



JESUÏTES El Clot  
Escola del Clot

# **M011-SEGURETAT INFORMÀTICA i ALTA SEGURETAT**

*UF2- Seguretat Activa i Accés remot*

## **PRÀCTICA 4 : Criptografia publica i openssl**

**Curs:** 2018-19

**CFGs:** ASIX2

**Alumne :** Arnau Subirós Puigarnau

**Data :** 1-12-2018

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

1-12-2018

# **PRACTICA 4 :**

## **Criptografia publica i openssl i criptografia pública**

### **PART TEÒRICA**

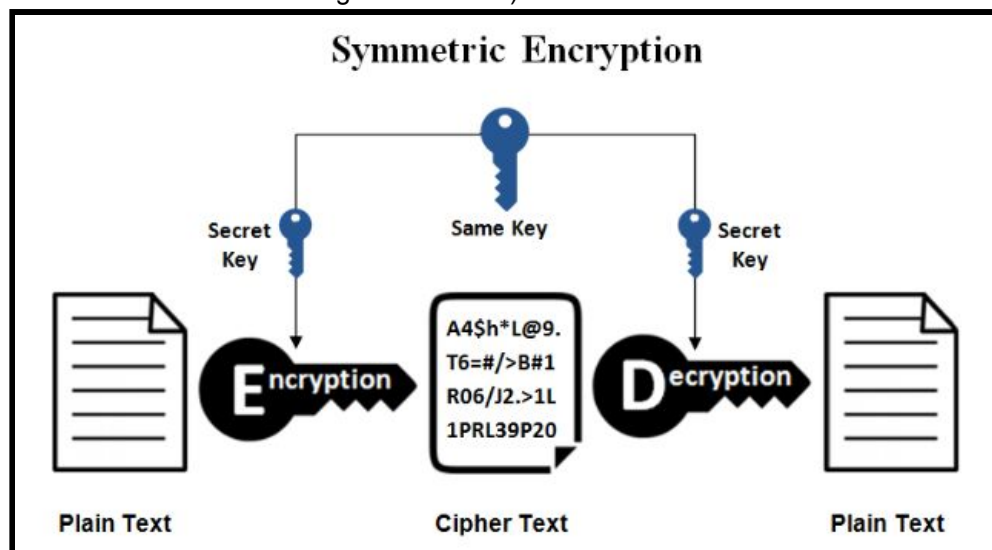
**Qüestions prèvies:**

**Responen a les següents qüestions de manera breu, amb les vostres paraules, raonant la resposta i posant referències de on heu extret la informació:**

#### **1. Que és la criptografia de clau privada?**

La criptografia de clau privada ( o criptografia simètrica) és una forma de criptografia que s'utilitza una clau secreta senzilla tan per xifrar com desxifrar el missatge.

- Per utilitzar aquesta criptografia, previament el receptor i el emisor han de conèixer la clau ( o s'haurien d'enviar un missatge amb la clau)



**Nom i Cognoms**

Arnau Subirós Puigarnau

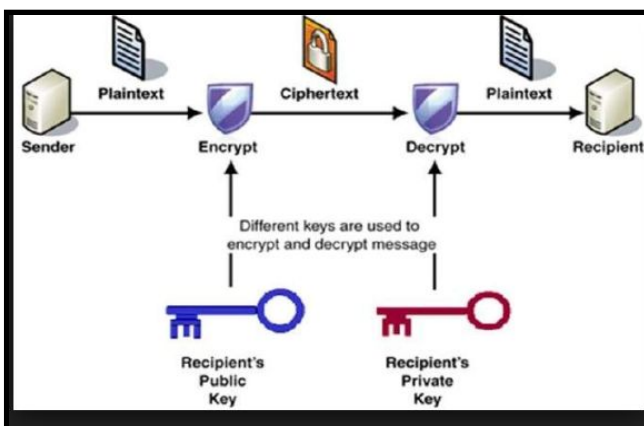
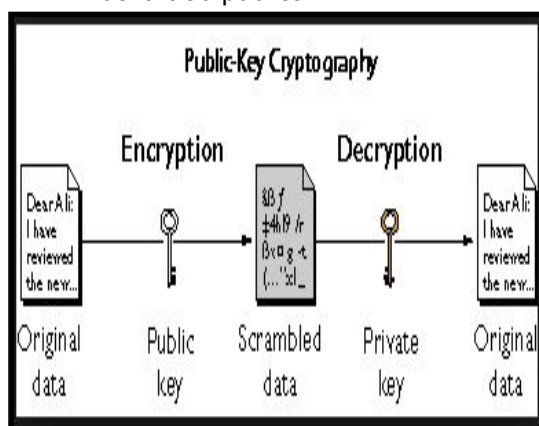
**Data**

1-12-2018

## 2. Que és la criptografia de clau pública?

La criptografia de clau pública ( o criptografia asimètrica) és una forma de criptografia en la qual la clau utilitzada per xifrar un missatge difereix de la clau utilitzada per desxifrar-lo

- Un usuari té un parell de claus una clau pública i una clau privada.
- La clau privada es manté secreta
- La clau pública es pot dir a tothom.
- Els missatges nous s'han de xifrar amb la clau pública del receptor
- Només es poden desxifrar amb la seva clau privada corresponent.
- Les claus es relacionen matemàticament, però la clau privada a la pràctica no es pot obtenir a partir de la clau pública



## 3. Qué és el tunneling quan parlem de seguretat informàtica?

La tècnica de tunneling consisteix a encapsular un protocol de xarxa sobre un altre (protocol de xarxa encapsulador) creant un túnel dins d'una xarxa de computadores.

