الاختبار الفصلي الثاني 442 ريض الفصل الأول 1431-32

ملاحظة: رتب اجابتك في الدفتر حسب ترتيب ورود الأسئلة.

1. صف نظام RSA مع ذكر المقادير السرية و المعلنة و إثبات أن دالة التعمية $e(x)$ قابلة للإقلاب تحت شرط معين. أكتب الشرط و بيّن أنه متوفر في أغلب الأحيان.

2. عرِّف المقصود باللوغاريتم المتقطع ثم أحسب $\log_3 12$ قياس 43 .

3. أحسب الأخطاء التي تكتشفها و تصوبها الشفرة $C = \{101,110,111\}$.

4. إذا كانت p إعتمادية قناة ثنائية متناظرة ، فأثبت إمكانية الفرض أن $\frac{1}{2} < p < 1$.