عملي أمن نظم المعلومات

جلسة العملي الخامسة

مدرسة المقرر

د. بشرى علي معلا

المسألة الأولى

إذا كان لدينا نظام حقيبة الظهر المستخدم يعتمد على إحدى المجموعتين :

b'=[1,2,4,5,9] , b=[2,7,11,21,42]

بفرض أن $n \in [80,85]$ وهي عدد فردي ، و أن $r \in]3,6[$ وبفرض أن التدوير المفروض هو :[4,2,1,5,3]

و المطلوب:

1.أوجد المفتاحين العام و الخاص

2 .شفر النص الصريح X= 01010

3 . فك تشفير النص S=52بفرض أن معكوس r ينتمي إلى المجال[63,65]

الطلب الأول:أوجد المفتاحين العام و الخاص

1. **يجب أن نختار إحدى المجموعتين المتزايدتين** b′=[1,2,4,5,9] , b=[2,7,11,21,42]

1. نلاحظ في المجموعة أن الشرط غير محقق $b' = [1,2,4,5,9]$

$$b_i \geq b_1 + b_2 + \cdots + b_{i-1}$$

$$5 \geq b_1 + b_2 + b_3 = 1 + 2 + 4 = 7$$ غير محقق

بالنتيجة ليست مجموعة متزايدة.

تابع الطلب الأول:أوجد المفتاحين العام و الخاص

2. نختبر فيما إذا كانت المجموعة $b = [2,7,11,21,42]$ تحقق الشرط $b_i \geq b_1 + b_2 + \cdots + b_{i-1}$

$7 \geq b_1 = 2$ محقق

$11 \geq b_1 + b_2 = 2 + 7 = 9$ محقق

$21 \geq b_1 + b_2 + b_3 = 2 + 7 + 11 = 20$ محقق

وهي تحقق الشرط و هي المجموعة المتزايدة التي سنختارها

تابع الطلب الأول:أوجد المفتاحين العام و الخاص

2. نختار n بحيث هي تحقق الشرط $n > b_1 + b_2 + b_3 + b_4 + b_5$

$$n > 2 + 7 + 11 + 21 + 42 = 83$$

وحسب فرض المسألة $n \in [80,85]$ و هي عدد فردي فتكون n=85

3 . نختار r=4 فتكون أولية مع n و حسب فرض المسألة $r \in]3,6[$

4. نحسب بعدها المصفوفة t باستخدام العلاقة : $t_i = (b_i \times r) mod(n)$

$$t_1 = (2 \times 4) mod(85) = 8$$

$$t_2 = (7 \times 4) mod(85) = 28$$

$$t_3 = (11 \times 4) mod(85) = 44$$

$$t_4 = (21 \times 4) mod(85) = 84$$

$$t_5 = (42 \times 4) mod(85) = 83$$

فتكون المصفوفة t=[8,28,44,84,83]

تابع الطلب الأول:أوجد المفتاحين العام و الخاص

5. بفرض أن التدوير هو : [4,2,1,5,3] بعد تدوير t ينتج **المفتاح العام** : a=[84, 28,8,83,44]

6.ويكون المفتاح الخاص هو: n=85 r=4 $b = [2,7,11,21,42]$ التدوير: [4,2,1,5,3]

الطلب الثاني : تشفير النص X=01010

من أجل عملية التشفير نستخدم المفتاح العام: a=[84, 28,8,83,44]

$$S = X_1 a_1 + X_2 a_2 + X_3 a_3 + X_4\, a_4 + X_5\, a_5$$

$$S = 0.84 + 1.28 + 0.8 + 1.83 + 0.44 = 111$$

الطلب الثالث: فك تشفير S=52

1. معكوس r=4 بالنسبة لـ mod(85)

$$4^{-1}mod(85) \equiv 64$$

بحيث: $4 \times 64mod(85) = 256mod(85) = 1$

2. نحسب $s' = (r^{-1} \times s)mod(n)=(64 \times 52)mod85 = 3328\ mod85 = 13$

3. لدينا b=[2,7,11,21,42] فيكون $s' = X'_1b_1 + X'_2b_2 + X'_3b_3 + X'_4b_4 + X'_5b_5$

$13 = 1 \times 2 + 0 \times 7 + 1 \times 11 + 0 \times 21 + 0 \times 42$

فتكون قيم X': $X' = 10100$

4. ندور قيم X' وفق التدوير المفروض [4,2,1,5,3] فنحصل على X=00101

المسألة الثانية

إذا كان لدينا نظام حقيبة الظهر المستخدم يعتمد على المجموعة : b=[1,2,4,10,20,40]