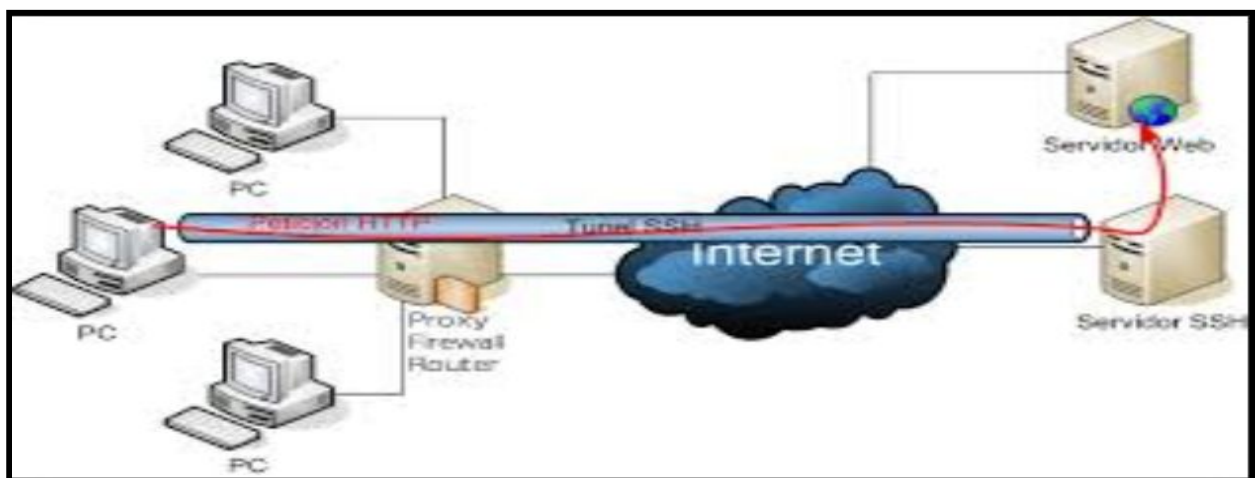
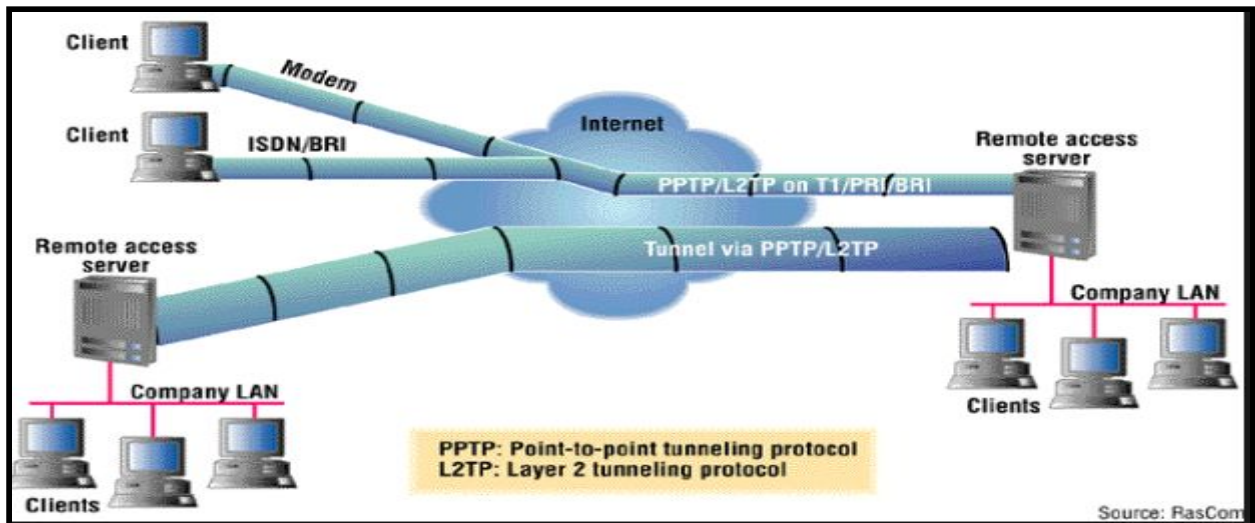
- L'establiment d'aquest túnel s'implementa incloent una PDU determinada dins d'una altra PDU amb l'objectiu de transmetre-la des d'un extrem a l'altre del túnel sense que sigui necessària una interpretació intermèdia de la PDU encapsulada. D'aquesta manera s'encaminen els paquets de dades sobre nodes intermedis que són incapaços de veure en clar el contingut d'aquests paquets.
- El túnel queda definit pels punts extrems i el protocol de comunicació emprat, que entre uns altres, podria ser SSH..
- Per regla general, aquests protocols s'utilitzen per enviar dades de xarxa privada a través d'una xarxa pública, sovint quan es crea una xarxa privada virtual (VPN); no obstant això, també es poden usar per augmentar la seguretat de les dades sense xifrar que s'envien a través d'una xarxa pública. Existeixen diversos protocols de tunelització coneguts, com Secure Shell (SSH), PPTP, IPsec, GRE47, L2TP, etc. i cadascun d'ells està adaptat a un propòsit específic.

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

1-12-2018



#### 4. Què afegeix el sistema PGP respecte l'enciptació pública en openssl?

PGP, (o Pretty Good Privacy) utilitza una combinació de mètodes d'enciptació per mantenir les dades segures. Tals com:

