

BASE DE DADES

XIFRATGE I DESXIFRATGE DE DADES



NOM: *Bixiang Zhu*

CURS: *1r ASIX*

ESCOLA: *InstitutMVM*

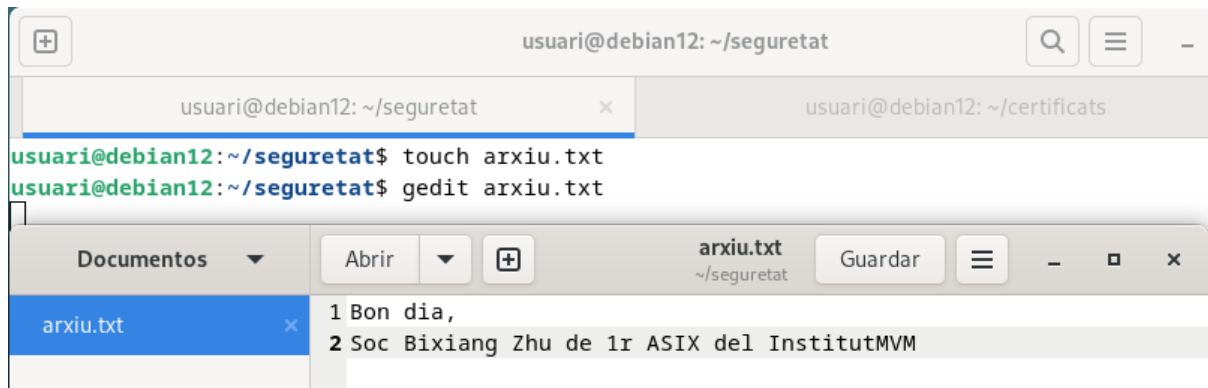
ÍNDEX

ÍNDEX	2
CREACIÓ CLAUS	3
CREACIÓ PDF	4
PREREQUISITS	4
INSTAL·LACIÓ	4
CONVERSIÓ .TXT A .PDF	5
VERIFICACIÓ	6
XIFRATGE I DESXIFRATGE	7
CREACIÓ CARPETA	7
STEGHIDE	7
ENCRIPACIÓ ZIP	8
CORREU	9
CORREU COMPANY	10
ENCRYPTACIÓ SECRET.TXT	11
SIGNATURA NOREPUDI AMB CLAU PRIVADA	12
CORREU	13
CORREU COMPANY	13
DESENCRIPTACIÓ SECRET_ENCRYPTED DEL COMPANY	14
DESCRIPTACIÓ L'ARXIU MISSATGE_ENCRYPTED.ZIP DEL COMPANY	14
OBRIR PDF COMPANY	15

CREACIÓ PDF

PREREQUISITS

Necessitarem tenir un arxiu.txt per poder convertir en pdf, com que no tinc creare un i introduire algunes dades.



```
usuari@debian12: ~/seguretat
usuari@debian12:~/seguretat$ touch arxiu.txt
usuari@debian12:~/seguretat$ gedit arxiu.txt
```

