جامعة المنارة
كلية الهندسة
قسم المعلوماتية

Information System Security
أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

عناوين المحاضرة الخامسة

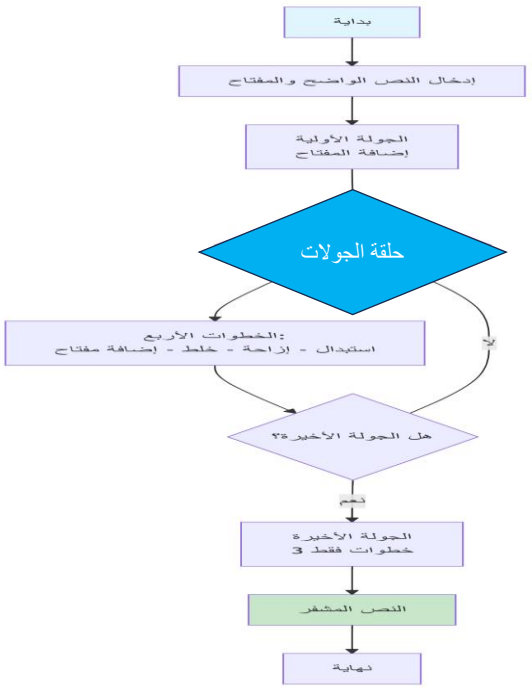
- خوارزمية AES (Advanced Encryption Standard)
- تعريف بالخوارزمية
- المخطط الصندوقي للخوارزمية
- خطوات تنفيذ الجولة
- خطوات خوارزمية توسيع المفتاح Key Expansion

جميع الجداول الملحقة بهذه المحاضرة يجب اصطحابها إلى الامتحان

تعريف بخوارزمية معيار التشفير المتقدم(AES)

- خوارزمية AES هي خوارزمية تشفير كتلي **متناظر**
- **اختيرت** من قبل المعهد الوطني للمعايير والتقنية ((NIST) الأمريكي في عام 2001 لتحل محل خوارزمية DES
- دخل خوارزمية AES هو كتلة **طولها 128 bits**، وتستخدم مفاتيح بأطوال مختلفة:
  - ✓ AES-128: مفتاح طوله 128 بت وتتكون من 10 جولات.
  - ✓ AES-192: مفتاح طوله 192 بت وتتكون من 12 جولة .
  - ✓ AES-256: مفتاح طوله 256 بت وتتكون من 14 جولة.

المخطط الصندوقي لخوارزمية(AES)



الخطوات العامة لخوارزمية (AES) (1/2)

١. إدخالات الخوارزمية :

- ✓ **النص الصريح** (البيانات الأصلية) : state
- ✓ **المفتاح السري** (مفتاح التشفير): K

٢. جولة أولية:

- ✓ **تتضمن إضافة مفتاح الدخل(المفتاح السري) أي العملية هي:** AddRoundKey = State XOR K

٣. حلقة الجولات:

- ✓ **تتكرر حسب طول المفتاح**
  - **خطوات كل جولة:**

١. استبدال : State = SubBytes(State)
٢. إزاحة : State = ShiftRows(State)
٣. مزج الأعمدة : State = MixColumns(State)
٤. إضافة مفتاح الجولة: State = AddRoundKey(State, RoundKey[i])

الخطوات العامة لخوارزمية(AES) (2/2)

٤. الجولة الأخيرة :

١. استبدال
٢. إزاحة
٣. إضافة مفتاح

1. State = SubBytes(State)
2. State = ShiftRows(State)
3. State = AddRoundKey(State, RoundKey[i])

- **لا توجد خطوة مزج الأعمدة**

٥. إخراج النص المشفر النهائي

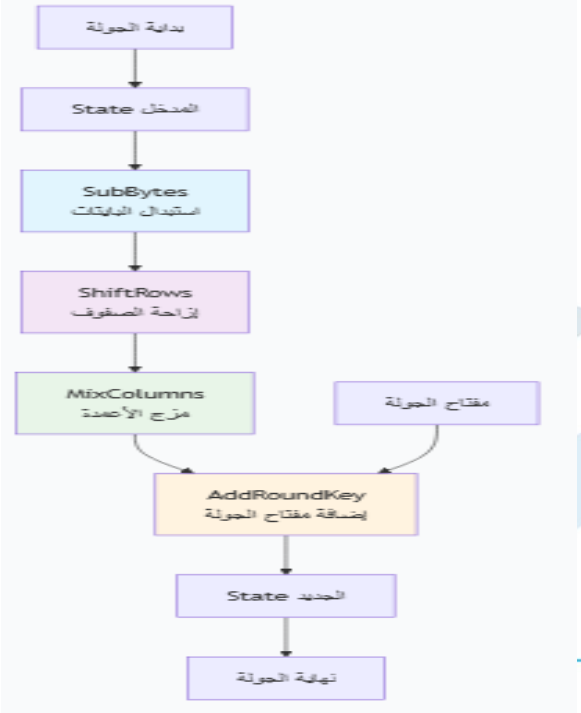
إدخالات الخوارزمية (قيم التهيئة)

