الجمهورية العربية السورية
جامعة دمشق
كلية الهندسة المعلوماتية
قسم هندسة البرمجيات ونظم المعلومات

اعداد الطالبة
أسماء محمد ياسر أبوكم

الفئة الثامنة
2025\11\13

المقدمة والاهداف

المقدمة

تزايدت الحاجة اليوم إلى تأمين المعلومات الرقمية بسبب انتشار الإنترنت وتبادل البيانات الحساسة بين الأفراد والمؤسسات. من أهم أساليب حماية البيانات :**التشفير الهجيني** الذي يجمع بين قوة التشفير المتناظر (AES) وسهولة توزيع المفاتيح باستخدام التشفير غير المتناظر(RSA) ، و**التوقيع الرقمي** الذي يضمن صحة الرسالة وعدم التلاعب بها.

في هذه التجربة، يقوم الطالب بمحاكاة إرسال رسالة سرية من Alice إلى Bob بحيث يتم تشفير الرسالة بطريقة هجينية مع التوقيع الرقمي، ومن ثم يقوم Bob بفك التشفير والتحقق من صحة الرسالة.

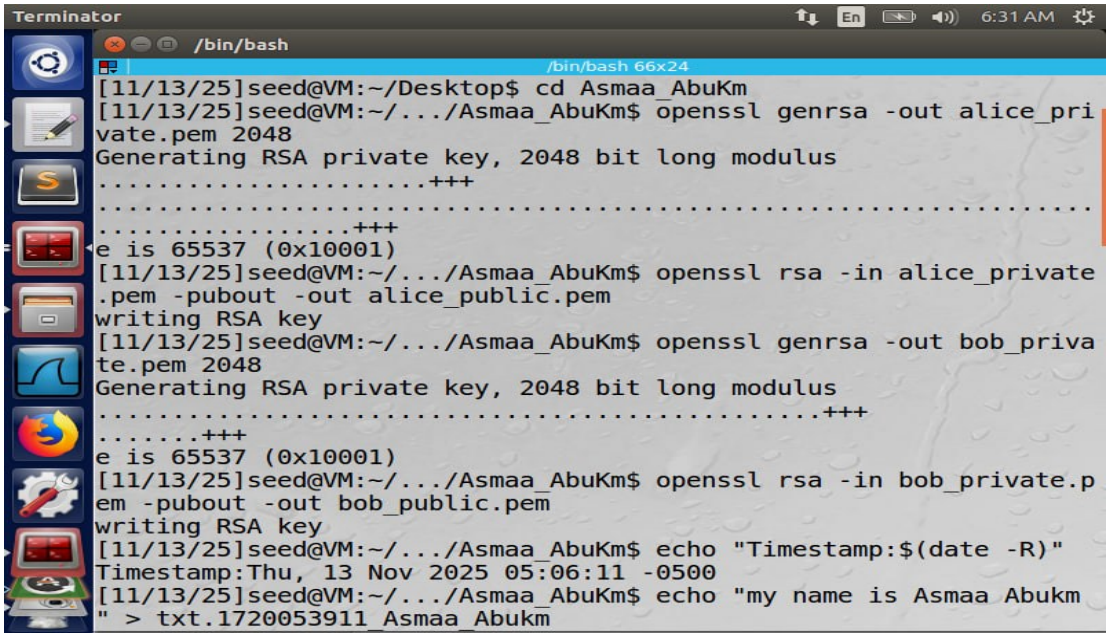
الاهداف

1. **توليد مفاتيح RSA** للأطراف المشاركة Alice و Bob لضمان التشفير غير المتناظر.
2. **تشفير رسالة نصية** باستخدام مفتاحAES-256 التشفير المتناظر.
3. **تشفير مفتاح AES** باستخدام مفتاح RSA العام للطرف المستقبل.
4. **إنشاء توقيع رقمي** للرسالة لضمان صحة البيانات وعدم التلاعب بها.
5. **تجميع الملفات المرسلة** في أرشيف واحد (p7m) لتسهيل النقل.
6. **استرجاع الرسالة وفك التشفير** بواسطة الطرف المستقبل والتحقق من التوقيع الرقمي.
7. **فهم الأخطاء الشائعة** أثناء التشفير/فك التشفير وحلها مثل تنسيق المفتاح،IV

الإلعداد والبنية التحتية

1. إنشاء المفاتيح (Alice و Bob)

- يتم إنشاء مفتاح RSA بطول 2048 بت لكل طرف.
- المفتاح العام يستخدم لتشفير الرسائل، والمفتاح الخاص لفك التشفير أو للتوقيع الرقمي.



