الاختبار الفصلي الثاني ٤٤٢ ريض تطبيقات في الجبر الفصل الثاني ١٤٣٠-١٤٣١

ملحوظة: رتب إجابتك في الدفتر حسب ترتيب ورود الأسئلة

١- لنعتبر نظام القوة في التعمية:

(أ) هل مجموعة رموز النص الواضح تساوي مجموعة رموز النص المعمى؟ برر إجابتك.

(ب) إذا كا $p = 37$ و $a = 5$ ، فأحسب تعمية الكلمة ksu .

٢- (أ) عرِّف اللوغريتم المتقطع $\log_b a$ قياس n .

(ب) احسب $\log_2 12$ قياس 23 .

٣- في نظام RSA اثبت أن معرفة $\varphi(n)$ تكافئ معرفة تحليل n إلى عامليه الأوليين.

٤- لتكن C شفرة مسافتها d_C . أثبت أن C تصوب أي نمط خطأ u وزنه لا يزيد عن $\left\lfloor \frac{d_C - 1}{2} \right\rfloor$ ، و يوجد نمط خطأ u_0 وزنه $1+\left\lfloor \frac{d_C - 1}{2} \right\rfloor$ لا يمكن تصويبه.