جامعة المنارة

كلية الهندسة

قسم المعلوماتية

Information System Security

أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

الأربعاء18/11/2024

جَامعة المَنارة
MANARA UNIVERSITY

جلسة العملي الثالثة

مسائل عن خوارزمية RSA

المسألة الأولى

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:

1. استخدم خوارزمية RSA ذات القيم p=3,q=11 لتشفير هذا النص علماً أنه يتم التعامل معه كسلسلة من الأعداد الصحيحة الممثلة للأحرف
2. ما هو البلوك ذو القيمة الأعلى الذي يمكن تشفيره بواسطة هذه الخوارزمية باستخدام طريقة الترميز المستخدمة؟
3. برأيك هل يمكن أن تتشكل بلوكات غير قابلة للتشفير وفق خوارزمية RSA المفروضة في نص المسألة؟

حل المسألة الأولى (1/3)

الطلب الأول:

1. نرمز النص الصريح المعطى:

اعتماداً على الترميز المعطى تكون السلسلة الممثلة للنص الصريح هي: $(m_1, m_2, m_3, m_4, m_5) = (9,6,13,13,16)$

2. إيجاد المفتاح العام: $K_{pub} = \{e, n\}$

لتشفير النص الصريح نحتاج لحساب المفتاح العام: $n = p \times q = 11 \times 3 = 33$

$$\phi(n) = (p-1) \times (q-1) = 10 \times 2 = 20$$

نختار عدد صحيح (e) بحيث يكون : $\gcd(\phi(n), e) = 1; \quad 1 < e < \phi(n)$

$$\gcd(20,e)=1 \; ; \; 1< e < 20 \Rightarrow e = 3$$

$$\Rightarrow K_{pub} = \{e, n\} = \{3,33\}$$

حل المسألة الأولى (2/3)

تابع للطلب الأول:

3. عملية التشفير:

يجب أن نتأكد من شرط التشفير M<N نلاحظ أن شرط التشفير محقق لأن 33> 9,6,13,16

$$C_1 = M_1{}^e \bmod(n) = 9^3 \bmod(33) = 3$$

$$C_2 = M_2{}^e \bmod(n) = 6^3 \bmod(33) = 18$$

$$C_3 = M_3{}^e \bmod(n) = 13^3 \bmod(33) = 19 = C_4$$

$$C_5 = M_3{}^e \bmod(n) = 16^3 \bmod(33) = 4$$

$$\Rightarrow C = (C_1, C_2, C_3, C_4, C_5) = (3,18,19,19,4)$$

فيكون النص المشفر BQRRC

حل المسألة الأولى (3/3)

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

البلوك هو Z و قيمته 27 وهو يحقق الشرط M=27 < N=33

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

كلا إذ أن شرط التشفير محقق دوماً M<n حيث لأن قيمة أكبر بلوك z=27<n=33

المسألة الثانية

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:

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

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

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

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.

حل المسألة الثانية (1/3)

الطلب الأول:

1. نرمز النص الصريح المعطى:

يقسم النص الصريح إلى كتل طول كل منها 3 محارف:

ATT ACK

$$m_1 = ATT = 0\times 26^2 + 19\times 26^1 + 19 = 513$$
$$m_2 = ACK = 0\times 26^2 + 2\times 26^1 + 10 = 62$$

$$\Rightarrow M = (m_1, m_2) = (513,62)$$

2. إيجاد المفتاح العام:

$$n = p\times q = 131\times 137 = 17947$$

$$\Rightarrow K_{pub} = \{e, n\} = \{3,17947\}$$

حل المسألة الثانية (2/3)

تابع للطلب الأول:

3. عملية التشفير:

نتحقق من شرط التشفير M <n نلاحظ أنه محقق لأن 513,62 <17947

$$C_1 = M_1{}^e \bmod(n) = 513^3 \bmod(17947) = 8363$$

$$C_2 = M_2{}^e \bmod(n) = 62^3 \bmod(17947) = 5017$$

$$C = (C_1, C_2)$$

$$\Rightarrow C = (8363,5017)$$

حل المسألة الثانية (3/3)

