الاختبار الفصلي الثاني

تطبيقات الجبر (٤٤٤ ريض)

الفصل الأول ١٤٤٩ - ١٤٣٠ هـ

اسم الطالب :

الرقم الجامعي :

(١) اجب $(21)^{32} \pmod{65}$ و $(21)^{64} \pmod{65}$.

(٢) هل $21 \in \textcircled{1}_{65}$ ؟

(٣) إذا كان $a \in \mathcal{T}_n$ فأثبت أن $Epsp(a) \subseteq psp(a)$.
هل العكس صحيح ؟

(٤) ليكن $n>1$ عدداً صحيحاً. أثبت أن n عدد أولي إذا وفقط إذا كان $E(n) = \tau_n$.

(٥) إذا كان n عدداً مؤلفاً فأثبت أن $|E(n)| \leq \frac{\varphi(n)}{2}$.

(٦) اكتب خطوات خوارزمية سولوفي وستراسن لاختبار أولية العدد n .

(٧) بين خطوات توليد مفاتيح نظام RSA وخطوات عمليتي التعمية وكشف المعمى.

(٨) إذا كانت قوة التعمية a في نظام RSA هي $\frac{\varphi(n)}{2}+1$ فهل يستطيع عدوان قراءة الرسائل المرسلة من أحمد إلى بدر؟