بفرض أن n=110 و أن $r \in [30,32]$ وبفرض أن التدوير المفروض هو :[1,2,4,3,6,5]

و المطلوب:

1. ما هي قيمة K ؟
2. أوجد المفتاحين العام و الخاص
3. شفر النص الصريح 10010011111001011110
4. فك تشفير النص 121 S=45 بفرض أن معكوس r ينتمي إلى المجال[70,73]

الطلب الأول:

قيمة K=6 لأنها مساوية لعدد عناصر المجموعة b

الطلب الثاني :

1. نختبر فيما إذا كانت المجموعة المتزايدة b=[1,2,4,10,20,40] تحقق الشرط $b_i \geq b_1 + b_2 + \cdots + b_{i-1}$

$2 \geq b_1 = 1$ محقق

$4 \geq b_1 + b_2 = 1 + 2 = 3$ محقق

$10 \geq b_1 + b_2 + b_3 = 1 + 2 + 4 = 7$ محقق

$20 \geq b_1 + b_2 + b_3 + b_4 = 1 + 2 + 4 + 10 = 17$ محقق

$40 \geq b_1 + b_2 + b_3 + b_4 + b_5 = 1 + 2 + 4 + 10 + 20 = 37$ محقق

وهي تحقق الشرط

الطلب الثاني :

2 . لدينا من فرض المسألة n=110 لذا نختار r=31 فتكون أولية مع n و ضمن المجال $r \in [30,32]$

3. نحسب بعدها المصفوفة t باستخدام العلاقة : $t_i = (b_i \times r) mod(n)$

$$t_1 = (1 \times 31) mod 110 = 31 \qquad t_4 = (10 \times 31) mod 110 = 90$$

$$t_2 = (2 \times 31) mod 110 = 62 \qquad t_5 = (20 \times 31) mod 110 = 70$$

$$t_3 = (4 \times 31) mod 110 = 14 \qquad t_6 = (40 \times 31) mod 110 = 30$$

فتكون المصفوفة t=[31,62,14,90,70,30]

4. بفرض أن التدوير هو : [1,2,4,3,6,5] بعد تدوير t ينتج **المفتاح العام** : a=[31, 62,90,14,30,70]

5.ويكون المفتاح الخاص هو: n=110 r=31 b=[1,2,4,10,20,40] التدوير : [1,2,4,3,6,5]

الطلب الثالث : شفر النص الصريح 1001001111100101110

نلاحظ ان طول النص المطلوب تشفير أكبر عدد الأغراض من k=6 لذا نقسم النص الصريح إلى سلاسل طول كل منها مساوٍ

k=6 فيكون: x1= 100100, X2= 111100, X3= 101110

من أجل عملية التشفير نستخدم المفتاح العام: a=[31, 62,90,14,30,70]

$$S = X_1 a_1 + X_2 a_2 + X_3 a_3 + X_4 a_4 + X_5 a_5 + X_6 a_6$$

$$S1 = 1.31 + 0.62 + 0.90 + 1.14 + 0.30 + 0.70 = 45$$

$$S2 = 1.31 + 1.62 + 1.90 + 1.14 + 0.30 + 0.70 = 197$$

$$S3 = 1.31 + 0.62 + 1.90 + 1.14 + 1.30 + 0.70 = 165$$

$$S = s1 \quad s2 \quad s3$$

$$S = 45 \quad 197 \quad 165$$

الطلب الرابع: فك تشفير S=45 121

1.من أجل عملية فك التشفير يلزمنا حساب معكوس r بالنسبة لـ mod (n) :

نختبر القيم الموجودة ضمن المجال المفروض فنجد أن قيمة المعكوس هي 71 لأن

معكوس r=31 بالنسبة لـ mod(110) $31^{-1}mod(110) \equiv 71$

بحيث: $31 \times 71mod(110) = 2201mod(110) = 1$

نلاحظ أن لدينا S=S1 S2 حيث: S1=45 و S2=121

الطلب الرابع: فك تشفير S=45 121

2. لفك تشفير S1=45

$$s1' = (r^{-1} \times s1) mod(n) = (71 \times 45) mod 110 = 3195\ mod 110 = 5$$

- نحسب:

$$s1' = X_1' b_1 + X_2' b_2 + X_3' b_3 + X_4' b_4 + X_5' b_5 + X_6' b_6$$

- لدينا:

$$11 = 1 \times 1 + 0 \times 1 + 1 \times 4 + 0 \times 10 + 0 \times 20 + 0 \times 40$$

