جامعة المنارة

كلية الهندسة

قسم ميكاترونيكس

Information System Security

أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

المسألة الأولى

من أجل خوارزمية RC4 إذا كان شعاع الحالة S مؤلف من 4 بايت و كان مفتاح الدخل هو K = {2,5}

المطلوب احسب النص المشفر للرسالة AI (**موضحاً الخوارزميات المستخدمة في الحل**)؟

مستفيداً من جدول الأسكي الآتي:

Char	Dec	Char	Dec
@	64	D	68
A	65	E	69
B	66	F	70
C	67	I	73

الحل:

1. بما أن شعاع الحالة S مؤلف من 4 بايت يكون: $S = \{0, 1, 2, 3\}$

2. إنشاء الشعاع المؤقت T

نطبق الخوارزمية الآتية:

طول الشعاع S-1

```
/* Initialization */
for  i = 0 to 255 do
S[i] = i;
T[i] = K[i mod keylen];
```

```
/* Initialization */
for  i = 0 to 3 do
S[i] = i;
T[i] = K[i mod 2];
```

طول مفتاح الدخل

نطبق الخوارزمية كالآتي من أجل مفتاح الدخل K = {2,5} :

i = 0

S[0] = 0;

T[0] = K[0 mod 2]= K[0]=2

i = 1

S[1] = 1;

T[1] = K[1 mod 2]= K[1]=5

i = 2

S[2] = 2;

T[2] = K[2 mod 2]= K[0]=2

i = 3

S[3] = 3;

T[3] = K[3 mod 2]= K[1]=5

0 1

↓ ↓

K = {2,5}

فيكون الشعاع المؤقت : T= {2, 5,2,5}

3- تهيئة الشعاع S

نطبق الخوارزمية الآتية :

طول الشعاع S-1

```
/* Initial Permutation of S */
j = 0;
for  i = 0 to 255 do
j = (j + S[i] + T[i]) mod 256;
Swap (S[i], S[j]);
```

طول الشعاع S

```
/* Initial Permutation of S */
j = 0;
for  i = 0 to 3 do
j = (j + S[i] + T[i]) mod 4;
Swap (S[i], S[j]);
```

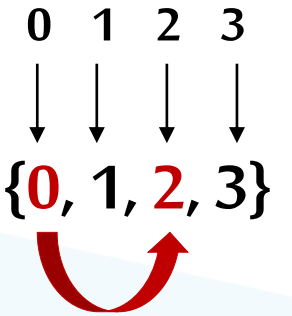
Iteration 1:

(i = 0, j = 0, S = {0, 1, 2, 3}): T= {2, 5,2,5}

j = (j + S[i] + T[i])mod4 = (0 + S[0] + T[0])mod4= (0 + 0 + 2)mod4 = 2

Swap S[i] with S[j]: Swap S[0] with S[2]: **S = {2, 1, 0, 3}**

عملية التبديل swap



S = {2, 1, 0, 3}

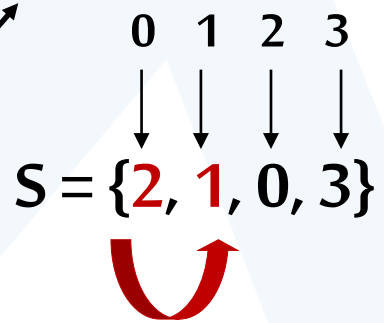
Iteration 2:

(i = 1, j = 2, S = {2, 1, 0, 3}): T= {2, 5,2,5}

j = (2+ S[1] + T[1])mod4 = (2 + 1 + 5)mod4 = 0

Swap S[i] with S[j]: Swap S[1] with S[0]: **S = {1, 2, 0, 3}**

عملية التبديل swap



S = {1, 2, 0, 3}

Iteration 3:

(i = 2, j = 0, S = {1, 2, 0, 3}): T= {2, 5,2,5}

$j = (0 + S[2] + T[2]) \bmod 4 = (0 + 0 + 2) \bmod 4 = 2$

Swap S[i] with S[j], Swap S[2] with S[2]: **S = {1, 2, 0, 3}**

Iteration 4:

(i = 3, j = 2, S = {1, 2, 0, 3}): T= {2, 5,2,5}

$j = (2 + S[3] + T[3]) \bmod 4 = (2 + 3 + 5) \bmod 4 = 2$

Swap S[i] with S[j], Swap S[3] with S[2]: **S = {1, 2, 3, 0}**

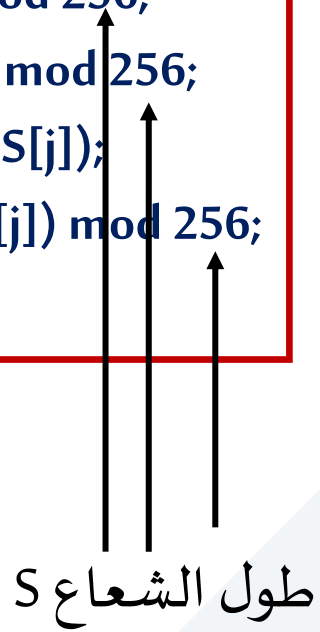
هذا هو شعاع S الذي سيستخدم في حساب سلسلة المفتاح الأولى

