	64	6c	6d
67	20	20	65

$\oplus$

68	61	79	20
6F	72	6F	31
77	65	75	32
20	20	3F	33

=

STATE=				
	0a	0e	18	54
	0a	1d	03	58
	57	01	19	5f
	47	00	1f	56

المسألة الثانية

بفرض أن الـ State الناتجة عن الجولة الأولية هي :

STATE=	0a	0e	18	54
	0a	1d	03	58
	57	01	19	5f
	47	00	1f	56

اكتب الحالة الناتجة عن خطوة الاستبدال في الجولة الأولى.

الحل:

1.استبدال (Subbyte) : باستخدام جدول S-BOX :

STATE=	67	ab	ad	20
	67	4a	7b	6a
	5b	7c	d4	cf
	a0	63	c0	b1

المسألة الثالثة

بفرض أن قيم العمود الأول في الحالة State الناتجة عن تطبيق الإزاحة هي :

63
53
24
12

احسب قيمة البايت الأول b0 في العمود الأول من مصفوفة المزج.

الحل:

❖ تكون قيمة البايت الأول في العمود الجديد هي: $b_0 = (63.02) \oplus (53.03) \oplus (24.01) \oplus (12.01)$

✓ حساب (63.02) :

❖ نحول قيمة 63 من ست عشري إلى ثنائي فتكون 01100011
❖ نطبق الإزاحة نحو اليسار 11000110 MSB=0 نأخذ الناتج الأول كما هو
❖ نحول 11000110 إلى ست عشري : C6

✓ **حساب** (53.03) :

$$(53.03) = (53.02) \oplus 53$$

❖ نحول قيمة 53 من ست عشري إلى ثنائي فتكون 01010011

❖ نطبق الإزاحة نحو اليسار 10100110 MSB=0 نأخذ الناتج الأول كما هو

❖ نطبق XOR: 10100110 ⊕ 01010011=11110101=f5

$$(53.03) = f5$$

✓ حساب(24.01) : $(24.01) = 24$

✓ حساب(12.01) : $(12.01) = 12$

$$b_0 = C6 \oplus F5 \oplus 24 \oplus 12 \Rightarrow b_0 = 05$$

المسألة الرابعة

لنفترض أن مفتاح الجولة الأولى هو: a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05

وبفرض أن مصفوفة state بعد مزج الأعمدة هي كالآتي:

12	8a	B4	21
89	fe	3d	92
a1	23	55	77
f3	19	82	1c

الحل

1-نرتب المفتاح في مصفوفة 4x4

a0	fa	fe	17
88	54	2c	b1
23	a3	39	39
2a	6c	76	05

2. نطبق XOR بين كل بايت من State وكل بايت مقابل له من مفتاح الجولة State $\oplus$ RoundKey[1]=$State$

بعد تطبيق AddRoundKeyعلى جميع البايتات، نحصل على Stateالنهائية للجولة الأولى، والتي تصبح مدخلاً للجولة الثانية.

12	8a	B4	21
89	fe	3d	92
a1	23	55	77
f3	19	82	1c

$\oplus$

a0	fa	fe	17
88	54	2c	b1
23	a3	39	39
2a	6c	76	05

=

b2	70	4a	26
01	aa	11	23
82	80	6c	4c
d9	75	f4	19

المسألة الخامسة

في خوارزمية AES بفرض مفتاح التشفيرهو: 33 32 31 20 3f 75 6f 78 20 65 72 61 20 77 6f 68

احسب مفتاح الجولة الأولية (الجولة 0) ومفتاح الجولة الأولى (الجولة 1)

الحل: ١. يقسم مفتاح التشفير إلى أربع كلمات:

W[0]=68 6f 77 20
W[1]=61 72 65 20
W[2]=78 6f 75 3f
W[3]= 20 31 32 33

ملاحظة: كل أربعة بايت تمثل كلمة وكل مفتاح يمثل 4 كلمات

- **المفتاح الجولة 0 :** W[0] W[1] W[2] W[3]