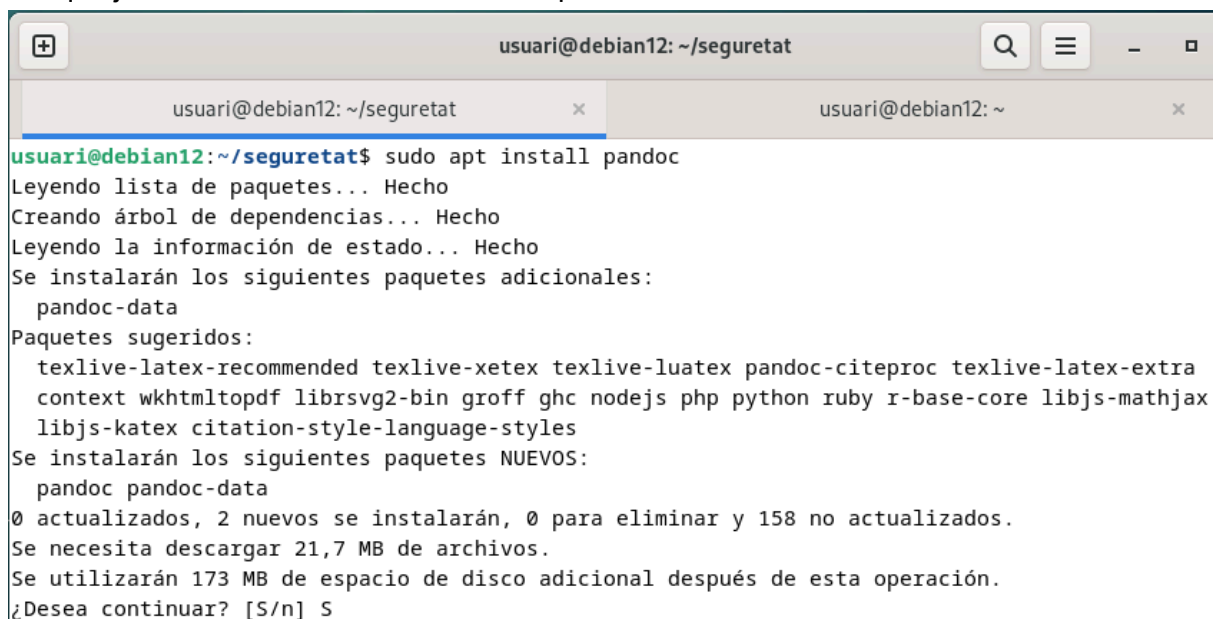
Documentos | Abrir | arxiu.txt ~/seguretat | Guardar

arxiu.txt

```
1 Bon dia,
2 Soc Bixiang Zhu de 1r ASIX del InstitutMVM
```

INSTAL·LACIÓ

Ara que ja tenim el arxiu.txt instal·larem el pandoc i texlive-xetex:



```
usuari@debian12: ~/seguretat
usuari@debian12:~/seguretat$ sudo apt install pandoc
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  pandoc-data
Paquetes sugeridos:
  texlive-latex-recommended texlive-xetex texlive-luatex pandoc-citeproc texlive-latex-extra
  context wkhtmltopdf librsvg2-bin groff ghc nodejs php python ruby r-base-core libjs-mathjax
  libjs-katex citation-style-language-styles
Se instalarán los siguientes paquetes NUEVOS:
  pandoc pandoc-data
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 158 no actualizados.
Se necesita descargar 21,7 MB de archivos.
Se utilizarán 173 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
```

```
usuari@debian12:~/seguretat$ sudo apt install texlive-xetex
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
ca-certificates-java default-jre default-jre-headless dvisvgm fonts-lato fonts-lmodern
fonts-texgyre fonts-texgyre-math java-common libapache-pom-java libatk-wrapper-java
libatk-wrapper-java-jni libbit-vector-perl libcarp-clan-perl libcommons-logging-java
libcommons-parent-java libcrypt-rc4-perl libdate-calc-perl libdate-calc-xs-perl
libdate-manip-perl libdigest-perl-md5-perl libfontbox-java libgumbo1 libjcode-pm-perl
libjs-jquery libmujs2 libole-storage-lite-perl libparse-recdescent-perl libpdfbox-java
libpotrace0 libptexenc1 libruby libruby3.1 libspreadsheet-parseexcel-perl
libspreadsheet-writeexcel-perl libtcl8.6 libteckit0 libtexlua53-5 libtexluajit2 libtk8.6
libunicode-map-perl libzip-0-13 lmodern mupdf-tools openjdk-17-jre openjdk-17-jre-headless
preview-latex-style rake ruby ruby-net-telnet ruby-rubygems ruby-sdbm ruby-webrick
ruby-xmllrpc ruby3.1 rubygems-integration tclutils tcl tcl8.6 teckit tex-common tex-gyre
texlive-base texlive-binaries texlive-fonts-recommended texlive-latex-base
texlive-latex-extra texlive-latex-recommended texlive-pictures texlive-plain-generic tipa tk
tk8.6 zip
Paquetes sugeridos:
```

