الاختبار النهائي
لتطبيقات الحاسب
الفصل الأول ١٤٤٩ - ١٤٤٠هـ

اسم الطالب :

الرقم الجامعي :

السؤال الأول :

(P) اعترضت الرسالة IEXXKFZKX المعمية بالنظام التآلفي وعلمت أن بداية النص الواضح هو Sure . جد مفتاح التعمية وأقرأ الرسالة.

(ب) لتكن كل من $e_1(x) \equiv ax+b \pmod m$ و $e_2(x) \equiv cx+d \pmod m$ دالة تعمية لنظام تآلفي.
جد $e_2(e_1(x))$. هل التابع دالة تعمية لنظام تآلفي ؟ وإذا كان كذلك فهل استخدامها يزيد من أمن النظام ؟ لماذا ؟

السؤال الثاني :

(أ) إذا تمكن عدوان من الحصول على مدخل مؤقت لعملية تعمية في نظام هيل فبين كيف يستطيع عدوان معرفة مفتاح التعمية ومن ثم كسر النظام.

(ب) بين كيفية تحويل النظام التبادلي إلى نظام هيل .

(٤.) اعترضت الرسالة ZINHYOC المعمية بنظام المفتاح الذاتي. إذا علمت أنه المفتاح الابتدائي هو k=11 فاقرأ الرسالة.

السؤال الثالث:

(أ) استقبل بدر الرسالة المعماة 42 بنظام RSA حيث $n = 209 = 11 \times 19$. جد جميع النصوص الواضحة الممكنة .

(ب) لنفرض أن لدى عدوان خوارزمية حدودية A لحساب الجذور التربيعية للعدد $n=pq$. بين كيف يتمكن عدوان من استخدام هذه الخوارزمية لمعرفة p و q ومن ثم كسر نظام رابن .

السؤال الرابع :

(P) ليكن $n=pq$ المفتاح المعلن في نظام RSA . إذا استخدمنا $\lambda=lcm(p-1, q-1)$ عوضًا عن $\varphi(n)$ فأثبت أننا نحصل على نظام تعمية يشبه نظام RSA .

(U) أراد أحمد وبدر انشاء مفتاح سري لاستخدامه في عملية تعمية . أعلنا عن العددين $p=43$ و $\alpha=3$ واختار أحمد العدد السري $x=8$ واختار بدر العدد السري $y=37$. ما هو المفتاح المشترك بينهما إذا استخدما خطة ديفي وهيلمان لتبادل المفاتيح ؟

(٢.) اعترض عدوان الرسالة $y \equiv x^a \pmod n$ أثناء محاولة أحمد ارسالها إلى بدر بنظام RSA. اختار عدوان عدد عشوائي $z \in \mathbb{Z}_n$ واستبدل رسالة أحمد بالرسالة $y_1 \equiv yz^a \pmod n$ ثم أرسل y_1 إلى بدر عوضاً عن y. عند استقبال بدر للرسالة y_1 قام بحساب $x_1 \equiv y_1^b \pmod n$ وأعاد x_1 إلى أحمد. بين كيف يتمكن عدوان من كسر النظام بعد اعتراضه x_1.

(10)