- hashing
- compressió de dades
- criptografia de clau simètrica
- criptografia de clau pública

per mantenir les dades segures

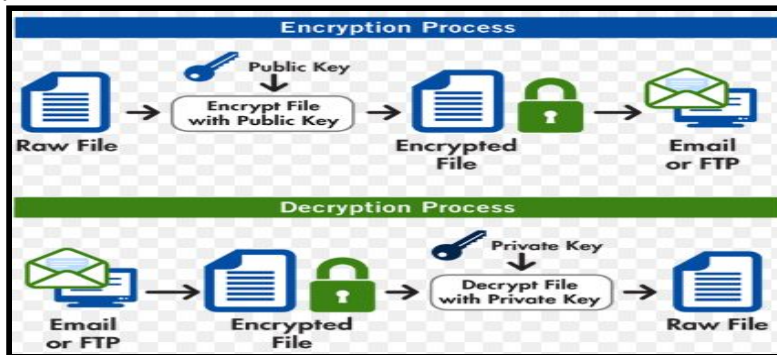
**Nom i Cognoms**

Arnau Subirós Puigarnau

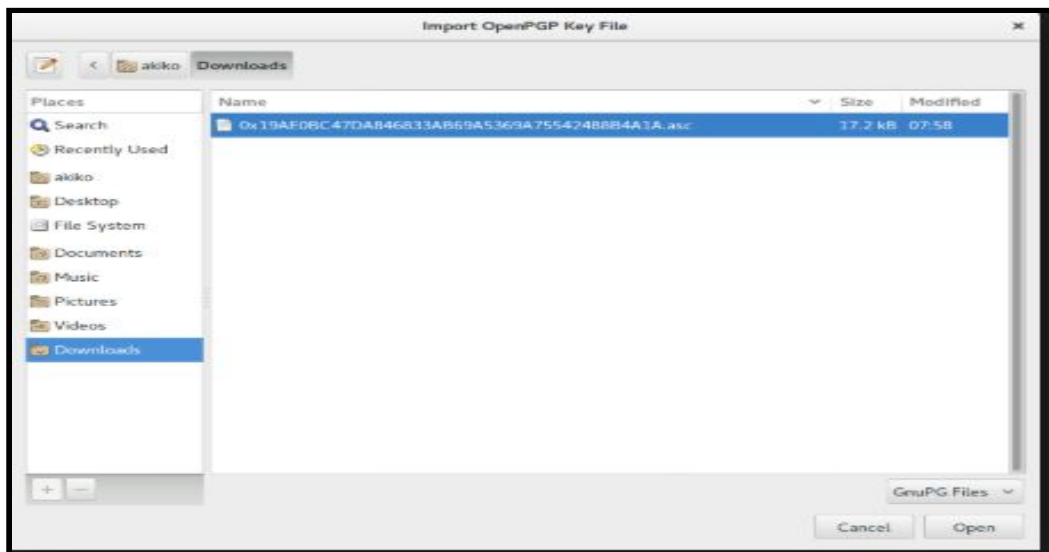
**Data**

1-12-2018

Aquest procés es pot utilitzar per encriptar arxius de text, correus electrònics, arxius de dades, directoris i particions de disc.



**Exemple : OpenPGP**

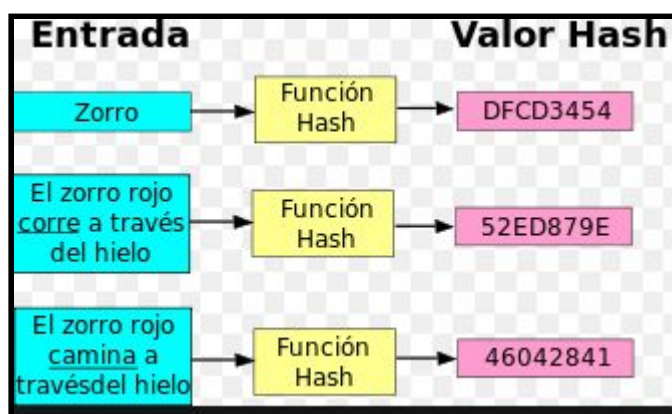


**5. Que és el hasing? Per a que s'utilitza el hashing? Que és el MD5?Mostra un exemple d'una generació de hashing online en MD5.**

**HASHING** : És un algorisme matemàtic que transforma qualsevol bloc arbitrari de dades en una nova sèrie de caràcters amb una longitud fixa. Independentment de la longitud de les dades d'entrada, el valor hash de sortida tindrà sempre la mateixa longitud.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	1-12-2018

- La forma més comuna del **hash** té a veure amb les contrasenyes. Per exemple, si alguna vegada oblides la teva contrasenya d'algun servei en línia, probablement s'hagi de fer un reset. Quan es restableix una contrasenya, en general no es rep una clau en text pla. Això és a causa que els servei en línia no emmagatzemen les contrasenyes en text pla, sinó que les emmagatzemen sota el valor hash de la contrasenya. De fet, el servei (tret que s'utilitza una contrasenya massa simple, que faci que el valor hash sigui àmpliament conegut) no té idea de quin és la contrasenya real.



**MD5** : És un algorisme que proporciona un codi associat a un arxiu o un text concret.. D'aquesta forma, a l'hora de descarregar un determinat arxiu, com pot ser un instal·lador, el codi generat per l'algorisme, també anomenat hash, ve "unit" a l'arxiu.

<https://passwordsgenerator.net/md5-hash-generator/>

**MD5 Hash Generator**

This online tool allows you to generate the MD5 hash of any string. The MD5 hash can not be decrypted if the text you entered is complicated enough.

Enter your text below:

Hola com estàs

Generate Clear All Base64 Decode ☐ Treat each line as a separate string

MD5 Hash of your string:  
BFF416B3D7345A4F76951095B01248BB

**TEXT** : Hola com estàs

**MD5 Hash** :BFF416B3D7345A4F76951095B01248BB

**Nom i Cognoms**

Arnau Subirós Puigarnau

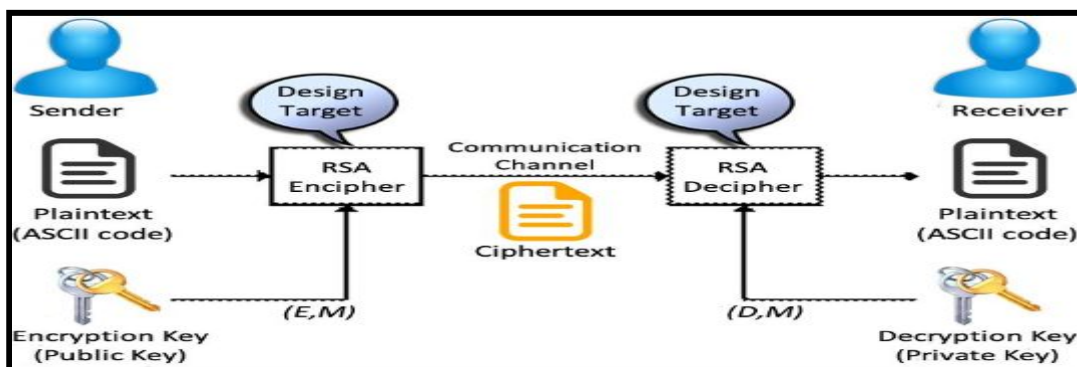
**Data**

1-12-2018

## 6. Que és RSA?

**RSA** és un algorisme de xifrat de clau pública que li permet a l'usuari conservar la confidencialitat de la informació quan és transmesa o compartida amb altres usuaris. Conèixer que consisteix és la millor opció per utilitzar-ho de forma adequada i salvaguardar la informació més sensible.

La fortalesa de l'algorisme RSA es basa en la complexitat de càlcul que té trobar els dos factors primers d'un nombre compost molt gran. L'operació inversa d'aquest problema, és a dir multiplicar dos nombres primers grans, és una operació poc costosa computacionalment i que es pot realitzar ràpidament, però en sentit contrari, és a dir trobar els factors primers d'un nombre és una operació que a mesura que s'incrementa la grandària del nombre augmenta els requeriments de maquinari per al seu càlcul a més d'augmentar el temps requerit per al seu càlcul.





Nom i Cognoms	Data
Arnau Subirós Puigarnau	1-12-2018

## 7. Que és IDEA en termes de algorismes de seguretat?

El **International Data Encryption Algorithm( IDEA)** va ser desenvolupat a Alemanya a principis dels noranta per James L. Massey i Xuejia Lai.

- Sistema criptogràfic simètric que treballa amb blocs de text de 64 bits. operan una clau de 128 bits , com es cas de DES que utilitza el mateix algorisme per xifra que desxifrar
- IDEA és un algorisme opcional en l'estàndard OpenPGP
- L'algorisme de descriptació és molt semblat al d'enciptació, per la qual cosa resulta molt fàcil i ràpid de programar, i fins ara no ha estat trencat mai, aportant la seva longitud de clau una seguretat forta davant els atacs per força bruta (prova i assaig o diccionaris).
- Aquest algorisme és de lliure difusió i no està sotmès a cap tipus de restriccions o permisos nacionals, per la qual cosa s'ha difós àmpliamente, utilitzant-se en sistemes com UNIX i en programes de xifrat de correu com PGP.
- IDEA és un algorisme bastant segur, i fins ara s'ha mostrat resistent a multitud d'atacs, entre ells el cripto-anàlisis diferencial. No presenta claus debiles, i la seva longitud de clau fa impossible en la practica un atac per la força bruta. Com ocorre amb tots els algorismes simèrics de xifrat per blocs, IDEA es basa en els conceptes de confusió i difusió , fent ús de les següents operacions elementals (totes elles faciles d'implementar):
  - XOR
  - Suma mòdul 2 ( base 16)
  - Producte mòdul 2 ( base 16)+1
- L'algorisme IDEA consta de 8 rondes. Es divideix el bloc X a codicar, de 64 bits, en quatre parts X1, X2, X3 i X4 de 16 bits denominades Zi a cadascuna de les 52 subclaves de 16 bits que anem a necessitar. Les operacions que duren a terme en cada ronda són les següents:

1. Multiplicar X1 per Z1.
2. Sumar X2 amb Z2.
3. Sumar X3 amb Z3.
4. Multiplicar X4 per Z4.
5. Fer un XOR entre els resultats del pas 1 i el pas 3.
6. Fer un XOR entre els resultats del pas 2 i el pas 4.
7. Multiplicar el resultat del pas 5 per Z5.
8. Sumar els resultats dels passos 6 i 7.
9. Multiplicar el resultat del pas 8 per Z6.
10. Sumar els resultats dels passos 7 i 9.
11. Fer un XOR entre els resultats dels passos 1 i 9.
12. Fer un XOR entre els resultats dels passos 3 i 9.



**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

1-12-2018

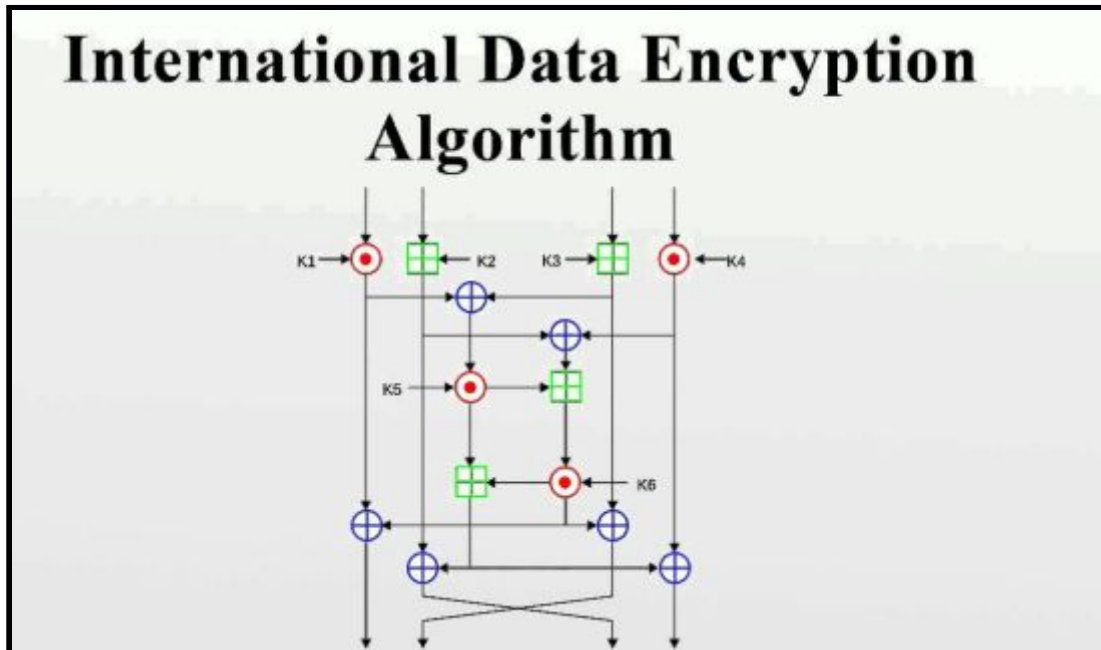
13. Fer un XOR entre els resultats dels passos 2 i 10.