١.يحول النص الصريح (128بت)من محارف إلى ترميز الأسكي
٢. يحول النص الصريح من ترميز الأسكي إلى النظام الست عشري HEX
٣.يكتب النص الصريح الناتج على شكل مصفوفة 4X4 بحيث كل أربع بايتات متتالية تمثل عمود تسمى المصفوفة الناتجة حالة **State**
٤.مع مفتاح الدخل نتبع نفس الخطوات السابقة تماماً

الجولة الأولية

تتضمن : State XOR K

المخطط الصندوقي للخطوات المنفذة داخل الجولة (1-9)في خوارزمية AES



الخطوات المنفذة داخل الجولة في خوارزمية AES(1/6)

1.استبدال البايتات (SubBytes)

- ✓ كل بايت في الـ Stateيُستبدل بقيمة مقابلة من جدول S-Box المبين تالياً
- ✓ الـ S-Boxهو جدول ثابت محدد مسبقاً يقوم بتحويل غير خطي للبيانات
- ✓ بنتيجة الاستبدال نحصل على جدول State جديد

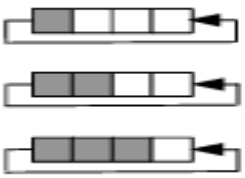
➢ طريقة الاستبدال

بفرض أن قيمة S-box= 32 هذا يعني أن القيمة state المقابلة موجودة ضمن الموقع الذي :

- سطره x=قيمة العشرات =3
- عموده y =قيمة الآحاد =2 أي state = 23

	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

الخطوات المنفذة داخل الجولة في خوارزمية AES(2/6)



2.إزاحة الصفوف(ShiftRows) :

- ✓ الصف الأول: لا إزاحة (يبقى كما هو)
- ✓ الصف الثاني: إزاحة دوارنية لليسار بمقدار 1 بايت
- ✓ الصف الثالث: إزاحة دوارنية لليسار بمقدار 2 بايت
- ✓ الصف الرابع: إزاحة دورانية لليسار بمقدار 3 بايت

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

مثال

بفرض أن الحالة الناتجة عن خطوة الاستبدال في الجولة الأولى كالآتي:

اكتب الحالة الناتجة بعد تطبيق الإزاحة:

STATE=

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

الخطوات المنفذة داخل الجولة في خوارزمية AES(3/6)

3.مزج الأعمدة (MixColumns):

✓ يعالج كل عمود في الـ State بشكل منفصل

✓ يُضرب كل عمود بمصفوفة ثابتة 4x4 في حقل غاوس Galois Field $GF(2^8)$ هذا ليس ضرباً عادياً، بل هو ضرب خاص في الحقول المنتهية

✓ رياضياً هذه العملية تخلط البايتات داخل كل عمود

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

مصفوفة **mix-columns** الثابتة

الخطوات المنفذة داخل الجولة في خوارزمية AES (4/6)

3.مزج الأعمدة (MixColumns):

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

➢ طريقة حساب بايتات كل عمود في مزج الأعمدة :

a_0
a_1
a_2
a_3

✓ بفرض أن قيم العمود الأول في مصفوفة State هي :

❖ تكون قيمة البايت الأول في العمود الجديد هي: $b_0 = (a_0.02)\oplus(a_1.03)\oplus(a_2.01)\oplus(a_3.01)$

❖ تكون قيمة البايت الثاني في العمود الجديد هي: $b_1 = (a_0.01)\oplus(a_1.02)\oplus(a_2.03)\oplus(a_3.01)$

❖ تكون قيمة البايت الثالث في العمود الجديد هي: $b_2 = (a_0.01)\oplus(a_1.01)\oplus(a_2.02)\oplus(a_3.03)$

❖ تكون قيمة البايت الرابع في العمود الجديد هي: $b_3 = (a_0.03)\oplus(a_1.01)\oplus(a_2.01)\oplus(a_3.02)$

