ملاحظة: رتب إجابتك في الدفتر حسب ترتيب ورود الأسئلة.

1- في نظام القوة ،حيث $p=37$ إختر مفتاح مناسب a مع التبرير ، ثم أحسب تعمية النص put .

2- لنعتبر نظام RSA حيث المفتاح المعلن هو $(a,n)=(13,77)$.

أ- أحسب دالة كشف المعمى

ب- احسب احتمال كون القاسم المشترك الأكبر $(x,77)>1$ ، حيث x قيمه عددية من النص الواضح.

ت- بصورة عامة ، بيّن لماذا نختار n كحاصل ضرب أوليين مختلفين و ليس ثلاثة أوليات.

3. جد جميع الأخطاء التي تكتشفها و التي تصوبها الشفرة $C=\{101,111,011\}$.

4. لتكن C شفرة مسافتها d_C . أثبت أن C تكتشف أي نمط خطأ u وزنه لا يزيد عن d_C-1 و أنه يوجد نمط خطأ u_0 وزنه d_C لا يمكن تصويبه. بيّن من خلا مثال إمكانية وجود أنماط أخطاء وزنها يزيد عن d_C و تكتشفها الشفرة.