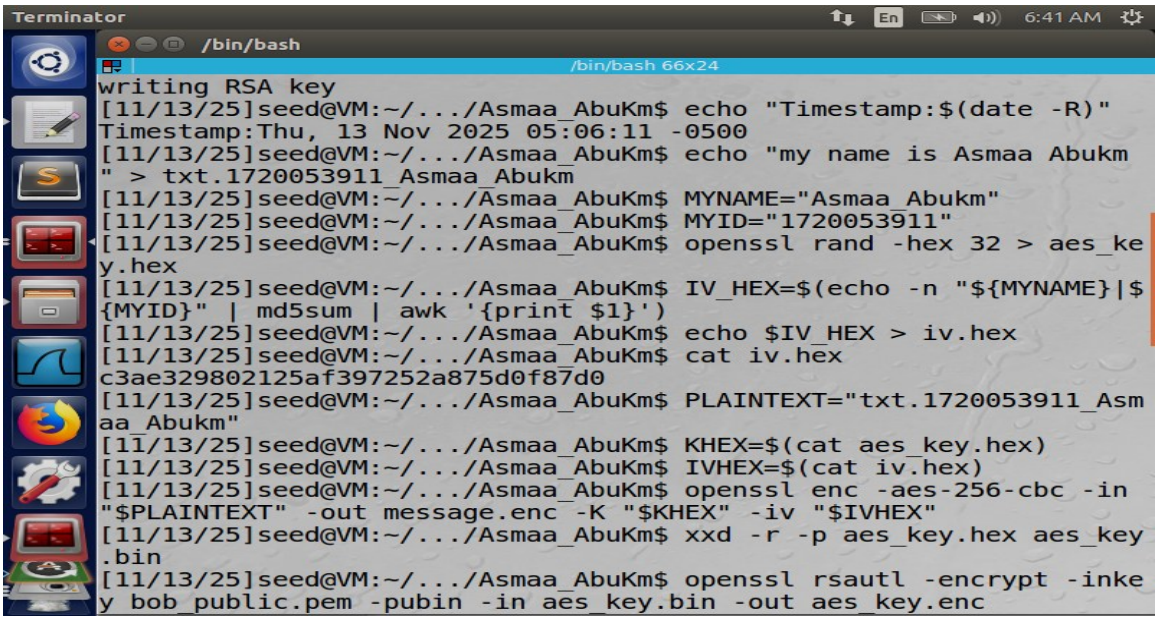
عملية الإلرسال الآمن (Alice)

خطوات التشفير الهجين:

1. **تشفير الرسالة بمفتاح AES-256 متناظر**
   - تم توليد مفتاح AES-256 عشوائي.(aes_key.hex / aes_key.bin)
   - تم إنشاء IV من دمج الاسم والرقم الجامعي
     (Asmaa_Abukm|1720053911)وحسابه باستخدام.MD5

2. تشفير مفتاح AES بمفتاح Bob العام (غير متناظر)

- الرسالة نفسها مشفرة AES للحصول على سرعة وكفاءة التشفير.
- مفتاح AES مشفر باستخدام RSA لضمان أن Bob فقط يستطيع فك التشفير



.

التوقيع الرقمي

- يتم حساب هاش SHA-256 للرسالة الأصلية.
- الهش يُوقّع باستخدام المفتاح الخاص لـ Alice لإنتاج التوقيع الرقمي.
- هذا يضمن سلامة الرسالة ومصادقة المرسل.

عملية االستقبال والتحقق (Bob)

فك أرشيف الرسالة

tar -xzf signed_and_encrypted.p7m

فك تشفير مفتاح AES بمفتاح Bob الخاص

openssl rsautl -decrypt -inkey bob_private.pem -in aes_key.enc -out aes_key.bin

تحويل المفتاح إلى صيغة hex لتجنب أخطاء openssl

xxd -p aes_key.bin > aes_key.hex

دمج الأسطر في سطر واحد إذا احتوى المفتاح على أكثر من سطر

tr -d '\n' < aes_key.hex > aes_key_clean.hex

mv aes_key_clean.hex aes_key.hex