14. Fer un XOR entre els resultats dels passos 4 i 10.

La sortida de cada iteracion seran els quatre sub-blocs obtinguts en els passos 11, 12, 13 i 14, que seran l'entrada del següent cicle, en el qual emprarem les següents sis subclaves, fins a un total de 48. Al final de tot intercanviarem els dos blocs centrals (en realitat amb això desfem l'intercanvi que duem a terme en els passos 12 i 13). Después de l'octava iteracion, es realitza la següent transformacion:

1. Multiplicar X1 per Z49.
2. Sumar X2 amb Z50.
3. Sumar X3 amb Z51.
4. Multiplicar X4 per Z52.

- Les primeres vuit subclaus es calculen dividint la clau d'entrada en blocs de 16 bits.
- Les següents vuit es calculen rotant la clau d'entrada 25 bits a l'esquerra i tornant a dividir-la, i así successivament.
- Les subclaus necessàries per desxifrar s'obtenen canviant d'ordre les Zi i calculant les seves inverses per a la suma o la multiplicació ja que  $216 + 1$  és un número primer, *mai podrem obtenir zero com a producte de dos numeros, per la qual cosa no necessitem representar aquest valor.*
- Quan estiguem calculant productes, utilitzarem el zero per expressar el numero 216 un un de seguit de 16 zeros. Aquesta representacion és coherent posat que els registres que s'empren internament en l'algorisme posseeixen unicament 16 bits.



**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

1-12-2018

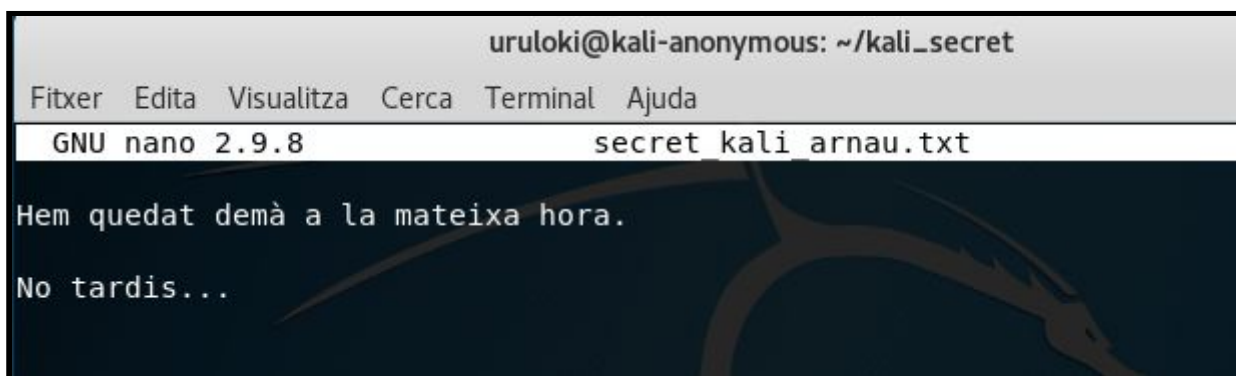
## PART PRÀCTICA

**Aquest treball es realitza per parelles. L'objectiu de la pràctica és reproduir el sistema d'encryptació pública que es va mostrar a classe. Per realitzar aquesta pràctica realitzeu captures de pantalla de tots els passos, explicant amb detall els passos que heu seguit.**

**Passos a seguir (referència: <https://gist.github.com/crazybyte/4142975>)**

**1-** Els dos membres crea cadascú un missatge en text pla, que serà el missatge per encriptar i només podrà llegir l'altre membre. Al arxiu digueu-li **missatge\_nom\_parella.txt**

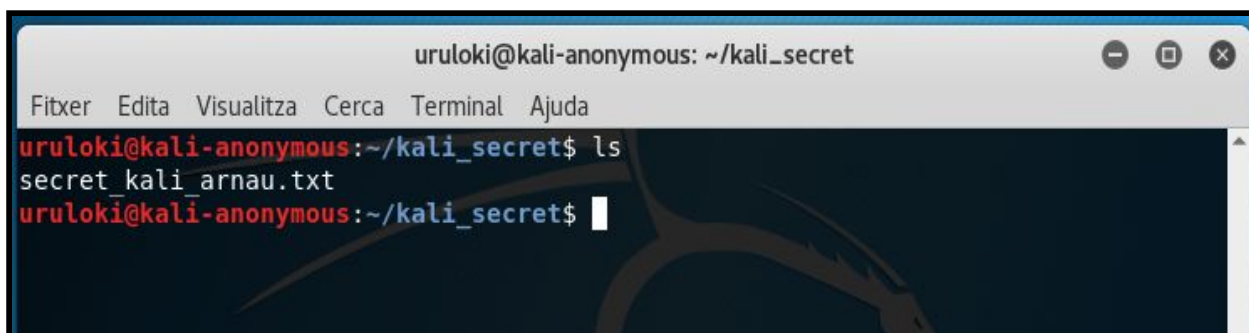
*Missatge sense encriptar de l'USUARI 1*



```
uruloki@kali-anonymous: ~/kali_secret
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
GNU nano 2.9.8      secret_kali_arnau.txt

Hem quedat demà a la mateixa hora.

No tardis...
```



```
uruloki@kali-anonymous: ~/kali_secret
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
uruloki@kali-anonymous:~/kali_secret$ ls
secret_kali_arnau.txt
uruloki@kali-anonymous:~/kali_secret$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

1-12-2018

*Missatge sense encriptar de l'USUARI 2*

```
arsupu@ubuntu-asix2: ~/secret
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
GNU nano 2.9.3      secret_ubuntu_arnau.txt

No pateixis...