CONVERSIÓ .TXT A .PDF

Ara que ja tenim instal·lat els programes utilitzarem la comanda `'sudo find /usr/share/fonts/ -name '*.ttf''` per buscar una font principal per a fer servir en la generació del PDF:

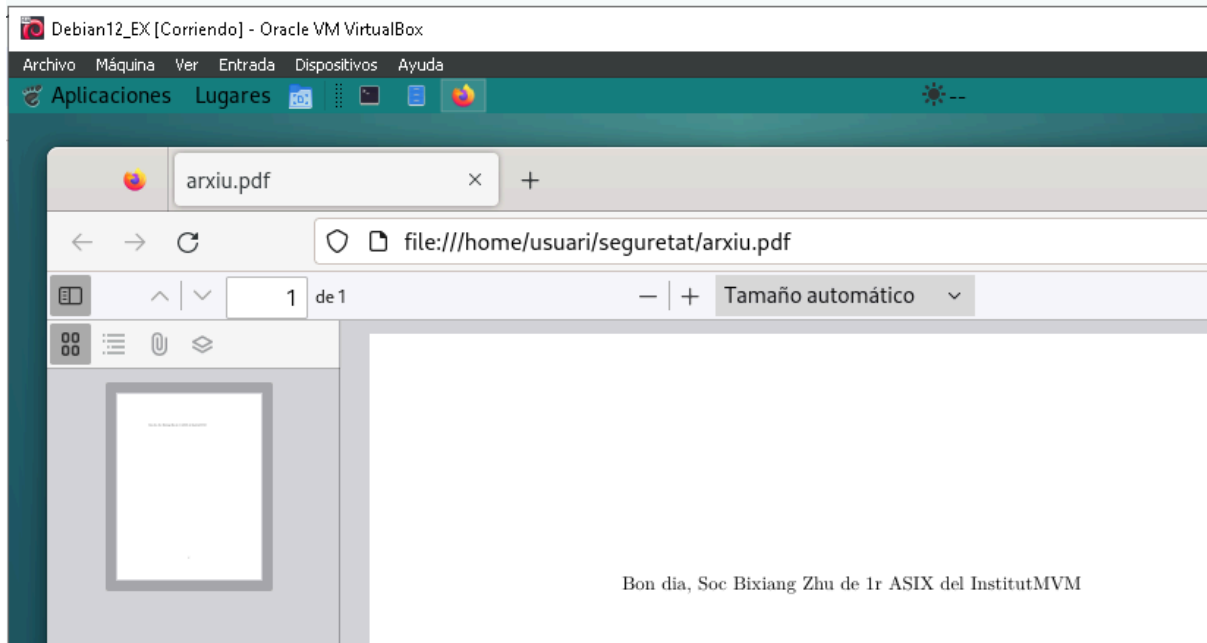
```
usuari@debian12:~/seguretat$ sudo find /usr/share/fonts/ -name '*.ttf'
/usr/share/fonts/truetype/lato/Lato-Hairline.ttf
/usr/share/fonts/truetype/lato/Lato-Italic.ttf
/usr/share/fonts/truetype/lato/Lato-HeavyItalic.ttf
/usr/share/fonts/truetype/lato/Lato-Bold.ttf
/usr/share/fonts/truetype/lato/Lato-HairlineItalic.ttf
/usr/share/fonts/truetype/lato/Lato-SemiboldItalic.ttf
/usr/share/fonts/truetype/lato/Lato-MediumItalic.ttf
/usr/share/fonts/truetype/lato/Lato-Black.ttf
/usr/share/fonts/truetype/lato/Lato-Semibold.ttf
/usr/share/fonts/truetype/lato/Lato-BlackItalic.ttf
/usr/share/fonts/truetype/lato/Lato-Heavy.ttf
```

