



جامعة دمشق
كلية الهندسة المعلوماتية

وظيفة أمن نظم المعلومات

(السنة الخامسة قسم هندسة البرمجيات)

اعداد الطالبة:

لانا زهير ماخوش

المقدمة والأهداف:

*الأهداف الامنية

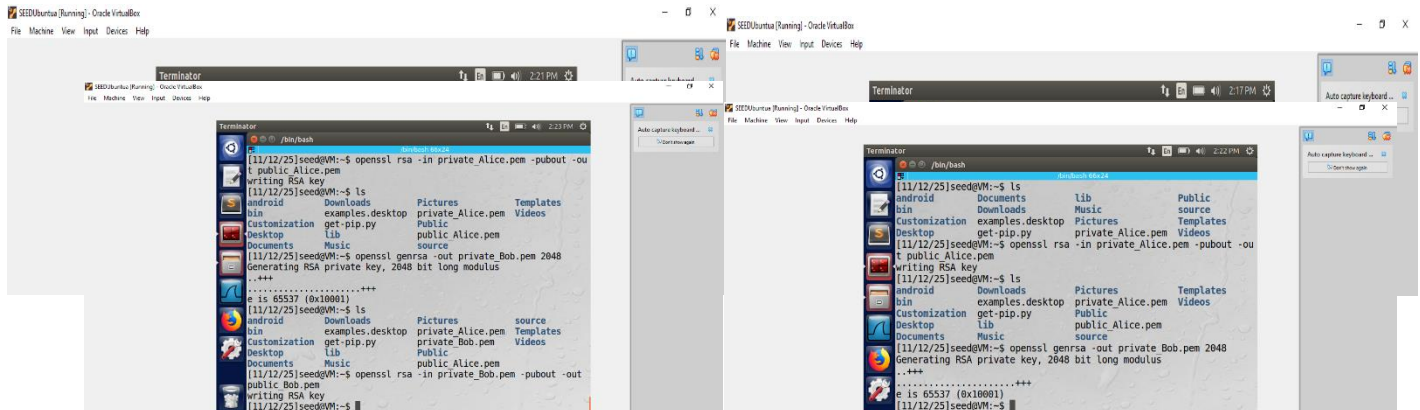
تم في هذا المشروع تنفيذ لإرسال رسالة مشفرة وموقعة رقمياً بين Alice و Bob باستخدام التشفير الهجين لضمان سرية الرسائل وسلامتها ومصداقية المرسل.

المعايير الأمنية المطبقة:

1. السرية (Confidentiality): حماية محتوى الرسالة باستخدام التشفير المتماثل AES-256.
2. السلامة (Integrity): التأكد من عدم تعديل الرسالة عبر التوقيع الرقمي.
3. المصادقية (Authenticity): التحقق من هوية المرسل عبر شهادة Alice.
4. عدم الإنكار (Non-repudiation): منع المرسل من إنكار إرسال الرسالة بعد توقيعها رقمياً.

الاعداد والبنية التحتية

المفاتيح العامة والخاصة ل Alice , Bob



عملية الارسال الامن من alice الى Bob

التشفير الهجين:

تم الجمع بين التشفير المتناظر والتشفير غير المتناظر لتحقيق السرية والأمان في نقل الرسالة. حيث استخدم AES-256-CBC لتشفير محتوى الرسالة بسرعة وكفاءة (التشفير المتناظر)، بينما تم تشفير مفتاح AES نفسه باستخدام المفتاح العام لـ Bob عبر RSA (التشفير غير المتناظر)، لضمان أن Bob وحده يستطيع فك تشفيره.

```
openssl enc -aes-256-cbc -in lanaMakhoush_1721122808.txt -out message.enc -K "$(cat  
"aes_key.hex)" -iv "$(cat iv.hex)
```

التوقيع الرقمي:

تم توقيع الرسالة المشفرة رقميًا باستخدام المفتاح الخاص بـ Alice للتحقق من هوية المرسل وضمان سلامة البيانات من أي تعديل أثناء النقل.

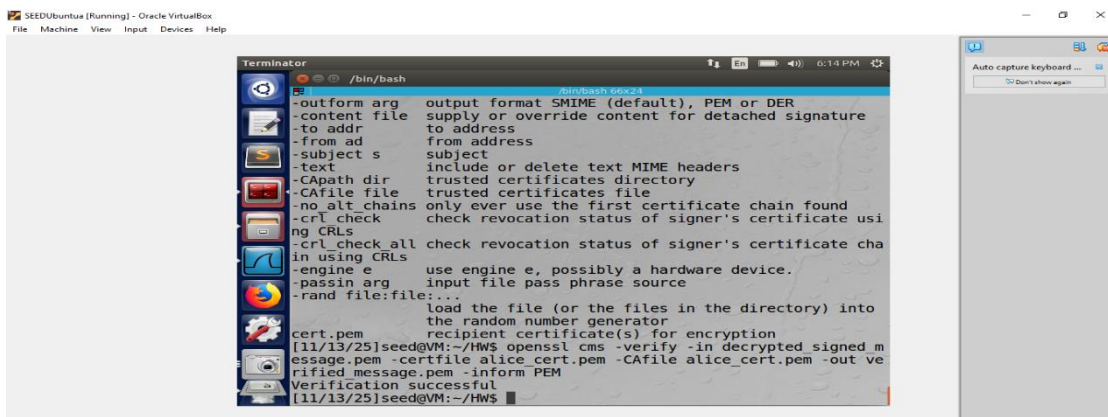
هذا التوقيع يمكن Bob لاحقًا من التحقق من أن الرسالة لم يتم العبث بها وأنها فعلاً صادرة من Alice.

```
openssl cms -sign -in lanaMakhoush_1721122808 -signer alice_cert.pem -inkey  
alice_private.pem -out decrypted_signed_message.pem -outform PEM -nodetach
```

عملية الاستقبال والتحقق:

التحقق:

```
openssl cms -sign -in lanaMakhoush_1721122808 -signer alice_cert.pem -inkey  
alice_private.pem -out decrypted_signed_message.pem -outform PEM -nodetach
```



فك التشفير:

\ openssl cms -decrypt

\ in signed_and_encrypted.p7m-

\ recip bob_cert.pem-

\ inkey bob_private.pem-

\ out decrypted_signed_message.pem-

inform PEM-

SEEDUbuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help

```
Terminator
/bin/bash
/bin/bash 66x24
-from ad      from address
-subject s    subject
-text        include or delete text MIME headers
-CApath dir   trusted certificates directory
-CAfile file  trusted certificates file
-no alt chains only ever use the first certificate chain found
-crl check    check revocation status of signer's certificate using CRLs
-crl check all check revocation status of signer's certificate chain using CRLs
-engine e     use engine e, possibly a hardware device.
-passin arg   input file pass phrase source
-rand file:file:...
              load the file (or the files in the directory) into
              the random number generator
cert.pem      recipient certificate(s) for encryption
[11/13/25]seed@VM:~/HW$ openssl cms -verify -in decrypted_signed_message.pem -certfile alice_cert.pem -CAfile alice_cert.pem -out original_Message.txt -inform PEM
Verification successful
[11/13/25]seed@VM:~/HW$ cat original_Message.txt
original message:FullName:anaMakhoush ,UniversityNumber:1721122808
[11/13/25]seed@VM:~/HW$
```

Auto capture keyboard ...
Don't show again