Arribarè tal com varem quedar...

Portarè el material assignat.█
```

```
arsupu@ubuntu-asix2: ~/secret
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
arsupu@ubuntu-asix2:~/secret$ ls
secret_ubuntu_arnau.txt
arsupu@ubuntu-asix2:~/secret$ █
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

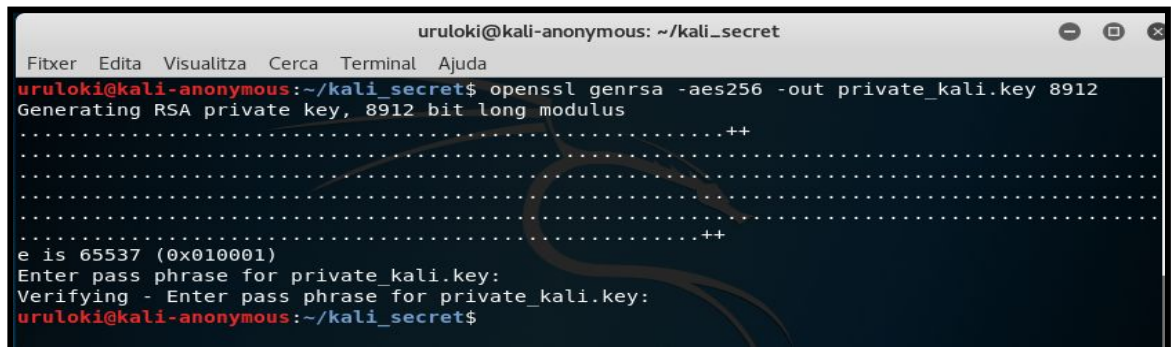
**Data**

1-12-2018

2- Cada membre, en la seva màquina, crea un parell de claus amb l'eina openssl. Primer s'ha de crear la clau privada amb el següent comandament:

**openssl genrsa -aes256 -out private\_nom.key 8912**

*Clau privada de l'USUARI 1*



```
uruloki@kali-anonymous: ~/kali_secret
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
uruloki@kali-anonymous:~/kali_secret$ openssl genrsa -aes256 -out private_kali.key 8912
Generating RSA private key, 8912 bit long modulus
.....++
.....++
e is 65537 (0x010001)
Enter pass phrase for private_kali.key:
Verifying - Enter pass phrase for private_kali.key:
uruloki@kali-anonymous:~/kali_secret$
```

*Clau privada de l'USUARI 2*



```
arsupu@ubuntu-asix2: ~/secret
Fitxer  Edita  Visualitza  Cerca  Terminal  Ajuda
arsupu@ubuntu-asix2:~/secret$ openssl genrsa -aes256 -out private_ubuntu.key 8912
Generating RSA private key, 8912 bit long modulus
.....++
.....++
e is 65537 (0x010001)
Enter pass phrase for private_ubuntu.key:
Verifying - Enter pass phrase for private_ubuntu.key:
arsupu@ubuntu-asix2:~/secret$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

1-12-2018

Després cada membre crea la clau pública:

**openssl rsa -in private\_*nom*.key -pubout -out public\_*nom*.key**

*Clau pública de l' 'USUARI 1*

```
uruloki@kali-anonymous: ~/kali_secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~/kali_secret$ openssl rsa -in private_kali.key -pubout -out public_kali.key
Enter pass phrase for private_kali.key:
writing RSA key
uruloki@kali-anonymous:~/kali_secret$
```

*USUARI 1: podem veure l'arxiu de text, la clau privada i la clau pública*

```
uruloki@kali-anonymous: ~/kali_secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~/kali_secret$ ls
private_kali.key  public_kali.key  secret_kali_arnau.txt
uruloki@kali-anonymous:~/kali_secret$
```

*Clau pública de l' 'USUARI 2*

```
arsupu@ubuntu-asix2: ~/secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/secret$ openssl rsa -in private_ubuntu.key -pubout -out public_ubuntu.key
Enter pass phrase for private_ubuntu.key:
writing RSA key
arsupu@ubuntu-asix2:~/secret$
```

*USUARI 2: podem veure l'arxiu de text, la clau privada i la clau pública*

```
arsupu@ubuntu-asix2: ~/secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/secret$ ls
private_ubuntu.key  public_ubuntu.key  secret_ubuntu_arnau.txt
arsupu@ubuntu-asix2:~/secret$
```



## Nom i Cognoms

Arnau Subirós Puigarnau

## Data

1-12-2018

**3- Distribució de les claus públiques.** Cada membre entrega a l'altre membre de la parella una còpia de la seva clau pública.

**USUARI 1:** copia la clau pública **public\_ubuntu.key** del usuari 2 al USB

```
uruloki@kali-anonymous: /media/uruloki/XAMPP_USB/OPENSSL_Public_Key
txer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous: /media/uruloki/XAMPP_USB/OPENSSL_Public_Key$ cp public_ubuntu.key ~/kali_secret/public_ubuntu.key
```

**USUARI 1:** copia la clau pública **public\_ubuntu.key** del usuari 2 a **~/kali\_secret**

```
uruloki@kali-anonymous: ~/kali_secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~/kali_secret$ ls
private_kali.key public_kali.key secret_kali_arnau.txt
uruloki@kali-anonymous:~/kali_secret$ ls
private_kali.key public_kali.key public_ubuntu.key secret_kali_arnau.txt
uruloki@kali-anonymous:~/kali_secret$
```

**USUARI 2:** copia la clau pública **public\_kali** del usuari 1 al USB