ومنه : $X'1 = 101000$

- ندور $X1'$ وفق التدوير المفروض [1,2,4,3,6,5] فنحصل على X1=100100

3. فك تشفير S2=121

- نحسب: $s2' = (r^{-1} \times s2) mod(n) = (71 \times 121) mod 110 = 8591\, mod 110 = 11$
- لدينا: $s' = X'_1 b_1 + X'_2 b_2 + X'_3 b_3 + X'_4 b_4 + X'_5 b_5 + X'_6 b_6$

$$11 = 1 \times 1 + 0 \times 1 + 0 \times 4 + 1 \times 10 + 0 \times 20 + 0 \times 40$$

- فتكون X': $X' = 100100$

ندور X' وفق التدوير المفروض [1,2,4,3,6,5] فنحصل على X=101000

المسألة الثالثة

في خوارزمية حقيبة الظهر بفرض لدينا المجموعة $b = [1,2,6,12]$ وبفرض أن $n \in [23,26]$ ومن مضاعفات العدد 6 و بفرض أن $r \in]3,6[$ و أن التدوير المفروض هو $[4,1,2,3]$

المطلوب:

1. أثبت أن المجموعة b هي مجموعة متزايدة
2. أوجد المفتاح العام و المفتاح الخاص لهذه الخوارزمية.
3. شفر النص x=1101.
4. فك تشفير النص s=102 ، إذا علمت أن معكوس r هي ضمن المجال $[3,6]$.

الطلب الأول:

1. إذا كانت المجموعة المتزايدة $b = [1,2,6,12]$ يجب أن تحقق الشرط

$$b_i \geq b_1 + b_2 + \cdots + b_{i-1}$$

$2 \geq b_1 = 1$ محقق

$6 \geq b_1 + b_2 = 1 + 2 = 3$ محقق

$12 \geq b_1 + b_2 + b_3 = 1 + 2 + 6 = 9$ محقق وهي تحقق الشرط

الطلب االثاني:

1 . نختار n بحيث تحقق الشرط $n > b_1 + b_2 + b_3 + b_4$

$$n > 1 + 2 + 6 + 12$$

$$n > 21$$

لدينا من نص المسألة أن n مضاعفات العدد 6 و $n \in [23,26]$ وبالنتيجة n=24

2 . نختار r بحيث أولية مع n و حسب فرض المسألة $r \in]3,6[$: فتكون r=5

3. نحسب بعدها المصفوفة t باستخدام العلاقة : $t_i = (b_i \times r) mod(n)$

$$t_1 = (1 \times 5) mod 24 = 5 \qquad t_3 = (6 \times 5) mod 24 = 6$$

$$t_2 = (2 \times 5) mod 24 = 10 \qquad t_4 = (12 \times 5) mod 24 = 12$$

فتكون المصفوفة t=[5,10,6,12]

تابع الطلب االثاني:

4. بفرض أن التدوير هو : [4,1,2,3] بعد تدوير t ينتج المفتاح العام : a=[12, 5,10,6]

5.ويكون المفتاح الخاص هو: n=24 r=5 $b = [1,2,6,12]$ التدوير : [4,1,2,3]

الطلب الثالث : شفر النص x=1101.

طول النص الصريح مساوٍ لعدد الأغراض k=4

من أجل عملية التشفير نستخدم المفتاح العام: a=[12, 5,10,6]

$$S = X_1 a_1 + X_2 a_2 + X_3 a_3 + X_4 a_4$$

$$S = 1.12 + 1.5 + 0.10 + 1.6 = 33$$

الطلب الرابع: فك تشفير النص s=102 ، إذا علمت أن معكوس r هي ضمن المجال [3,6]

1.من أجل عملية فك التشفير يلزمنا حساب معكوس r بالنسبة لـ mod (n) :

نختبر القيم الموجودة ضمن المجال المفروض فنجد أن قيمة المعكوس هي 5 لأن

معكوس r=5 بالنسبة لـ mod(24) $5^{-1}mod(24) \equiv 5$

بحيث: $5 \times 5mod(24) = 25mod(24) = 1$

2. نحسب $s' = (r^{-1} \times s)mod(n)=(5 \times 102)mod24 = 510\ mod24 = 6$

تابع الطلب الرابع:

3. لدينا فيكون $s' = X'_1 b_1 + X'_2 b_2 + X'_3 b_3 + X'_4 b_4$

$$6 = 0 \times 1 + 0 \times 2 + 1 \times 6 + 0 \times 12$$

فتكون قيم X': $X'_1 = 0010$

4. ندور قيم X' وفق التدوير المفروض [4,1,2,3] فنحصل على X=0001

جَامعة
المَنارة
MANARA UNIVERSITY

نهاية المحاضرة الخامسة عملي