ملاحظة: رتب إجابتك في الدفتر حسب ترتيب ورود الأسئلة

١- اشرح تفصيلاً، مع ذكر كل الشروط على المقادير المستخدمة، كيفية استخدام نظام القوة لإنشاء مفتاح مشترك في شبكة تحوي 4 أشخاص.

٢- في نظام RSA ذي المفتاح المعلن (a,n) :

(أ) إذا علمت أن $(x,n)>1$ ، حيث x قيمة عددية لقالب من النص الواضح، فبين أن هذا يؤدي إلى كسر النظام.

(ب) أثبت أن معرفة تحليل n إلى عامليه الأوليين تكافئ معرفة $\varphi(n)$ ، حيث φ دالة أويلر.

٣- عرّف نظام الجمل مع ذكر جميع الشروط و المقادير السرية و المعلنة. بيّن دالة التعمية و دالة كشف المعمى.

٤- جد جميع الأخطاء التي تكتشفها و الأخطاء التي تصوبها الشفرة $C=\{001,111,100\}$.