```
arsupu@ubuntu-asix2: /media/arsupu/XAMPP_USB/OPENSSL_Public_Key
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2: /media/arsupu/XAMPP_USB/OPENSSL_Public_Key$ ls
public_kali.key public_ubuntu.key
arsupu@ubuntu-asix2: /media/arsupu/XAMPP_USB/OPENSSL_Public_Key$ cp public_kali.key ~/secret/public.kali.key
arsupu@ubuntu-asix2: /media/arsupu/XAMPP_USB/OPENSSL_Public_Key$
```

**USUARI 2:** copia la clau pública **public\_kali** del usuari 1 a **~/secret**

```
arsupu@ubuntu-asix2: ~/secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/secret$ ls
private_ubuntu.key public_ubuntu.key secret_ubuntu_arnau.txt
arsupu@ubuntu-asix2:~/secret$ ls
private_ubuntu.key public.kali.key public_ubuntu.key secret_ubuntu_arnau.txt
arsupu@ubuntu-asix2:~/secret$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

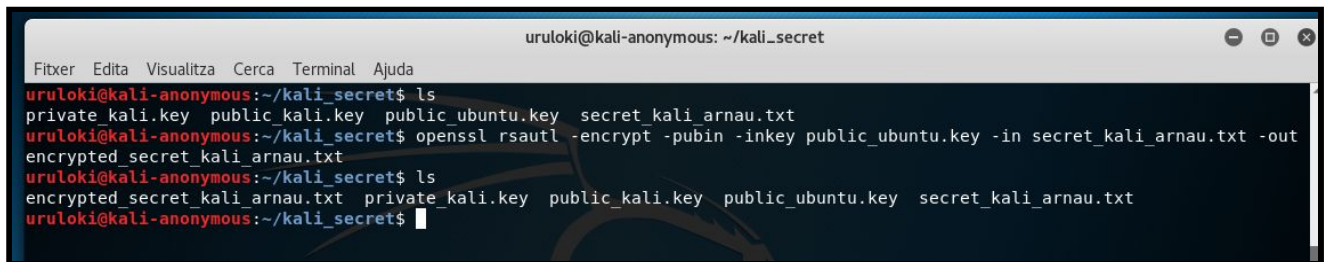
**Data**

1-12-2018

4- Cada membre encripta el missatge de text de la seva màquina. Per fer-ho utilitzeu el comandament següent:

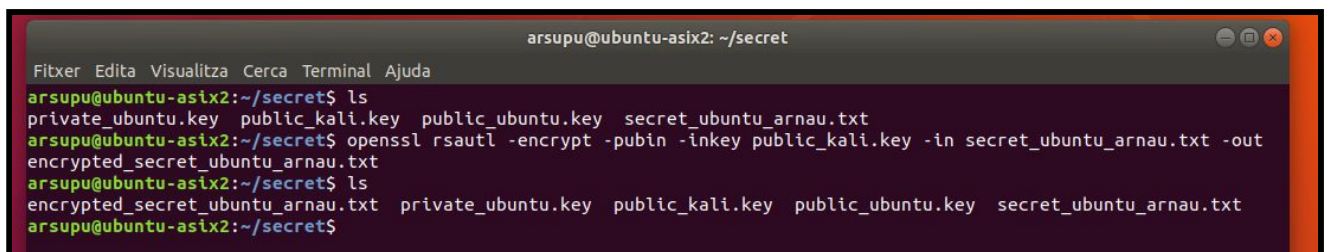
**openssl rsautl -encrypt -pubin -inkey public\_nom\_parella.key -in missatge\_nom\_parella.txt -out encrypted\_nom\_parella.txt**

**USUARI 1:** encripta el seu missatge **secret\_kali\_arnau.txt** amb la clau pública del usuari 2 **public.ubuntu.key** i el missatge encriptat guardat a **encrypted\_secret\_kali\_arnau.txt**



```
uruloki@kali-anonymous: ~/kali_secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~/kali_secret$ ls
private_kali.key public_kali.key public_ubuntu.key secret_kali_arnau.txt
uruloki@kali-anonymous:~/kali_secret$ openssl rsautl -encrypt -pubin -inkey public_ubuntu.key -in secret_kali_arnau.txt -out encrypted_secret_kali_arnau.txt
uruloki@kali-anonymous:~/kali_secret$ ls
encrypted_secret_kali_arnau.txt private_kali.key public_kali.key public_ubuntu.key secret_kali_arnau.txt
uruloki@kali-anonymous:~/kali_secret$
```

**USUARI 2:** encripta el seu missatge **secret\_ubuntu\_arnau.txt** amb la clau pública del usuari 1 **public.kalikey** i el missatge encriptat guardat a **encrypted\_secret\_ubuntu\_arnau.txt**



```
arsupu@ubuntu-asix2: ~/secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/secret$ ls
private_ubuntu.key public_kali.key public_ubuntu.key secret_ubuntu_arnau.txt
arsupu@ubuntu-asix2:~/secret$ openssl rsautl -encrypt -pubin -inkey public_kali.key -in secret_ubuntu_arnau.txt -out encrypted_secret_ubuntu_arnau.txt
arsupu@ubuntu-asix2:~/secret$ ls
encrypted_secret_ubuntu_arnau.txt private_ubuntu.key public_kali.key public_ubuntu.key secret_ubuntu_arnau.txt
arsupu@ubuntu-asix2:~/secret$
```





