الاختبار الفصلي الثاني 442 ريض الفصل الأول 1432-33

ملاحظة: رتب أجوبتك في الدفتر حسب ترتيب ورود الأسئلة.

1. صِف نظام RSA ، مبيناً المقادير المعلنة و السّرية. أثبت أن دالة كشف المعمى هي فعلاً معكوس دالة التعمية.
2. استخدم نظام الجمل و الأولي $p = 41$ لتعمية النص go ، إذا علمت أن 6 مولد للزمرة $\square_{41}^{*}$ و المفتاح السّري $a = 10$ و $k_1 = 2$ ، $k_2 = 7$ عددان مُختاران عشوائياً.
3. جد الأخطاء التي تكتشفها و التي تصوبها الشفرة $C = \{011,101,100\}$.
4. عرِّف مسافة الشفرة d_C لشفرة C ، ثم أثبت أن C تصوب أي نمط خطأ u لا يزيد وزنه عن $\left\lfloor \frac{d_C - 1}{2} \right\rfloor$. في حالة $d_C = 5$ أثبت وجود 10 أخطاء على الأقل لا يمكن للشفرة C تصويبها.