وهكذا تحسب لباقي الأعمدة باستبدال فقط قيم العمود من مصفوفة state ضمن العلاقات السابقة

قواعد عملية الضرب المستخدمة في مزج الأعمدة (1/2)

❖ الضرب بـ 01 : يبقى البايت كما هو a3.01=a3

❖ الضرب بـ 02 :

- تزاح البتات لليسار (shift left)
- يكون لدينا حالتين ننظر إلى البت الأخير في العدد قبل الإزاحة :
  - ✓ إذا كان البت الأكثر أهميةMSB = 0 نأخذ الناتج كما هو
  - ✓ إذا كان البت الأكثر أهمية MSB= 1 تطبق XOR للناتج مع 1B

ملاحظة: في مقررنا سنعتمد على قيمة MSB قبل الإزاحة علماً أن هناك بعض النسخ تعتمد على أخذ قيمة MSB بعد الإزاحة.

➢ مثال:=3a.02

نحول إلى ثنائي:00111010

نطبق الإزاحة نحو اليسار: 01110100 ➔ 00111010

MSB=0 ، تكون قيمة الناتج كما هو ونحول إلى ست عشري:74

➢ مثال:=f2.02

نحول إلى ثنائي: 11110010

نطبق الإزاحة نحو اليسار: 11110010➔11100100

MSB=1 ، نطبق XOR : 11100100 XOR00011011=11111111=ff

قواعد عملية الضرب المستخدمة في مزج الأعمدة (2/2)

❖ الضرب بـ 03 : العدد XOR (العدد • 02) = العدد • 03

- نطبق ضرب بـ 2 أولاً حسب قاعدة الضرب السابقة الذكر
- تنفذ XOR بين ناتج الضرب وبين العدد نفسه

➢ مثال:=a3.03

3a .03 = (3a .02) XOR a3

نحول إلى ثنائي:00111010

نطبق الإزاحة نحو اليسار: 01110100 ➔ 00111010

MSB=0 ، تكون قيمة الناتج كما هونحول إلى ست عشري:74

نطبق XOR مع 74 :

01110100 XOR 00111010 =01001110=4e

➢ مثال:=f2.03

f2 .03 = (f2 .02) XOR f2

نحول إلى ثنائي: 11110010

نطبق الإزاحة نحو اليسار: 11110010➔11100100

MSB=1 ، نطبق XOR مع 1b :

11100100 XOR00011011=11111111

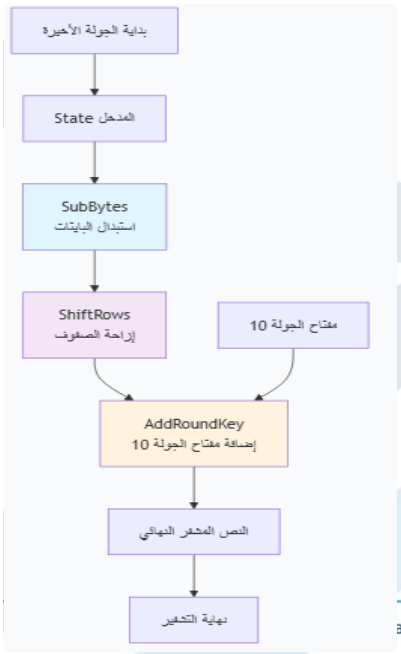
نطبق XOR مع f2 :

11111111 XOR 11110010=00001101=0d

الخطوات المنفذة داخل الجولة في خوارزمية AES (5/6)

4 إضافة مفتاح الجولة (AddRoundKey)

- ✓ تنفذ عملية XORبين الـ State ومفتاح الجولة الحالي
- ✓ يكون مفتاح الجولة بنفس حجم الـState أي 128 بت.
- ✓ يُنشأ مفتاح فرعي (Round Key) جديد من المفتاح الأصلي لكل جولة باستخدام خوارزمية Key Expansion
- ✓ ثم تنفذ عملية XOR بين الـ State ومفتاح الجولة.