A mi m'agrada el font *LiberationSans-Italic.ttf* i ho posaré en el canvi de .txt a pdf amb la comanda `'pandoc (arxiu).txt -o (arxiu).pdf --variable mainfont="(font).ttf''`

```
usuari@debian12:~/seguretat$ pandoc arxiu.txt -o arxiu.pdf --variable mainfont="LiberationSans-Italic.ttf"
usuari@debian12:~/seguretat$ ls
arxiu.pdf arxiu.txt emissor receptor
usuari@debian12:~/seguretat$
```

VERIFICACIÓ

per verificar-ho obrim l'arxiu.pdf



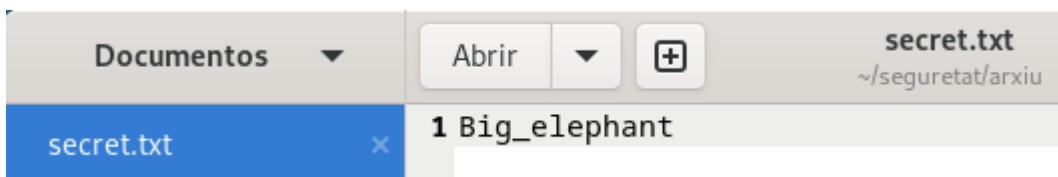
XIFRATGE I DESXIFRATGE

EN AQUEST PART DE LA TAREA SEREM 2 PERSONES
(BIXIANG ZHU, RUBEN GAMIZ)

CREACIÓ CARPETA

Per fer-ho i per no liar he creat una carpeta anomenada arxiu, he creat el secret.txt i posat la sunset.jpg dins

```
usuari@debian12:~/seguretat$ mkdir arxiu
usuari@debian12:~/seguretat$ cd arxiu/
usuari@debian12:~/seguretat/arxiu$ ls
usuari@debian12:~/seguretat/arxiu$ touch secret.txt
usuari@debian12:~/seguretat/arxiu$ gedit secret.txt
usuari@debian12:~/seguretat/arxiu$ cp /usr/share/pixmaps/faces/legacy/sunset.jpg ~/seguretat/arxiu/
usuari@debian12:~/seguretat/arxiu$ ls
secret.txt  sunset.jpg
usuari@debian12:~/seguretat/arxiu$
```



STEGHIDE

He tingut que instal·lar el steghide per poder steganograficar l'arxiu

```
usuari@debian12:~/seguretat/arxiu$ sudo apt-get install steghide
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libmcrypt4
Paquetes sugeridos:
  libmcrypt-dev mcrypt
Se instalarán los siguientes paquetes NUEVOS:
  libmcrypt4 steghide
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 158 no actualizados.
Se necesita descargar 217 kB de archivos.
Se utilizarán 701 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
```

he ocultat l'arxiu 'secret.txt' que conté la contrasenya de xifratge simètric a el sunset.jpg

```
usuari@debian12:~/seguretat/arxiu$ sudo steghide embed -cf sunset.jpg -ef secret.txt
Anotar salvoconducto:
Re-ingresar salvoconducto:
adjuntando "secret.txt" en "sunset.jpg"... hecho
usuari@debian12:~/seguretat/arxiu$
```


ENCRIPTACIÓ ZIP

Copiem l'arxiu pdf dins de la carpeta arxiu per poder fer un zip posteriorment

```
usuari@debian12:~/seguretat$ ls
arxiu  arxiu.pdf  arxiu.txt  emissor  receptor
usuari@debian12:~/seguretat$ cp arxiu.pdf arxiu/
usuari@debian12:~/seguretat$ cd arxiu/
usuari@debian12:~/seguretat/arxiu$ ls
arxiu.pdf          'norepudi(1).txt'  secret_descrypted.txt
missatge_encrypted.zip  norepudi.sha256  'secret_encrypted(1).txt'
missatge_encrypted.zip  norepudi.txt      secret.txt
missatge.zip         private_key.pem    sunset.jpg
usuari@debian12:~/seguretat/arxiu$
```

