جامعة المنارة
كلية الهندسة
قسم المعلوماتية

Information System Security
أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

الجلسة الثامنة

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

المسألة الأولى

إذا كان لدينا النص الصريح الآتي: ADAM
بفرض أن هذا النص رمزاعتماداً على تمثيل الأحرف الأبجدية بمكافئها الرقمي المكون من خانتين عشريتين:
A=00,B=01,C=02.....,Z=25

المطلوب:

١. **استخدم خوارزمية RSA ذات القيم lp=13,q=17التشفيرهذا النص علماً أن طول الكتلة يساوي محرفين علماً أن $e \in [1,5]$**

٢. **هل يمكن استخدم نفس الخوارزمية السابقة لكن مع اعتماد طول كتلة تساوي 4 محارف لتشفيرالنص السابق ذاته؟ علل إجابتك.**

الحل

الطلب الأول:

ترميز النص: ADAM

M={ AD, AM }
M={ M1, M2 }={0003,0012}

حساب المفتاح العام : $k_{pub} = \{e, n\}$

نستخدم العلاقة : $n = p \times q = 13 \times 17 = 221$

شرط التشفير : m<n محقق 3,12 < 221

حساب e : e عدد صحيح موجب، $gcd(\emptyset(n), e) = 1, 1 < e < \emptyset(n)$

$\emptyset(n) = (p-1)(q-1) = 12 \times 16 = 192$ ➔ e=5

فيكون المفتاح العام: $k_{pub} = \{5,221\}$

الحل

تابع الطلب الأول:

نطبق عملية التشفير $c = m^e mod n$

$$c1 = 3^5 mod 221 = 22 = 0022 \Leftrightarrow AV$$
$$c2 = 12^5 mod 221 = 207 = 0207 \Leftrightarrow CH$$

➔ **C= AVCH**

الطلب الثاني:

كلا لا يمكن لأن ترميز النص 30012 =ADAM شرط التشفير غير محقق لأن M<N

المسألة الثانية

إذا كان لدينا نظام حقيبة الظهر المستخدم يعتمد على المجموعة المتزايدة : b=[2,5,10,20] بفرض n=29 و r=8
وأن وبفرض أن التدوير المفروض هو: [4,2,1,3] والمطلوب:

1. ما هي قيمة k (عدد الأغراض)؟

2 . **أوجد المفتاحين العام والخاص.**

3. شفر النص x=11010001 .

4. فك تشفير النص S=16 بفرض أن $r^{-1} \in]10,13[$

الحل

1. قيمة k (عدد الأغراض)= حجم المصفوفة b = 4

2 . المفتاحين العام و الخاص.

من فرض المسألة المفتاح الخاص هو: n=29 و r=8 و التدوير و المجموعة المتزايدة :b=[2,5,10,20]

المفتاح العام:

من فرض المسألة المجموعة b هي مجموعة متزايدة.

نحسب المصفوفة t : $t_i = (b_i \times r) mod n$

$t_1 = (b_1 \times r) mod n = (2 \times 8) mod 29 = 16$

$t_2 = (b_2 \times r) mod n = (5 \times 8) mod 29 = 11$

$t_3 = (b_3 \times r) mod n = (10 \times 8) mod 29 = 22$

$t_4 = (b_4 \times r) mod n = (20 \times 8) mod 29 = 15$

فتكون t=[16,11,22,15]

نطبق التدوير فيكون المفتاح العام a=[15,11,16,22

الحل

3. شفر النص x=11010001 .

نلاحظ أن طول النص الصريح أكبر من k=4 ، نقسمه إلى كتلتين: X2=0001 و X1=1101

حسب العلاقة : $S_i = X1.a_1 + X2.a_2 + X3.a_3 + X4.a_4$

$S_1 = 1.15 + 1.11 + 0.16 + 1.22 = 48$

$S_2 = 0.15 + 0.11 + 0.16 + 1.22 = 22$

S=48 22

الحل

4. فك تشفير النص S=16 بفرض أن $r^{-1} \in]10,13[$

$$\dot{S} = (r^{-1} \times S) mod n$$

$$r \times r^{-1} mod\ n = 1 \Rightarrow (11 \times 8) mod 29 = 1 \Rightarrow r^{-1} = 11$$

$$\dot{S} = (11 \times 16) mod 29 = 2$$

$$\dot{S} = \dot{X}1.b_1 + \dot{X}2.b_2 + \dot{X}3.b_3 + \dot{X}4.b_4$$

$$\dot{S} = 1.2 + 0.5 + 0.10 + 0.20 \Rightarrow \dot{S} = 1000$$

نطبق التدوير S=0010

المسألة الثالثة

بفرض لدينا خوارزمية AES إذا علمت أن النص الصريح هو **Help him, please**

وأن الخوارزمية تستخدم المفتاح **cat eats meat890** المطلوب:

١.احسب قيم التهيئة لهذه الخوارزمية

٢. نفذ الجولة الأولية

المحرف	أسكي
H	1001000
e	1100101
l	1101100
p	1110000
space	0100000
h	1101000
a	1100001
i	1101001
s	1110011
m	1101101
,	0101100

جامعة المنارة
MANARA UNIVERSITY

الحل

١.حساب قيم التهيئة لهذه الخوارزمية

تهيئة النص الصريح:

١. المدخلات من جدول الأسكي :

٢.كتابة النص الصريح بالست عشري (hex)