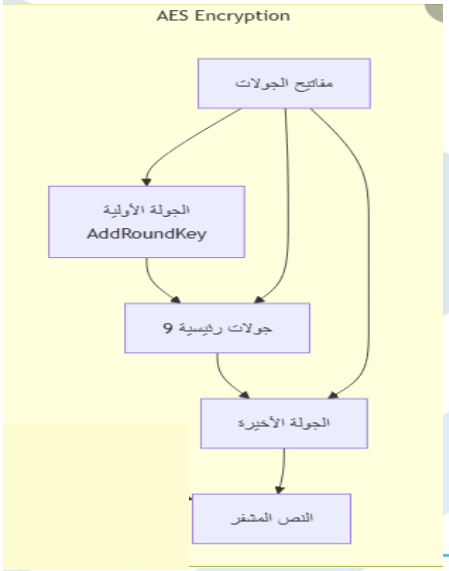


الخطوات المنفذة داخل الجولة الأخيرة في خوارزمية AES

- ✓ استبدال البايتات (SubBytes) State = SubBytes(State)
- ✓ إزاحة الصفوف (ShiftRows) State = ShiftRows(State)
- ✓ إضافة مفتاح (AddRoundKey) State = AddRoundKey(State, RoundKey[i])

لا توجد خطوة مزج الأعمدة في هذه الجولة

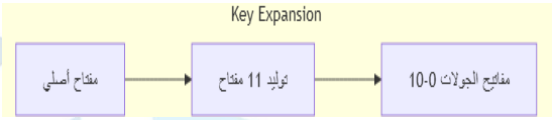
❖ خرج هذه المرحلة هو النص المشفر



خوارزمية توسيع المفتاح (Key Expansion) في خوارزمية AES

✓الغاية منها الحصول على كل المفاتيح الفرعية من المفتاح الأصلي.

✓يكون كل مفتاح فرعي مكون من 128 بت مساوٍ لحجم الـ (State)



✓خطوات خوارزمية توسيع المفتاح (Key Expansion) :

❖ الدخل : المفتاح الأصلي بطول 16 بايت

❖ الخرج :

- 44 كلمة كل منها مكون من 4 بايت
- 11 مفتاح فرعي (من أجل خوارزمية AES-128)،كل مفتاح فرعي مكون من 4 كلمات

خطوات الخوارزمية Key Expansion (1/2)

١. يقسم المفتاح الأصلي إلى أربع كلمات هي الكلمات : W[0],W[1],W[2],W[3]

٢. تولد الكلمات الجديدة وفق الخوارزمية الآتية:

- نميز حالتين:

❖ إذا كان رقم الكلمة W[i] ليس من مضاعفات العدد 4 :

تكون قيمة الكلمة هي ناتج تنفذ XOR بين: الكلمة الواقعة قبل الكلمة المراد حسابها بـ4 مواقع والكلمة السابقة مباشرة

$$W[i]=W[i-1] \text{ XOR } W[i-4]$$

خطوات الخوارزمية Key Expansion (2/2)

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

❖ إذا كان رقم الكلمة W[i] من مضاعفات العدد 4 :

١. تدوير الكلمة السابقة مباشرة للكلمة المراد حسابها (RotWord) ندور موقع بايت واحد لليسار :

RotWordw[i-1]

٢. استبدال(**SubWord**) : نستبدل كل بايت من بالقيمة المقابلة له في جدول S-Box :

SubWord (RotWordw[i-1])

٣. إضافة ثابت الجولة (() **Rcon**): ننفذ XOR للناتج عن الخطوتين السابقتين مع ثابت الجولة **Rcon[i]**

SubWord (RotWordw[i-1]) XOR Rcon[i]

٤. ننفذ XOR مع الكلمة الواقعة قبلها بـ 4 مواقع

W[i]=(SubWord (RotWordw[i-1])) XOR Rcon[i]) XOR W[i-4]

الخطوات المنفذة عند فك التشفير في خوارزمية AES

➢ **الجولات الرئيسة في فك التشفير:**

✓ إضافة المفتاح AddRoundKey لكنها تنفذ مع المفتاح الفرعي للجولة أي:

State= Cipher text XOR Subkey of round

✓ عكس إزاحة الأعمدة (InvMixColumns): عملية رياضية عكسية لخلط الأعمدة

✓ عكس إزاحة الصفوف (InvShiftRows): **إزاحة عكسية للصفوف لليمين بدلاً من اليسار**

- **الصف 0**: لا إزاحة
- **الصف 1**: إزاحة لليمين 1 بايت
- **الصف 2**: إزاحة لليمين 2 بايت
- **الصف 3**: إزاحة لليمين 3 بايت

✓ عكس استبدال البيانات (InvSubBytes): استبدال عكسي باستخدام S-Boxمعكوس

➢ **الجولة النهائية:** ✓ إضافة المفتاح AddRoundKey : **State= State XOR original key**

نهاية المحاضرة 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