لدينا قيم الكلمات التي تكون المفتاح : RoundKey(0)=68 6f 77 20 61 72 65 20 78 6f 75 3f 20 31 32 33

➢ **المفتاح الجولة 1 :** W[4] W[5] W[6] W[7] هذه الكلمات غير معلومة . يجب حسابها

حساب الكلمة w[4]:

١. ندور الكلمة W[3]= 20 31 32 33 : RotWord (W[3])= 31 32 33 20

٢. ننفذ الاستبدال: SubWord (RotWord (W[3]))=c7 23 c3 b7

٣. ننفذ XOR مع ثابت الجولة (يؤخذ من الجدول)

SubWord (RotWord (W[3])) XOR Rco(1)=c7 23 c3 b7 XOR 01 00 00 00 =C6 23 C3 B7

٤. ننفذ XOR مع الكلمة السابقة لها بأربع مواقع w[i-4=4-4=0]:

(SubWord (RotWord (W[3])) XOR Rco(1)) XOR W[0]= c6 23 c3 b7 XOR 68 6F 77 20

فتكون الكلمة: W[4]= ae 4c b4 97

جدول S-BOX تنفيذ SubWord

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

حساب الكلمة w[5]: 5 ليست من مضاعفات العدد 4 نطبق الآتي: W[i]=W[i-4] XOR W[i-1]

W[5]=W[1] XOR W[4]= 61 72 65 20 XOR ae 4c b4 97

W[5]=cf 3e d1 b7

حساب الكلمة w[6]: 6 ليس من مضاعفات العدد 4

W[6]=W[2] XOR W[5]= 78 6f 75 3f XOR cf 3e d1 b7

W[6]= b7 51 a4 88

حساب الكلمة w[7]: 7 ليست من مضاعفات العدد 4

W[7]=W[3] XOR W[6]= 20 31 32 33 XOR b7 51 a4 88

W[7]=97 60 96 bb

أصبح لدينا الآتي:

W[0]=68 6f 77 20
W[1]=61 72 65 20
W[2]=78 6f 75 3f
W[3]= 20 31 32 33
W[4]= ae 4c b4 97
W[5]=cf 3e d1 b7
W[6]= b7 51 a4 88
W[7]=97 60 96 bb

✓ فيكون مفتاح الجولة 1:

RoundKey (1)=W[4] W[5] W[6] W[7] = ae 4c b4 97 cf 3e d1 b7 b7 51 a4 88 97 60 96 bb

نهاية الجلسة الخامسة

جميع الجداول الملحقة بهذه المحاضرة يجب اصطحابها إلى الامتحان

جدول الأسكي

	000	001	010	011	100	101	110	111
0000	NULL	DLE		0	@	P	`	p
0001	SOH	DC1	!	1	A	Q	a	q
0010	STX	DC2	"	2	B	R	b	r
0011	ETX	DC3	#	3	C	S	c	s
0100	EDT	DC4	$	4	D	T	d	t
0101	ENQ	NAK	%	5	E	U	e	u
0110	ACK	SYN	&	6	F	V	f	v
0111	BEL	ETB	'	7	G	W	g	w
1000	BS	CAN	(	8	H	X	h	x
1001	HT	EM	)	9	I	Y	i	y
1010	LF	SUB	*	:	J	Z	j	z
1011	VT	ESC	+	;	K	[	k	{
1100	FF	FS	,	<	L	\	l	|
1101	CR	GS	-	=	M	]	m	}
1110	SO	RS	.	>	N	^	n	~
1111	SI	US	/	?	O	_	o	DEL

جدول S-box

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

مصفوفة mix-columns الثابتة

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

رقم الجولة	ثابت الجولة Rcon
1	01 00 00 00
2	02 00 00 00
3	04 00 00 00
4	08 00 00 00
5	10 00 00 00
6	20 00 00 00
7	40 00 00 00
8	80 00 00 00
9	1b 00 00 00
10	36 00 00 00