

عملي أمن نظم المعلومات

جلسة العملي الثالثة

مدرسة المقرر

د. بشرى علي معلا

محاضرة مسائل

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 $S=52$ بفرض أن معكوس r ينتمي إلى المجال $[63,65]$

الطلب الأول: أوجد المفتاحين العام والخاص

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 $b' = [1,2,4,5,9]$

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

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

بالنتيجة ليست مجموعة متزايدة.

تابع الطلب الأول: أوجد المفتاحين العام والخاص

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

$$\text{محقق } 7 \geq b_1 = 2$$

$$\text{محقق } 11 \geq b_1 + b_2 = 2 + 7 = 9$$

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

وهي تحقق الشرط و هي المجموعة المتزايدة التي سنختارها

تابع الطلب الأول: أوجد المفتاحين العام والخاص

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: $t_i = (b_i \times r) \bmod(n)$

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

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

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

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

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

فتكون المصفوفة $t=[8, 28, 44, 84, 83]$

تابع الطلب الأول: أوجد المفتاحين العام والخاص

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 $\text{mod}(85)$

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

$$4 \times 64 \text{mod}(85) = 256 \text{mod}(85) = 1 \quad \text{بحيث:}$$

2. نحسب $s' = (r^{-1} \times s) \text{mod}(n) = (64 \times 52) \text{mod} 85 = 3328 \text{mod} 85 = 13$

3. لدينا $b=[2,7,11,21,42]$ فيكون $s' = X'_1 b_1 + X'_2 b_2 + X'_3 b_3 + X'_4 b_4 + X'_5 b_5$

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

فتكون قيم $X' = 10100$

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:

١. ما هي قيمة K ؟
٢. أوجد المفتاحين العام و الخاص
٣. شفر النص الصريح 100100111100101110
٤. فك تشفير النص $S=45\ 121$ بفرض أن معكوس r ينتهي إلى المجال $[70,73]$

الطلب الأول:

قيمة $K=6$ لأنها مساوية لعدد عناصر المجموعة b

الطلب الثاني :

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

$$\text{محقق } 2 \geq b_1 = 1$$

$$\text{محقق } 4 \geq b_1 + b_2 = 1 + 2 = 3$$

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

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

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

وهي تحقق الشرط

الطلب الثاني :

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

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

$$t_1 = (1 \times 31) \bmod 110 = 31$$

$$t_4 = (10 \times 31) \bmod 110 = 90$$

$$t_2 = (2 \times 31) \bmod 110 = 62$$

$$t_5 = (20 \times 31) \bmod 110 = 70$$

$$t_3 = (4 \times 31) \bmod 110 = 14$$

$$t_6 = (40 \times 31) \bmod 110 = 30$$

فتكون المصفوفة $t=[31,62,14,90,70,30]$

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

٥. 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 100100111100101110

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: $x_1=100100, x_2=111100, x_3=101110$

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

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

$$S_1 = 1.31 + 0.62 + 0.90 + 1.14 + 0.30 + 0.70 = 45$$

$$S_2 = 1.31 + 1.62 + 1.90 + 1.14 + 0.30 + 0.70 = 197$$

$$S_3 = 1.31 + 0.62 + 1.90 + 1.14 + 1.30 + 0.70 = 165$$

$$S = s_1 \quad s_2 \quad s_3$$

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

الطلب الرابع: فك تشفير 121 45=S

١. من أجل عملية فك التشفير يلزمنا حساب معكوس r بالنسبة لـ $\text{mod}(n)$:

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

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

$$31 \times 71 \text{mod}(110) = 2201 \text{mod}(110) = 1 \quad \text{بحيث:}$$

نلاحظ أن لدينا S_2 و $S_1=45$ حيث: $S=S_1$ و $S_2=121$

الطلب الرابع: فك تشفير 121 45=S

2. لفك تشفير 45=S1

$$s1' = (r^{-1} \times s1) \bmod(n) = (7^{-1} \times 45) \bmod 110 = 3195 \bmod 110 = 5$$

$$s1' = X'_1 b_1 + X'_2 b_2 + X'_3 b_3 + X'_4 b_4 + X'_5 b_5 + X'_6 b_6$$

• نحسب:

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

• لدينا:

$$X'_1 = 101000 \text{ ومنه :}$$

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

٣. فك تشفير $S2=121$

• نحسب: $s2' = (r^{-1} \times s2) \bmod(n) = (7 \times 121) \bmod 110 = 8591 \bmod 110 = 11$

• 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 $X' = 100100$

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:

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

الطلب الأول:

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

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

$$2 \geq b_1 = 1 \text{ محقق}$$

$$6 \geq b_1 + b_2 = 1 + 2 = 3 \text{ محقق}$$

$$12 \geq b_1 + b_2 + b_3 = 1 + 2 + 6 = 9 \text{ محقق}$$

وهي تحقق الشرط

الطلب الثاني:

١. 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 $n=24$

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

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

$$t_1 = (1 \times 5) \bmod 24 = 5$$

$$t_3 = (6 \times 5) \bmod 24 = 6$$

$$t_2 = (2 \times 5) \bmod 24 = 10$$

$$t_4 = (12 \times 5) \bmod 24 = 12$$

فتكون المصفوفة $t=[5,10,6,12]$

تابع الطلب الثاني:

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

٥. 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 $[3,6]$

١. من أجل عملية فك التشفير يلزمنا حساب معكوس r بالنسبة لـ $\text{mod}(n)$:

نختبر القيم الموجودة ضمن المجال المفروض فنجد أن قيمة المعكوس هي ٥ لأن

$$5^{-1} \text{mod}(24) \equiv 5$$

معكوس $r=5$ بالنسبة لـ $\text{mod}(24)$

$$5 \times 5 \text{mod}(24) = 25 \text{mod}(24) = 1$$

بحيث:

$$s' = (r^{-1} \times s) \text{mod}(n) = (5 \times 102) \text{mod} 24 = 510 \text{mod} 24 = 6 \quad \text{2. نحسب}$$

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 $X=0001$

نهاية المحاضرة