he posat aquest 2 arxius en un zip i l'he anomenat missatge.zip

```
usuari@debian12:~/seguretat/arxiu$ zip missatge.zip secret.txt sunset.jpg arxiu.pdf
updating: secret.txt (stored 0%)
updating: sunset.jpg (deflated 5%)
adding: arxiu.pdf (deflated 1%)
usuari@debian12:~/seguretat/arxiu$ ls
arxiu.pdf          missatge.zip        norepudi.txt          'secret_encrypted(1).txt'
missatge_encrypted.zip  'norepudi(1).txt'  private_key.pem        secret.txt
missatge_encrypted.zip  norepudi.sha256    secret_descrypted.txt  sunset.jpg
usuari@debian12:~/seguretat/arxiu$
```

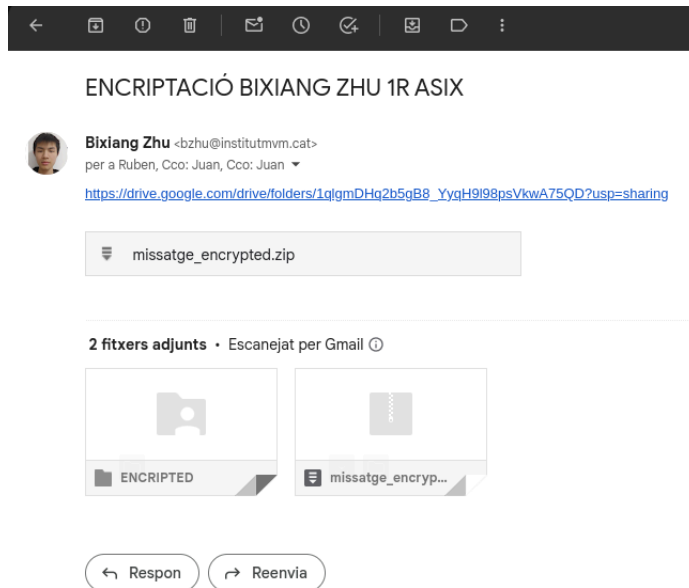
He encriptat el missatge.zip amb l'arxiu secret.txt i l'he anomenat missatge_encrypted.zip

```
usuari@debian12:~/seguretat/arxiu$ openssl enc -aes-256-cbc -in missatge.zip -out missatge_encrypted.zip -pass file:secret.txt
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
usuari@debian12:~/seguretat/arxiu$ ls
missatge_encrypted.zip  missatge.zip  secret.txt  sunset.jpg
usuari@debian12:~/seguretat/arxiu$
```

