وظيفة الأمن الأولى

تطبيق نظام اتصال آمن وموثوق به، يجمع بين التشفير المتناظر وغير المتناظر والتوقيع الرقمي، وذلك لضمان السرية والأصالة والنزاهة للرسائل المتبادلة.

المتطلبات الأساسية للبيئة:

يجب تنفيذ جميع الخطوات على نظام تشغيل Seed Ubuntu أو أي بيئة Linux تحتوي على أداة OpenSSL.

المخرجات المطلوبة (يُقدَّم الملف كمجلد مضغوط واحد بصيغة .zip):

* ملف README.txt يحتوي على:

- اسم الطالب
- الرقم الجامعي
- التاريخ والوقت أثناء التنفيذ

* ملف commands.txt يتضمّن جميع الأوامر التي تم استخدامها أثناء التنفيذ.

* تقرير.

* صورتان (لقطتا شاشة) ضمن التقرير:

- s1.png: تُظهر توليد المفتاح المتماثل (Symmetric Key) أو محتوى الـ IV، مع ظهور الرقم الجامعي والوقت (Timestamp) بوضوح.
- s2.png: تُظهر توليد مفتاح RSA مع ظهور الوقت (Timestamp) بوضوح.

التسليم:

* موعد التسليم النهائي يوم الخميس 13/11/2025 الساعة 12:00 منتصف الليل.
* يتم التسليم على الروابط التالية:

✓ قسم الذكاء الصناعي:
https://docs.google.com/forms/d/e/1FAIpQLScH5x5zdxC5lsOitizjHlYkjD5Or716AUJPS9QeLonRyO_I1Q/viewform

✓ قسم الشبكات وفئات البرمجيات (يوم الثلاثاء):
https://forms.gle/nsxCs7yERRZMvutU8

✓ قسم فئات البرمجيات (يوم الخميس):
https://docs.google.com/forms/d/e/1FAIpQLSd3o4zvx-VXM43BO4UK2xIagIGpRDnB0k5uqHrnoD-AsAGKVw/viewform

سيناريو الوظيفة:

تقوم Alice بإرسال رسالة سرية إلى Bob. يجب أن تكون الرسالة مشفرة بطريقة هجينة وموقعة رقميًا

ملاحظة: الأوامر أدناه هي إرشادات. يجب على الطالب تنفيذها بشكل متسلسل وإدراج مخرجاتها في التقرير.

المرحلة الأولى: إعداد الأطراف (١ درجة)

* إنشاء مفاتيح Alice و Bob الخاصة والعامة.

المرحلة الثانية: الإرسال الآمن من Alice الى Bob (١,٥ + ١,٥ درجة)

افترض أن الرسالة الأصلية لـ Alice هي في ملف اسمه [your name and ID].txt

ملاحظة: استبدل your name and ID بالقيم الخاصة بك.

٣. التشفير الهجين: إرسال الرسالة من Alice الى Bob باستخدام التشفير الهجين (المتناظر وغير المتناظر معاً).

ملاحظة: يجب أن يحوي مفتاح التشفير المتناظر أو IV اسمك والرقم الجامعي الخاص بك.

٤. التوقيع الرقمي: توقيع الرسالة من قبل Alice.

المرحلة الثالثة: التحقق وفك التشفير (Bob) (١,٠ درجة)

الملف الذي يتلقاه Bob هو signed_and_encrypted.p7m.

٥. التحقق من التوقيع.

* يجب أن يظهر "Verification OK".

٦. فك التشفير.

التقرير يتضمن الأقسام التالية:

١. المقدمة والأهداف

* الأهداف الأمنية: تحديد المعايير الأمنية التي تم تحقيقها في المشروع.

٢. الإعداد والبنية التحتية

* توليد المفاتيح

٣. عملية الإرسال الآمن (Alice)

* التشفير الهجين: اشرح بإيجاز كيف جمعت بين التشفير المتناظر وغير المتناظر. اعرض الأمر المستخدم لتشفير الرسالة.

* التوقيع الرقمي: وضح كيف تم توقيع الرسالة المشفرة بمفتاح Alice. اعرض الأمر المستخدم للتوقيع.

٤. عملية الاستقبال والتحقق (Bob)

* التحقق: اعرض الأمر المستخدم للتحقق من التوقيع. الأهم: قم بتضمين لقطة شاشة (Screenshot) لنتيجة هذا الأمر التي تؤكد "Verification OK".

* فك التشفير: اعرض الأمر المستخدم لفك التشفير بمفتاح Bob. قم بعرض محتوى ملف original_message.txt الذي استعاده Bob.

يجب أن يكون التقرير منظمًا ومختصرًا، مع التركيز على المخرجات العملية للأوامر، ويجب أن لا يتجاوز ٤صفحات.