مسألة الكويز : 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:

1. شفر النص الصريح READ باستخدام الخوارزمية السابقة.

M1	M2
RE	AD

$$m1 = 17 \times 26^0 + 4 \times 26^1 = 121$$

$$m2 = 0 \times 26^0 + 3 \times 26^1 = 78$$

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:

$$\mathrm{C} = M^e mod\ n$$

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

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

فتكون C=(49,91)

2. أوجد المقابل المحرفي للنص المشفر في الطلب السابق باستخدام الخوارزمية الآتية:

$$\mathrm{m} \div 26^{\mathrm{T}-1} = \mathrm{CH}_1 \text{ rem } \mathrm{m}_1$$
$$\mathrm{m}_1 \div 26^{\mathrm{T}-2} = \mathrm{CH}_2 \text{ rem } \mathrm{m}_2$$
$$\vdots$$
$$\vdots$$
$$\mathrm{m}_{\mathrm{i}} \div 26^0 = \mathrm{CH}_{\mathrm{T}} \text{ rem } 0$$

حيثm هي البلوك العددي المشفر و T طول البلوك، m1,….mi بواقي عملية القسمة، ch1,….chT هي ناتج القسمة وتمثل القيم العددية للمحارف مع الأخذ بالحسبان أن الأعداد التي ليس لها محرف مقابل تترك كما هي.

للحصول على المقابل المحرفي نطبق الخوارزمية:

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

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

فيكون النص المشفر:BXDN