1. أجب بصح أم خطأ مع التعليل

A. يمكن استخدام خوارزمية DH لتوزيع المفاتيح في تطبيق يستخدم خوارزمية RSA للتشفير

B. في خوارزمية DES ، لكل حلقة من الحلقات دخلان فقط

2. حل المسألة التالية:

لدينا خوارزمية RSA ذات القيم p=13,q=17 ، $e \in [3-7[$ و بفرض أن ترميز النص يكون اعتماداً على نظام للأساس 26 علماً أن الخانة الأكثر أهمية على اليمين و بطول كتلة محرفين، وتمثل الأحرف الأبجدية بأعداد صحيحة كالآتي: A=0, B=1, C=2.....Z=25.

المطلوب:

أوجد النص المشفر المحرفي المقابل للنص الصريح READ باستخدام الخوارزمية و الخوارزمية الآتية:

$$m \div 26^{T-1} = CH_1 \; rem \; m_1$$
$$m_1 \div 26^{T-2} = CH_2 \; rem \; m_2$$
$$\vdots$$
$$m_i \div 26^{0} = CH_T \; rem \; 0$$

حل نموذج A

1. أجب بصح أم خطأ مع التعليل:

A. خطأ. لأن RSA خوارزمية تشفير غير متناظر، والمفتاح الناتج عن DH هو مفتاح تشفير متناظر

B. خطأ. ثلاثة : Li-1, Ri-1, Ki (الجزء اليميني والجزء اليساري الناتجان عن الحلقة السابقة والكفتاح الجزئي للحلقة

2.حل المسألة :

ترميز النص:

M1	M2
RE	AD

$$m_1 = 17 \times 26^0 + 4 \times 26^1 = 121$$
$$m_2 = 0 \times 26^0 + 3 \times 26^1 = 78$$

M=(121,78)

نحسب المفتاح العام :

$$n = p \times q = 13 \times 17 = 221$$

$$\emptyset(n) = (p-1)(q-1) = (12)(16) = 192$$

اختيار e : e عدد صحيح، $1 < e < \emptyset(n)$ ، $\gcd(e,\emptyset(n)) = 1$ ، وحسب شرط المسألة يكون : e=5

فيكون المفتاح :$K_{PUB} = \{e,n\} = \{5,221\}$

نلاحظ أن النص المرمز يحقق شرط التشفير n>m1,m2

للتشفير نستخدم:

$$C = M^e mod\ n$$

$$C_1 = 121^5 mod 221 = 49$$

$$C_2 = 78^5 mod 221 = 91$$

فتكون C=(49,91)

حل نموذج A

$$49 \div 26^1 = 1 \text{ rem } 23 \Rightarrow CH1 = B$$
$$23 \div 26^0 = 23 \text{rem } 0 \Rightarrow CH2 = X$$

$$91 \div 26^1 = 3 \text{ rem } 13 \Rightarrow CH1 = D$$
$$13 \div 26^0 = 13 \text{rem } 0 \Rightarrow CH2 = N$$

فيكون النص المشفر:BXDN

جَامعة المَنارة
MANARA UNIVERSITY

نموذج B

1. أجب بصح أم خطأ مع التعليل

A.في خوارزمية DES ، تستخدم صناديق S-BOX لتخفيض طول السلسلة من 48 بت إلى 32 بت.

B.في خوارزمية DH ، تحسب قيمة المفتاح السري المشترك لكل مستخدم اعتماداً على قيمته السرية و قيمته الخاصة.

2. حل المسألة التالية:

خوارزمية RSA ذات القيم p=29,q=23 ، $e \in [2-4]$ وذلك بفرض أن النص يرمز اعتماداً على نظام للأساس 27 علماً أن الخانة الأكثر أهمية على اليمين و بطول كتلة محرفين، وتمثل الأحرف الأبجدية بأعداد صحيحة كالآتي : A=1, B=2, C=3...Z=26

المطلوب:

أوجد النص المشفر المحرفي المقابل للنص الصريح COME باستخدام الخوارزمية السابقة و الخوارزمية الآتية:

$$m \div 27^{T-1} = CH_1 \; rem \; m_1$$
$$m_1 \div 27^{T-2} = CH_2 \; rem \; m_2$$
$$\vdots$$
$$m_i \div 27^{0} = CH_T \; rem \; 0$$

جَامعة المَنارة
MANARA UNIVERSITY

نموذج B

2. حل المسألة التالية:

خوارزمية RSA ذات القيم p=29,q=23 ، $e \in [2-4]$ وذلك بفرض أن النص يرمز اعتماداً على نظام للأساس 27 علماً أن الخانة الأكثر أهمية على اليمين وبطول كتلة محرفين، وتمثل الأحرف الأبجدية بأعداد صحيحة كالآتي : A=1, B=2, C=3...Z=26

المطلوب:

أوجد النص المشفر المحرفي المقابل للنص الصريح COME باستخدام الخوارزمية السابقة والخوارزمية الآتية:

$$m \div 27^{T-1} = CH_1 \; rem \; m_1$$
$$m_1 \div 27^{T-2} = CH_2 \; rem \; m_2$$
$$\vdots$$
$$m_i \div 27^{0} = CH_T \; rem \; 0$$

حل نموذج B

1. أجب بصح أم خطأ مع التعليل:

A.صح . لنحصل على خرج يتناسب مع طول نصف الدخل (32 بت)

B.خطأ. اعتمادا على القيمة العامة الواصلة إليه من الطرف الآخر وقيمته السرية .

2.حل المسألة :

ترميز النص:

M1	M2
co	me

$$m_1 = 3 \times 27^0 + 15 \times 27^1 = 408$$
$$m_2 = 13 \times 27^0 + 5 \times 27^1 = 148$$

M=(408,184)

نحسب المفتاح العام :

$$n = p \times q = 23 \times 29 = 667$$

$$\emptyset(n) = (p-1)(q-1) = (22)(28) = 616$$

اختيار e : e عدد صحيح، $1 < e < \emptyset(n)$ ، $\gcd(e,\emptyset(n)) = 1$ ، وحسب شرط المسألة يكون : e=3

فيكون المفتاح :$K_{PUB} = \{e,n\} = \{3,667\}$

نلاحظ أن النص المرمز يحقق شرط التشفير n>m1,m2

للتشفير نستخدم:

$$C = M^e mod\ n$$

$$C_1 = 408^3 mod 667 = 37$$

$$C_2 = 148^3 mod 667 = 172$$

فتكون C=(37,172)

حل نموذج A

$$37 \div 27^1 = 2\,\text{rem}10 \Rightarrow \text{CH1} = \text{B}$$
$$10 \div 27^0 = 10\text{rem}\ 0 \Rightarrow \text{CH2} = \text{J}$$

$$172 \div 27^1 = 6\,\text{rem}\ 10 \Rightarrow \text{CH1} = \text{F}$$
$$10 \div 27^0 = 10\text{rem}\ 0 \Rightarrow \text{CH2} = \text{J}$$

فيكون النص المشفر:BJFJ