H	e	l	p		h	i	m	,		p	l	e	a	s	e
48	65	6c	70	20	68	69	6d	2c	20	70	6c	65	61	73	65

٣. نكتب قيم النص الصريح على شكل مصفوفة 4x4

State=				
	48	20	2c	65
	65	68	20	61
	6c	69	70	73
	70	6d	6c	65

المحرف	أسكي
c	1100011
a	1100001
t	1110100
e	1100101
space	0100000
s	1110011
m	1101101
8	0111000
9	0111001
0	0110000

جامعة المنارة
MANARA UNIVERSITY

١.حساب قيم التهيئة لهذه الخوارزمية

تهيئة مفتاح الدخل: ١. المدخلات من جدول الأسكي :

٢.كتابة المفتاح بالست عشري (hex)

c	a	t		e	a	t	s		m	e	a	t	8	9	0
63	61	74	20	65	61	74	73	20	6d	65	61	74	38	39	30

٣. نكتب قيم المفتاح على شكل مصفوفة 4x4

K=				
	63	65	20	74
	61	61	6d	38
	74	74	65	39
	20	73	61	30

2. تنفيذ الجولة الأولية:

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

إضافة المفتاح الأولي:

48	20	2c	65
65	68	20	61
6c	69	70	73
70	6d	6c	65

$\oplus$

63	65	20	74
61	61	6d	38
74	74	65	39
20	73	61	30

=

STATE=	2b	45	0c	11
	04	09	4d	59
	18	1d	15	4a
	50	1e	0d	55

المسألة الرابعة

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

61
20
01
2f

احسب قيمة البايت الثالث b2 في العمود الأول من مصفوفة المزج.

الحل:

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

$b_2 = (61.01)\oplus(20.01)\oplus(01.02)\oplus(2f.03)$

✓ **حساب** (61.01) : $61.01 = 61$

✓ **حساب** (20.01) : $20.01 = 20$

✓ **حساب** (01.02) :

- ❖ نحول قيمة 01من ست عشري إلى ثنائي فتكون 00000001
- ❖ نطبق الإزاحة نحو اليسار 00000010 MSB=0 نأخذ الناتج الأول كما هو
- ❖ نحول 00000010 إلى ست عشري : **02**

$$\mathbf{01.02 = 02}$$

✓ **حساب** $(2f.03)$:

$$(2f.03) = (2f.02) \oplus 2f$$

- ❖ نحول قيمة 2f من ست عشري إلى ثنائي فتكون 00101111
- ❖ نطبق الإزاحة نحو اليسار 01011110 MSB=0 نأخذ الناتج الأول كما هو
- ❖ نطبقXOR: 01011110 ⊕ 00101111 =01110001=71

$$(2f.03) = 71$$

$$b_2 = (61.01) \oplus (20.01) \oplus (01.02) \oplus (2f.03)$$

$$b_2 = 61 \oplus 20 \oplus 02 \oplus 71$$

$$b_2 = 32$$

المسألة الخامسة

في خوارزمية AES بفرض مفتاح التشفيرهو: 01 30 11 25 1a 10 45 78 40 56 55 81 1a 2e ff 16

احسب قيمة الكلمتين W[4], W[5]

الحل:

يقسم مفتاح التشفير(مفتاح الدخل) إلى أربع كلمات:

W[0]= **01 30 11 25**

W[1]= **1a 10 45 78**

W[2]= **40 56 55 81**

W[3]= **1a 2e ff 16**

حساب الكلمة w[4]:

١. ندور الكلمة W[3]= **1a 2e ff 16** RotWord (W[3])= **2e ff 16 1a**

٢. ننفذ الاستبدال: SubWord (RotWord (W[3]))=31 16 47 a2

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

SubWord (RotWord (W[3])) XOR Rco(1)= 31 16 47 a2 XOR 01 00 00 00 = 30 16 47 a2

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]= 30 16 47 a2 XOR **01 30 11 25**

فتكون الكلمة: **W[4]= 31 26 56 87**

حساب الكلمة w[5]: 5 ليس من مضاعفات العدد 4 لذا نستخدم القانون: W[i]=W[i-4] XOR W[i-1]

W[5]=W[1] XOR W[4]= **1a 10 45 78** XOR **31 26 56 87**

W[5]=2b 36 13 ff

المسألة السادسة

إذا كان لديك تابع بعثرة بخرج 8 بايت والمطلوب:

١. ما عدد المحاولات لإيجاد تصادم باحتمال 20% ؟

٢. إذا كان جهازك يحسب 2×10^5 (H/Sec) . كم الوقت اللازم لإيجاد التصادم؟

حل المسألة

١. عدد المحاولات لإيجاد تصادم باحتمال 20%

$$k \approx \sqrt{2N\ ln\left(\frac{1}{1-p}\right)}$$

خرج تابع البعثرة 8 بايت =64 بت فيكون عدد القيم الممكنة : $N = 2^n = 2^{64} = 1.844 \times 10^{19}$

نعوض في علاقة عدد المحاولات لإيجاد تصادم

$$k \approx \sqrt{2 \times 1.844 \times 10^{19} ln\left(\frac{1}{1-0.2}\right)}$$

$$k \approx \sqrt{36.88 \times 10^{18} \times \ln(1.25)}$$

٢. الزمن اللازم لإيجاد التصادم:

$$k \approx 2.867 \times 10^9 \text{ محاولة}$$

$$T(sec) = \frac{k}{V} = \frac{2.867 \times 10^9}{2 \times 10^5} = 1.4335 \times 10^4 \text{ sec} \approx 0.398\ hours$$

نهاية المحاضرة