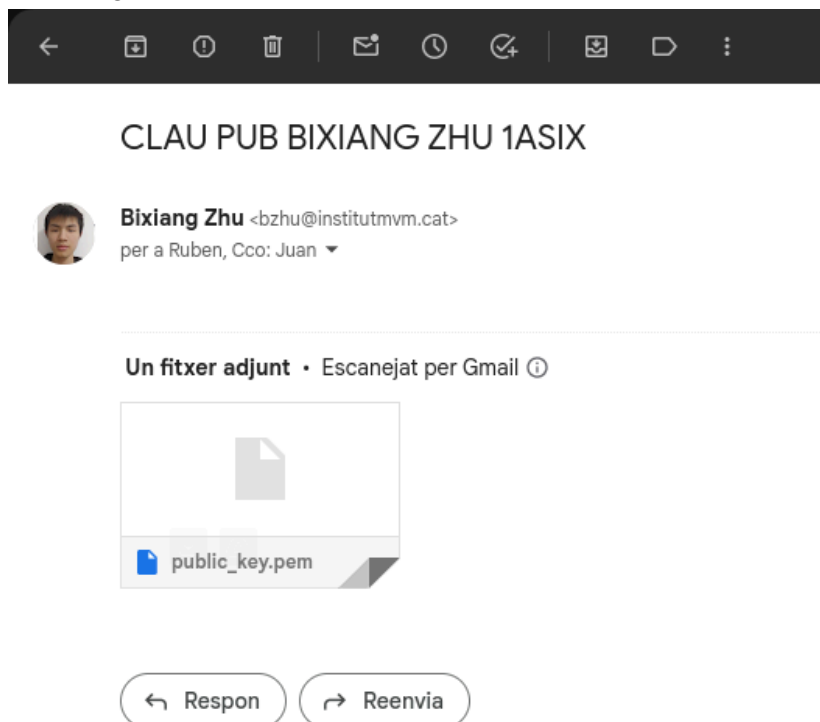
pero faltaba el -pbkdf2 que l'he corregit:

```
usuari@debian12:~/seguretat/arxiu$ openssl enc -aes-256-cbc -in missatge.zip -out missatge_encrypted.zip -pass file:secret.txt -pbkdf2
usuari@debian12:~/seguretat/arxiu$ ls
missatge_encrypted.zip  'norepudi(1).txt'  private_key.pem        secret.txt
missatge_encrypted.zip  norepudi.sha256    secret_descrypted.txt  sunset.jpg
missatge.zip           norepudi.txt      'secret_encrypted(1).txt'
usuari@debian12:~/seguretat/arxiu$
```


He passat el correu tant de la carpeta que conté el missatge_encrypted.zip i del mateix fitxer meu company.



En el segon correu li he passat la meva clau pública



CORREU COMPANYY

Aquí el meu company també m'ha passat el seu correu amb el seu missatge_encrypted.zip


Missatge Safata d'entrada x



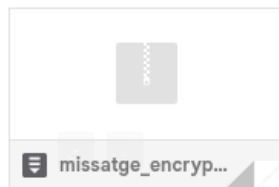
Ruben Gamiz Porcel

per a Juan, mi ▾

21:44 (fa 27 minuts)

 missatge_encrypted.zip

Un fitxer adjunt • Escanejat per Gmail ⓘ



i també del seu clau pública en el seu 2n correu

Clau Pub rgamiz Safata d'entrada x

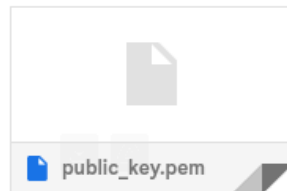


Ruben Gamiz Porcel

per a mi ▾

 Tradueix a: català x

Un fitxer adjunt • Escanejat per Gmail ⓘ



← Respon

→ Reenvia

ENCRYPTACIÓ SECRET.TXT

I'he guardat en la descarga temporalment les 2 arxius que m'ha enviat el meu company



he copiat el fitxer public_key a ruben_key.pem

```
usuari@debian12:~/seguretat/arxiu$ cd ~/Descargas/  
usuari@debian12:~/Descargas$ ls  
missatge_encrypted.zip public_key.pem  
usuari@debian12:~/Descargas$ cp public_key.pem ruben_key.pem  
usuari@debian12:~/Descargas$ ls  
missatge_encrypted.zip public_key.pem ruben_key.pem  
usuari@debian12:~/Descargas$
```

he fet una copia del fitxer secret.txt a descargues

```
usuari@debian12:~/seguretat/arxiu$ ls  
missatge_encrypted.zip missatge.zip norepudi.txt secret.txt sunset.jpg  
usuari@debian12:~/seguretat/arxiu$ cp secret.txt ~/Descargas/  
usuari@debian12:~/seguretat/arxiu$
```

per verificar que l'he passat correctament he fet un ls per veure els fitxers

```
usuari@debian12:~/Descargas$ ls  
missatge_encrypted.zip public_key.pem ruben_key.pem secret.txt  
usuari@debian12:~/Descargas$
```

