مهارات الحاسوب

الدكتور المهندس
مثنى القبيلي

هندسة الروبوتيكس والأنظمة الذكية
كلية الهندسة
جامعة المنارة

الفصل الدراسي الأول ٢٠٢١-٢٠٢٢

المسألة الأولى

إذا كان لدينا نظام حقيبة الظهر المستخدم يعتمد على مجموعة متزايدة من المجموعات الآتية: b=[2,7,11,21,42] ، b'=[1,2,4,5,9]

و بفرض أن $n \in [80,85]$ وليست عدداً زوجياً و $r \in]3,6[$. و التدوير المفروض هو المطلوب: [4,2,1,5,3]

١. أوجد كلاً من المفتاحين العام والخاص.

٢. شفر النص الصريح x=01010

٣. فك تشفير النص المشفر s=52 بفرض أن معكوس r يقع ضمن المجال [63,65]

2

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 ينتمي إلى المجال[70,73]

3

المسألة الثالثة

إذا كان لدينا النص الصريح الآتي: HELLO

بفرض أن هذا النص تم ترميزه اعتماداً على تمثيل الأحرف الأبجدية بأعداد صحيحة كالآتي:

A=2,B=3,C=4.....Z=27

المطلوب:

١. استخدم خوارزمية RSA ذات القيم p=3,q=11 لتشفير هذا النص علماً أنه يتم التعامل معه كسلسلة من الأعداد الصحيحة الممثلة للأحرف

٢. ما هو البلوك ذو القيمة الأعلى الذي يمكن تشفيره بواسطة هذه الخوارزمية باستخدام طريقة الترميز المستخدمة؟

٣. برأيك هل يمكن أن تتشكل بلوكات غير قابلة للتشفير وفق خوارزمية RSA المفروضة في نص المسألة؟

4

المسألة الرابعة

إذا كان لدينا النص الصريح الآتي: ATTACK

التعامل مع هذا النص على شكل كتل طول كل كتلة 3 محارف ، بفرض أن ترميز هذا النص يعتمد على نظام للأساس (26) حيث يبدأ الترميز الأبجدي A=0 و الخانة ذات الأهمية الأعظمية على اليسار

المطلوب:

١. استخدم خوارزمية RSA ذات القيم e=3, p=131,q=137 لتشفير هذا النص

٢. إذا علمت أنه يمكن الحصول على كتلة المحارف (Ch1Ch2..ChT) من كتلة الأعداد(m) المرمز بالطريقة السابقة باتباع الخوارزمية الآتية:

$$m \div 26^{T-1} = Ch_1 \text{ rem } m_1$$
$$m_1 \div 26^{T-2} = Ch_2 \text{ rem } m_2$$
$$\vdots$$
$$m_i \div 26^{0} = Ch_i \text{ rem } m0$$

حيث T طول الكتلة، m1,....mi بواقي عملية القسمة، ch1,....chT هي ناتج القسمة و تمثل القيم العددية للمحارف مثلاً CH1=5 =>CH1=F مع الأخذ بالحسبان أن الأعداد التي ليس لها محرف مقابل تترك كما هي.

طبق خوارزمية الترميز هذه للحصول على النص المشفر على شكل محارف المقابل لكتلة الأعداد المحسوب في الطلب السابق.

5

المسألة الخامسة

إذا كان لدينا النص الصريح الآتي: PUBLIC

بفرض أن هذا النص رمز اعتماداً على تمثيل الأحرف الأبجدية بمكافئها الرقمي المكون من خانتين عشريتين: A=00,B=01,C=02.....

المطلوب:

١. استخدم خوارزمية RSA ذات القيم p=43,q=59 لتشفير هذا النص علماً أن طول الكتلة يساوي محرفين موضحاً حسابياً إمكانية استخدام e=13 في هذه الخوارزمية.

٢. هل يمكن استخدم نفس الخوارزمية السابقة لكن مع اعتماد طول كتلة تساوي ٣ محارف لتشفير النص السابق ذاته.

6

المسألة السادسة

إذا كان لدينا العبارة الآتية كنص صريح لدخل الخوارزمية RSA:

GOOD MAN

حيث يشكل كل محرفين بلوك واحد. بفرض أن هذا النص تم ترميزه اعتماداً على نظام للأساس 26 حيث A=0,B=1,.....,Z=25, SPACE=26

المطلوب:

أولاً. أجل خوارزمية RSA ذات القيم الأولية p=19, q=47 و e€]1,6[.

١. أوجد النص المشفر المقابل للنص الصريح على شكل بلوكات عددية باستخدام هذه الخوارزمية علماً أن الخانة الأكثر أهمية هي آخر خانة على اليسار.

٢. أثبت أن خوارزمية RSA المعطاة قادرة على تشفير جميع البلوكات المرمزة وفق طريقة الترميز المفروضة.

7

المسألة السادسة

إذا كان لدينا العبارة الآتية كنص صريح لدخل الخوارزمية RSA:

GOOD MAN

حيث يشكل كل محرفين بلوك واحد. بفرض أن هذا النص تم ترميزه اعتماداً على نظام للأساس 26 حيث A=0,B=1,.....,Z=25, SPACE=26

المطلوب:

ثانياً. أجل خوارزمية RSA ذات القيم الأولية p=7, q=11 و بفرض e=37 تحقق الشروط المطلوبة.

١. بين مع التعليل أي من القيم الثلاثة الآتية تصلح أن تكون قيمة d : {11,12,13}.

٢. احسب النص الصريح المقابل للنص المشفر C=26

٣. بفرض استخدمنا طريقة الترميز ذاتها المذكورة سابقاً، هل يوجد بلوكات غير قابلة للتشفير باستخدام خوارزمية RSA فرضياتها المعطاة في هذا الطلب ؟ علل إجابتك.

8