

جامعة دمشق

كلية الهندسة المعلوماتية



# وظيفة أمن نظم المعلومات

(السنة الخامسة قسم هندسة البرمجيات)

إعداد الطالبة:

لانا زهير ماخوش

## المقدمة والأهداف:

### \*الأهداف الأمنية

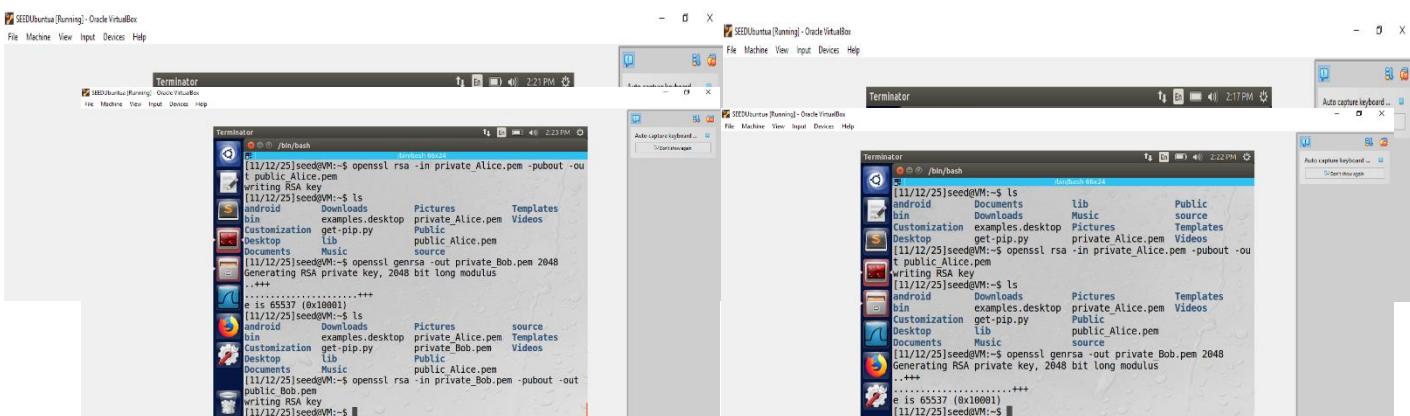
تم في هذا المشروع تفاصيل رسالة مشفرة وموثقة رقمياً بين Alice و Bob باستخدام التشفير الهجين لضمان سرية الرسائل وسلامتها ومصداقية المرسل.

### 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. المصداقية: Authenticity: التتحقق من هوية المرسل عبر شهادة Alice.
4. عدم الإنكار: Non-repudiation: منع المرسل من إنكار إرسال الرسالة بعد توقيعها رقمياً.

## الإعداد والبنية التحتية

### المفاتيح العامة والخاصة ل Alice , Bob



# عملية الارسال الامن من Bob الى alice

التشفير المجني:

تم الجمع بين التشفير المتناظر والتشفير غير المتناظر لتحقيق السرية والأمان في نقل الرسالة. حيث استخدم AES-256-CBC لتشفي رسالة بسرعة وكفاءة (التشفير المتناظر)، بينما تم تشفير مفتاح RSA نفسه باستخدام المفتاح العام لـ Bob (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 رقمياً باستخدام المفتاح الخاص بـ Alice للتحقق من هوية المرسل وضمان سلامة البيانات من أي تعديل أثناء النقل.

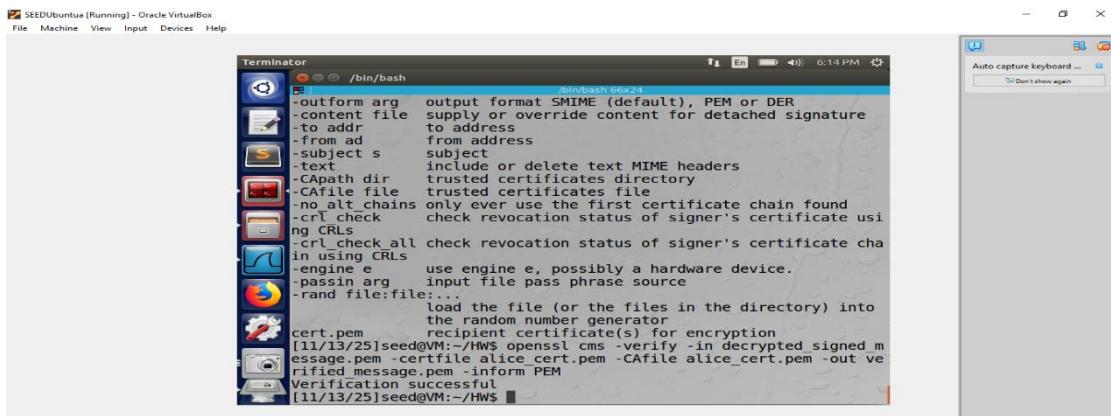
هذا التوقيع يمكن Bob لاحقاً من التتحقق من أن الرسالة لم يتم العبث بها وأنها فعلاً صادرة من Alice.

```
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-

The screenshot shows a Linux desktop environment with a terminal window open in a window titled "Terminator". The terminal window has a title bar showing "SEEDUbuntu [Running] - Oracle VirtualBox" and "File Machine View Input Devices Help". The main area of the terminal displays the following command-line session:

```
/bin/bash  
[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:lanaMakhoush ,UniversityNumber:172112280  
8  
[11/13/25]seed@VM:~/HW$
```

To the right of the terminal, there is a small message verification dialog box with the title "Auto capture keyboard ...". It contains a single line of text: "Don't show again".