Ara he encriptat el secret.txt amb la clau pública del meu company i l'he anomenat com a secret_encrypted.txt

```
usuari@debian12:~/Descargas$ openssl rsautl -encrypt -inkey ruben_key.pem -pubin  
-in secret.txt -out secret_encrypted.txt  
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.  
usuari@debian12:~/Descargas$ ls  
missatge_encrypted.zip ruben_key.pem secret.txt  
public_key.pem secret_encrypted.txt  
usuari@debian12:~/Descargas$
```

SIGNATURA NOREPUDI AMB CLAU PRIVADA

Farem una copia del nostre clau privada a la carpeta on esta guardat el norepudi.txt

```
usuari@debian12:~/seguretat/emissor$ cp private_key.pem ~/seguretat/arxiu  
usuari@debian12:~/seguretat/emissor$ cd ~/seguretat/arxiu/  
usuari@debian12:~/seguretat/arxiu$ ls  
missatge_encrypted.zip norepudi.txt secret.txt  
missatge.zip private_key.pem sunset.jpg  
usuari@debian12:~/seguretat/arxiu$
```

Signarem l'arxiu amb la nostra clau privada:

```
usuari@debian12:~/seguretat/arxiu$ openssl dgst -sha256 -sign private_key.pem -o  
ut norepudi.sha256 norepudi.txt  
usuari@debian12:~/seguretat/arxiu$ ls  
missatge_encrypted.zip norepudi.sha256 private_key.pem sunset.jpg  
missatge.zip norepudi.txt secret.txt  
usuari@debian12:~/seguretat/arxiu$
```

farem una còpia de norepudi.txt al directori descargues

```
usuari@debian12: ~/seguretat/arxiu$ cp norepudi.txt ~/Descargas/  
usuari@debian12: ~/seguretat/arxiu$ █
```

CORREU

He passat els 2 fitxers tant el norepudi.txt com secret_encrypted.txt

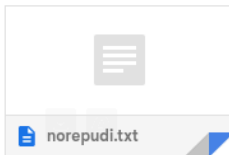
FIRMA I SECRET_ENCRYPTED



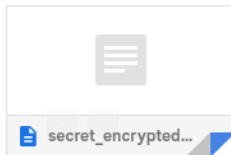
Bixiang Zhu <bzhu@institutmvm.cat>
per a Ruben, Cco: Juan ▾

22:52 (fa 6 minuts)

2 fitxers adjunts • Escanejat per Gmail ⓘ



norepudi.txt



secret_encrypted...

← Respon

→ Reenvia

CORREU COMPANYY

El meu company també m'ha passat els 2 fitxers

Secret Safata d'entrada x



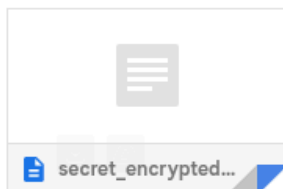
Ruben Gamiz Porcel
per a mi, Juan ▾



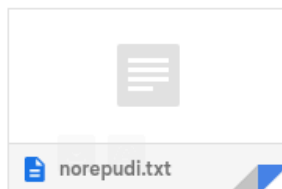
Tradueix a: català



2 fitxers adjunts • Escanejat per Gmail ⓘ



secret_encrypted...



norepudi.txt

← Respon

↶ Respon a tots

→ Reenvia

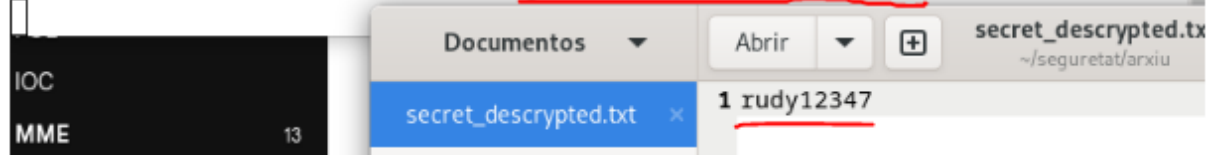
DESENCRIPTACIÓ SECRET_ENCRYPTED DEL COMPANYY

l'he descarregat en la carpeta arxiu

```
usuari@debian12:~/seguretat/arxiu$ ls
missatge_encrypted.zip  norepudi.sha256  'secret_encrypted(1).txt'
missatge.zip            norepudi.txt     secret.txt
'norepudi(1).txt'       private_key.pem  sunset.jpg
usuari@debian12:~/seguretat/arxiu$
```

la desencryptarem el secret_encrypted.txt del meu company amb la nostra private_key i podem veure que la contrasenya