4-توليد السلسلة:

نطبق الخوارزمية الآتية :

```
/* Stream Generation */
i, j = 0;
while (true)
        i = (i + 1) mod 256;
        j = (j + S[i]) mod 256;
        Swap (S[i], S[j]);
        t = (S[i] + S[j]) mod 256;
        k = S[t];
```

```
/* Stream Generation */
i, j = 0;
while (true)
        i = (i + 1) mod 4;
        j = (j + S[i]) mod 4;
        Swap (S[i], S[j]);
        t = (S[i] + S[j]) mod 256;
        k = S[t];
```



توليد سلسلة المفتاح الأولى:

Reset i = j = 0, Recall S = {1, 2, 3, 0}

i = (i + 1) mod4 = (0 + 1) mod4 = 1

j = (j + S[i])mod 4 = = (0 + S[1]) mod4 =(0 + 2) mod 4 = 2

Swap S[1] and S[2]: **S = {1, 3, 2, 0}**

t = (S[1] + S[2]) mod 4= (3+2)mod 4=1

k = S[1]=3

تشفير البايت الأول من الرسالة:

البايت الأول هو A=67 نكتب تمثيله بالثنائي 0100 0011

النص الصريح	0100 0011
⊕ سلسلة المفتاح	0000 0011
البايت المشفر	**0100 0000**

النص المشفر= 64 تقابل @

توليد سلسلة المفتاح الثانية :

i = 1,j = 2, Recall **S = {1, 3, 2, 0}**

i = (i + 1) mod4 = 2

j = (j + S[i])mod 4 = (2 + 2) mod 4 = 0

Swap S[i] and S[j]: **S = {2, 3, 1, 0}**

t = (S[2] + S[0]) mod 4= (1+2)mod 4=3

k = S[3]=0

تشفير البايت الثاني من الرسالة:

البايت الثاني هو I=73 نكتب تمثيله بالثنائي 0100 1001

النص الصريح	0100 1001
⊕ سلسلة المفتاح	0000 0000
البايت المشفر	**0100 1001**

النص المشفر= 73تقابل I

النص الصريح هو: AI
النص المشفر هو:@I

0100 0011 0100 1001
0100 0000 0100 1001

المسألة الثانية

بفرض أن الخوارزمية RC4 تستخدم شعاع S مكون من 4 بايت، و مفتاح الدخل k=[10 15 5] لتشفير النص الصريح هو P=FA

المطلوب:احسب النص المشفرC حسب خوارزمية RC4 المفروضة و مستفيداً من جدول الـ ASCII الآتي:

Char	Dec	Char	Dec	Char	Dec	Char	Dec
A	65	D	68	G	71	J	74
B	66	E	69	H	72	K	75
C	67	F	70	I	73	L	76

1. بما أن شعاع الحالة S مؤلف من 4 بايت يكون: $S = \{0, 1, 2, 3\}$

2. تهيئة الشعاع S

Iteration 1 :

$(i = 0, j = 0, S = \{0, 1, 2, 3\})$: $T = \{10, 15, 5, 10\}$

$j = (j + S[i] + T[i]) \bmod 4 = (0 + 0 + 10) \bmod 4 = 2$

Swap S[i] with S[j], Swap S[0] with S[2]: $S = \{2,1,0,3\}$

Iteration 2 :

$(i = 1, j = 2, S = \{2, 1, 0, 3\})$: $T = \{10, 15, 5, 10\}$

$j = (j + S[i] + T[i]) \bmod 4 = (2 + 1 + 15) \bmod 4 = 2$

Swap S[i] with S[j], Swap S[1] with S[2]: $S = \{2,0,1,3\}$

Iteration 3:

(i = 2, j = 2, S = {2,0,1,3}): T = {10, 15, 5,10}

j = (j + S[i] + T[i])mod4 = (2 +1+ 5)mod4 = 0

Swap S[i] with S[j], Swap S[2] with S[0]: S = {1,0,2,3}

Iteration 4:

(i = 3, j = 0, S = {1,0,2,3}): T = {10, 15, 5,10}

j = (j + S[i] + T[i])mod4 = (0 +3+ 10)mod4 = 1

Swap S[i] with S[j], Swap S[3] with S[1]: S = {1,3,2,0}

Reset i = j = 0, Recall S = {1,3,2,0}

3. توليد سلسلة المفتاح الأولى:

i = (i + 1) mod4 = 1

j = (j + S[i])mod 4 = (0 + 3) mod 4 = 3

Swap S[i] and S[j], Swap S[1] with S[3]: S = {1,0,2,3}

t= (S[i] + S[j])mod 4 = (0+3)mod 4=3

k= S[t]= S[3]=3

4. تشفير البايت الأول من النص الصريح: البايت الأول هو 70= Fنكتب تمثيله بالثنائي 01000110