الطلب الثاني:

$$m \div 26^{T-1} = Ch_1 \text{ rem } m_1$$

$$m_1 \div 26^{T-2} = Ch_2 \text{ rem } m_2$$

$$\vdots$$

$$m_i \div 26^{0} = Ch_T rem \text{ m0}$$

فيكون النص المشفرعلى شكل محارف

$$\Rightarrow C_1 = 8363$$

$$8363 \div 26^2 = 12 \text{ rem } 251 \Rightarrow \text{Ch1} = M$$

$$251 \div 26^1 = 9 \text{ rem } 17 \Rightarrow \text{Ch2} = \text{J}$$

$$17 \div 26^0 = 17 \; rem \; 0 \Rightarrow \text{Ch3} = R$$

C1=MJR

$$\Rightarrow C_2 = 5017$$

$$5017 \div 26^2 = 7 \text{ rem } 285 \Rightarrow \text{Ch1} = H$$

$$285 \div 26^1 = 10 \text{rem } 25 \Rightarrow \text{Ch2} = \text{K}$$

$$25 \div 26^0 = 25 \; rem \; 0 \Rightarrow \text{Ch3} = \text{Z}$$

C2=HKZ

➔C=MJRHKZ

المسألة الثالثة

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:

1. 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.

2. هل يمكن استخدم نفس الخوارزمية السابقة لكن مع اعتماد طول كتلة تساوي 3 محارف لتشفير النص السابق ذاته.

حل المسألة الثالثة(1/5)

الطلب الأول:

1. نرمز النص الصريح المعطى:

لدينا طول الكتلة تساوي 2 وكل محرف نقابله بمكافئه الرقمي المكون من خانتين عشريتين:

P U	B L	I C
15 20	01 11	08 02

M1=1520

M2=0111 ⟹ M=(1520,0111,0802)

M3=0802

حل المسألة الثالثة(2/5)

تابع للطلب الأول:

2. إيجاد المفتاح العام:

$$K_{pub} = \{e, n\}$$

$$n = p \times q = 43 \times 59 = 2537$$

$$\phi(n) = (p-1) \times (q-1) = 42 \times 58 = 2436$$

حل المسألة الثالثة(3/5)

تابع للطلب الأول:

3. التحقق من قيمة e :

نأكد من شروط e: e عدد صحيح ,

$$\gcd(\phi(n), e) = 1; \quad 1 < e < \phi(n)$$

e= 13 عدد صحيح محقق

$$\gcd(2436,13) = 1; \quad 1 < e = 13 < 2436$$

جميع الشروط محققة ، و يمكن استخدام e = 13في هذه الخوارزمية .

فيكون المفتاح العام: $\Rightarrow K_{pub} = \{e, n\} = \{13,2537\}$

حل المسألة الثالثة(4/5)

تابع للطلب الأول:

3. عملية التشفير:

نلاحظ أن شرط التشفير M<n محقق حيث : 1520,111,802<2537

$$C_1 = M_1{}^e \bmod(n) = (1520)^{13} \bmod(2537) = 95 = 0095$$

$$C_2 = M_2{}^e \bmod(n) = (0111)^{13} \bmod(2537) = 1648$$

$$C_3 = M_3{}^e \bmod(n) = (0802)^{13} \bmod(2537) = 1410$$

$$\Rightarrow C = (C_1, C_2, C_3) = (0095,1648,1410)$$

- فيكون النص المشفرهو: **A95Q48OK**

حل المسألة الثالثة(5/5)

2 .في حال استخدم بلوك بطول 3 سيكون لدينا قيم النص الصريح:

M=(152001,110802)
- m1: PUB=152001
- m2: LIC=110802

يمكن أن نلاحظ أن شرط التشفير M<n غير محقق:

m1=152001>n=2537

m2=1110802>n=2537

بالتالي لا يمكن التشفير باستخدام هذه الخوارزمية

جَامعة
المَنارة
MANARA UNIVERSITY

نهاية الجلسة