**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

1-12-2018

**6- Envieu el missatge encriptat a la parella.****USUARI 1:** copia el missatge encriptat **encrypted\_secret\_ubuntu\_arnau.txt** del USB a ~/kali\_secret

```
uruloki@kali-anonymous: /media/uruloki/XAMPP_USB/OPENSSL_Public_Key
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:/media/uruloki/XAMPP_USB/OPENSSL_Public_Key$ ls
encrypted_secret_kali_arnau.txt  encrypted_secret_ubuntu_arnau.txt  public_kali.key  public_ubuntu.key
uruloki@kali-anonymous:/media/uruloki/XAMPP_USB/OPENSSL_Public_Key$ cp encrypted_secret_ubuntu_arnau.txt ~/kali_secret
uruloki@kali-anonymous:/media/uruloki/XAMPP_USB/OPENSSL_Public_Key$
```

```
uruloki@kali-anonymous: ~/kali_secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~/kali_secret$ ls
encrypted_secret_kali_arnau.txt  private_kali.key  public_ubuntu.key
encrypted_secret_ubuntu_arnau.txt  public_kali.key  secret_kali_arnau.txt
uruloki@kali-anonymous:~/kali_secret$
```

**USUARI 2:** copia el missatge encriptat **encrypted\_secret\_kali\_arnau.txt** del USB a ~/secret

```
arsupu@ubuntu-asix2: /media/arsupu/XAMPP_USB/OPENSSL_Public_Key
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:/media/arsupu/XAMPP_USB/OPENSSL_Public_Key$ ls
encrypted_secret_kali_arnau.txt  encrypted_secret_ubuntu_arnau.txt  public_kali.key  public_ubuntu.key
arsupu@ubuntu-asix2:/media/arsupu/XAMPP_USB/OPENSSL_Public_Key$ cp encrypted_secret_kali_arnau.txt ~/secret/
arsupu@ubuntu-asix2:/media/arsupu/XAMPP_USB/OPENSSL_Public_Key$
```

```
arsupu@ubuntu-asix2: ~/secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/secret$ ls
encrypted_secret_kali_arnau.txt  private_ubuntu.key  public_ubuntu.key
encrypted_secret_ubuntu_arnau.txt  public_kali.key  secret_ubuntu_arnau.txt
arsupu@ubuntu-asix2:~/secret$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

1-12-2018

**7- Cada membre descripta el missatge amb la seva clau privada:**

**openssl rsautl -decrypt -inkey private\_nom.key -in missatge\_nom\_parella.txt -out solucio\_nom.txt**

**USUARI 1:** descripta el missatge t **encrypted\_secret\_ubuntu\_arnau.txt** amb la seva clau pública i guarda la solució a l'arxiu **solucio\_ubuntu.txt**

```
uruloki@kali-anonymous: ~/kali_secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~/kali_secret$ ls
encrypted_secret_kali_arnau.txt  private_kali.key  public_ubuntu.key
encrypted_secret_ubuntu_arnau.txt  public_kali.key  secret_kali_arnau.txt
uruloki@kali-anonymous:~/kali_secret$ openssl rsautl -decrypt -inkey private_kali.key -in encrypted_secret_ubuntu_arnau.txt -out
solucio_ubuntu.txt
Enter pass phrase for private_kali.key:
uruloki@kali-anonymous:~/kali_secret$ ls
encrypted_secret_kali_arnau.txt  private_kali.key  public_ubuntu.key  solucio_ubuntu.txt
encrypted_secret_ubuntu_arnau.txt  public_kali.key  secret_kali_arnau.txt
uruloki@kali-anonymous:~/kali_secret$
```

**USUARI 2:** descripta el missatge t **encrypted\_secret\_kali\_arnau.txt** amb la seva clau pública i guarda la solució a l'arxiu **solucio\_kali.txt**

```
arsupu@ubuntu-asix2: ~/secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/secret$ ls
encrypted_secret_kali_arnau.txt  private_ubuntu.key  public_ubuntu.key  solucio_kali.txt
encrypted_secret_ubuntu_arnau.txt  public_kali.key  secret_ubuntu_arnau.txt
arsupu@ubuntu-asix2:~/secret$
arsupu@ubuntu-asix2:~/secret$ openssl rsautl -decrypt -inkey private_ubuntu.key -in encrypted_secret_kali_arnau.txt -out
solucio_kali.txt
Enter pass phrase for private_ubuntu.key:
arsupu@ubuntu-asix2:~/secret$ ls
encrypted_secret_kali_arnau.txt  private_ubuntu.key  public_ubuntu.key  solucio_kali.txt
encrypted_secret_ubuntu_arnau.txt  public_kali.key  secret_ubuntu_arnau.txt
arsupu@ubuntu-asix2:~/secret$
```

**Nom i Cognoms**

Arnau Subirós Puigarnau

**Data**

1-12-2018

**8-** Cada membre mostra el contingut del missatge solució\_nom.txt utilitzant el comandament cat just després de desencriptat el missatge.

**USUARI 1:** *mosta la solució del seu missatge encriptat solucio\_ubuntu.txt*

```
uruloki@kali-anonymous: ~/kali_secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
uruloki@kali-anonymous:~/kali_secret$ ls
encrypted_secret_kali_arnau.txt  private_kali.key  public_ubuntu.key  solucio_ubuntu.txt
encrypted_secret_ubuntu_arnau.txt  public_kali.key  secret_kali_arnau.txt
uruloki@kali-anonymous:~/kali_secret$ cat solucio_ubuntu.txt
No pateixis...
USB
Arribaré tal com varem quedar...
Portaré el material assignat
uruloki@kali-anonymous:~/kali_secret$
```

**USUARI 2:** *mosta la solució del seu missatge encriptat solucio\_kali.txt*

```
arsupu@ubuntu-asix2: ~/secret
Fitxer Edita Visualitza Cerca Terminal Ajuda
arsupu@ubuntu-asix2:~/secret$ ls
encrypted_secret_kali_arnau.txt  private_ubuntu.key  public_ubuntu.key  solucio_kali.txt
encrypted_secret_ubuntu_arnau.txt  public_kali.key  secret_ubuntu_arnau.txt
arsupu@ubuntu-asix2:~/secret$ cat solucio_kali.txt
Hem quedat demà a la mateixa hora.
No tardis...
arsupu@ubuntu-asix2:~/secret$
```