النص الصريح	0100 0110
سلسلة المفتاح	⊕ 0000 0011
النص المشفر	**01000101**

01000101=69=E

5. توليد سلسلة المفتاح االثانية:

i =1, j = 3, Recall S = {1,0,2,3}

i = (i + 1) mod4 = 2

j = (j + S[i])mod 4 = (3 + 2) mod 4 = 1

Swap S[i] and S[j], Swap S[2] and S[1]: S = {1,2,0,3}

Output K = S[(S[i] + S[j])mod 4] = S[(S[2] + S[1])mod 4]= S[(0+2)mod 4] = S[2]=0

t= (S[i] + S[j])mod 4 = (0+2)mod 4=2

k= S[t]= S[2]=0

65 XOR 0= 01000001 XOR 00000000=01000111=64=A

6. تشفير البايت الثاني من النص الصريح: البايت الثاني هو 64= Aنكتب تمثيله بالثنائي 01000110

النص الصريح	0100 0001
⊕ سلسلة المفتاح	0000 0000
النص المشفر	01000001

01000001=64=A

فيكون النص المشفرهو:EA

المسألة الثالثة

بفرض أن الخوارزمية RC4 تستخدم مفتاح الدخل k=[12 25] لتشفير النص الصريح هو HI والمطلوب:

1. ما هي قيمة الشعاع S إذا كان شعاع المؤقت T=[12 25 12] مع التعليل ؟
2. احسب النص المشفر C حسب خوارزمية RC4 المفروضة و مستفيداً من جدول الـ ASCII الآتي:

Char	Dec	Char	Dec	Char	Dec	Char	Dec
A	65	D	68	G	71	J	74
B	66	E	69	H	72	K	75
C	67	F	70	I	73	L	76

1. ما هي قيمة الشعاع S إذا كان شعاع المؤقت T=[12 25 12] مع التعليل ؟

يكون الشعاع S=[0 1 2] لان له نفس طول الشعاع المؤقت T أي 3 بايت.

2. حساب النص المشفر للنص الصريح HI.

1. تهيئة الشعاع S

Iteration 1 :

(i = 0, j = 0, S = {0, 1, 2}): T = {12, 25, 12}

j = (j + S[i] + T[i])mod3 = (0 + 0 + 12)mod3 = 0

Swap S[i] with S[j], Swap S[0] with S[0]: S = {0,1,2}

Iteration 2 :

(i = 1, j = 0, S = {0, 1, 2}): T= {12, 25, 12}

j = (j + S[i] + T[i])mod3 = (0 + 1 + 25)mod3 = 2

Swap S[i] with S[j], Swap S[1] with S[2]: S = {0, 2, 1}

Iteration 3:

(i = 2, j = 2, S = {0, 2, 1}): T = {12, 25, 12}

j = (j + S[i] +T[i])mod3 = (2 +1+ 12)mod3 = 0

Swap S[i] with S[j], Swap S[2] with S[0]: S = {1, 2, 0}

3. توليد سلسلة المفتاح الأولى:

Reset i = j = 0, Recall S = {1, 2, 0}

i = (i + 1) mod3 = 1

j = (j + S[i])mod 3 = (0 + 2) mod 3 = 2

Swap S[i] and S[j], Swap S[1] with S[2]: S = {1, 0, 2}

Output K = S[(S[i] + S[j])mod 3] = S[(0+2)mod 3] = S[2]=2

t= (S[i] + S[j])mod 3 = (0+2)mod 3=2

k= S[t]= S[2]=2

72 XOR 2= 01001000 XOR 00000010=01001010=74=J

البايت الأول هو 72= Hنكتب تمثيله بالثنائي 01001000

النص الصريح 01001000

⊕

سلسلة المفتاح 0000 0010

النص المشفر 01001010

01001010=74=J

3. توليد سلسلة المفتاح الثانية:

i = 1,j = 2, RecalL: S = {1, 0, 2}

i = (i + 1) mod3 = 2

j = (j + S[i])mod 3 = (2 + 2) mod 3 = 1

Swap S[i] and S[j], Swap S[2] and S[1]: S = {1, 2, 0}

t= (S[i] + S[j])mod 3= (S[2] + S[1])mod 3 = (0+2)mod 3=2

k = S[2]=0

6. تشفير البايت الثاني من النص الصريح: 71 XOR 0= 01000111 XOR 00000000=01000111=71=I

البايت الثاني هو 71=Iنكتب تمثيله بالثنائي 01000111

	01000111	النص الصريح
⊕	0000 0000	سلسلة المفتاح
	01000111	النص المشفر

01000111=**71=I**

فيكون النص المشفرهو:**JI**

جَامعة
المَنارة
MANARA UNIVERSITY

نهاية الجلسة السابعة