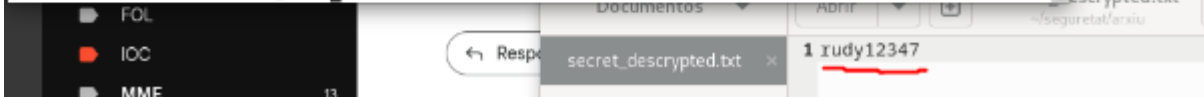
```
usuari@debian12:~/seguretat/arxiu$ openssl rsautl -decrypt -inkey private_key.pem -in secret_encrypted\1\).txt -out secret_descrypted.txt
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
usuari@debian12:~/seguretat/arxiu$ ls
missatge_encrypted.zip  norepudi.txt     secret.txt
missatge.zip            private_key.pem   sunset.jpg
'norepudi(1).txt'       secret_descrypted.txt
norepudi.sha256         'secret_encrypted(1).txt'
usuari@debian12:~/seguretat/arxiu$ gedit secret_descrypted.txt
```



DESCRIPTACIÓ L'ARXIU MISSATGE_ENCRYPTED.ZIP DEL COMPANYY

Desaencryptarem el missatge_encrypted.zip amb la contrasenya que hem descriptat abans del fitxer secret_descrypted.txt

```
usuari@debian12:~/Descargas$ openssl enc -pbkdf2 -d -aes-256-cbc -in missatge_encrypted.zip -out missatge.zip
enter AES-256-CBC decryption password:
usuari@debian12:~/Descargas$ ls
missatge_encrypted.zip  norepudi.txt     ruben      secret_encrypted.txt
missatge.zip            public_key.pem   ruben_key.pem  secret.txt
usuari@debian12:~/Descargas$
```



Fer un unzip per extreure els fitxers

```
usuari@debian12:~/Descargas$ unzip missatge.zip
Archive: missatge.zip
replace sunset.jpg? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: sunset.jpg
  inflating: heimerdinguer.pdf
usuari@debian12:~/Descargas$ ls
heimerdinguer.pdf  missatge.zip  ruben      secret.txt
missatge_encrypted34123213.zip  norepudi.txt  ruben_key.pem  sunset.jpg
missatge_encrypted.zip  public_key.pem  secret_encrypted.txt
usuari@debian12:~/Descargas$
```

The screenshot shows a Mac desktop with a light gray background. In the foreground, there is a file explorer window titled 'Carpeta personal / Descargas'. The sidebar on the left lists various folders: 'Recientes', 'Destacados', 'Carpeta personal', 'Descargas' (highlighted), 'Documentos', 'Imágenes', 'Música', 'Videos', and 'Papeleria'. The main area of the file explorer shows three files: 'missatge.zip' (highlighted with a red arrow), 'missatge_encrypted.zip', and 'heimerdinguer.pdf'. Below the file explorer, there is a smaller window titled 'missatge.zip' showing the process of extracting files. The window has a search bar and a list of files being extracted, including 'heimerdinguer.pdf' and 'sunset.jpg'.

Extraer + missatge.zip

Lugar: /

Nombre	Tamaño	Tipo	Modificado
heimerdinguer.pdf	2,3 kB	documento ...	15 abril 2024, 08:49
sunset.jpg	3,1 kB	imagen JPEG	14 abril 2024, 21:40

Per fer-ho en la carpeta que hem extret fem un open 'nom_arxiu'.pdf o bé obrint manualment des d'alguna aplicació web com firefox

[illegible]

