­

**M11 – Seguretat Informàtica – UF1**

Pràctica 1 – Seguretat física d'una nau industrial

Nil Massó

**Table of Contents**

[1) Plànol físic de l'empresa (2,5 punts) 4](#__RefHeading___Toc603_2282456629)

[2) Plànol de seguretat (2,5 punts) 5](#__RefHeading___Toc605_2282456629)

[3) Plànol de climatització (2,5 punts) 6](#__RefHeading___Toc607_2282456629)

[4) Realitzar un pressupost aproximat del pla de seguretat física. Inclou en el pressupost els elements de seguretat que has descrit anteriorment. (2,5 punts) 7](#__RefHeading___Toc609_2282456629)

[5) CPD (Tasques opcionals) 8](#__RefHeading___Toc611_2282456629)

La nostra cap d’informàtica a l'empresa **Notifixis S.A.** ens demana un pla de seguretat física de les seves instal·lacions. Ens defineixen les diferents zones de l'empresa:

Zones de l'empresa

**Sala de servidors**

1 Armari Rack de servidors. [Exemple](https://www.thomann.de/intl/millenium_sr2018.htm?shp=eyJjb3VudHJ5IjoiZ2IiLCJjdXJyZW5jeSI6MiwibGFuZ3VhZ2UiOjJ9&reload=1)

1 patch panel. [Exemple](https://www.cablecel.com/productos/redes-voz-y-datos/paneles-tomas-y-latiguillos/categoria-5e/paneles-cat5e/panel-24-rj45-cat5e-negro-excel/)

1 switch. [Exemple](https://www.cablecel.com/productos/networking-y-wireless/switch-l3-managed-24-port-gig-sfp-4-dual-pers-and-4x-10g-sfp-stackable-dual-psu-2/)

1 servidor web [Exemple](https://www.give1life.com/dell-r620-8sff-2xe5-264012cor-24thr-32gb-ramh3104x1gb2-psu/)

1 servidor de dades [Exemple](https://www.give1life.com/hp-proliant-dl380e-g7-2x-l5640-36gb-ram-4x-450gb-4-x-300gb-servidor-hp/)

**Taller mecànic**

2 taladradores (Per exemple <https://www.directindustry.es/prod/knuth-machine-tools/product-27150-2230301.html>)

1 fresadora (Per exemple <https://www.directindustry.es/prod/knuth-machine-tools/product-27150-1647163.html>)

2 màquines de control numèric (Per exemple <https://www.directindustry.es/prod/haas-automation/product-7235-1863017.html>)

1 torn manual (Per exemple <https://www.directindustry.es/prod/knuth-machine-tools/product-27150-2212793.html>)

**Direcció**

2 ordinadors

1 impressora/escàner

**Departament de vendes i màrqueting**

4 ordinadors

1 impressora/escàner

1 escàner

**Oficina tècnica**

4 ordinadors

1 punt d’accés sense fils

1 impressora/escàner

Realitza les següents tasques:

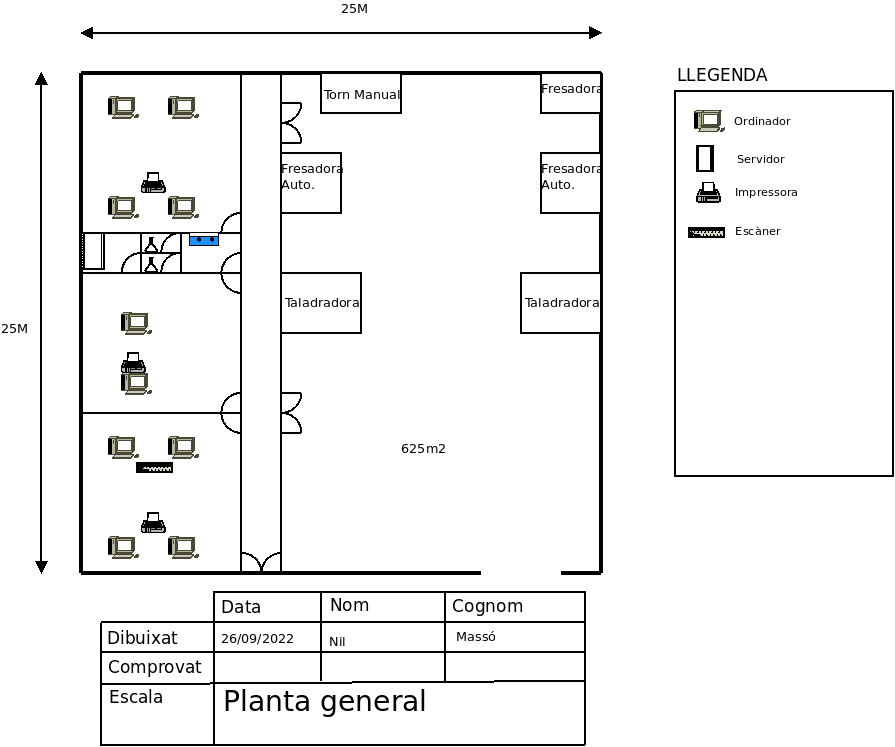
## 1) Plànol físic de l'empresa (2,5 punts)

Dibuixa amb alguna eina un plànol **NOMÉS** amb les dimensions totals de la nau, la distribució i el nom de cada zona. **Posa-hi amb icones a cada zona els elements que conté i crea una llegenda per a indicar què és cada cosa.** Pensa en fer més gran les zones amb elements més voluminosos.

Per exemple, podeu fer servir el [DIA](http://dia-installer.de/download/index.html.en) ([enllaç alternatiu](https://drive.google.com/file/d/1HpRGdaO9PFyZiJ1tN5Jr-SX8DvHWHEGJ/view?usp=sharing)) i partir de la plantilla que teniu al Moodle o fer servir una eina al núvol com [LucidChart](https://www.lucidchart.com/)

**Poseu-me una captura del plànol. No m’entregueu el fitxer del programa de dibuixar!!!**

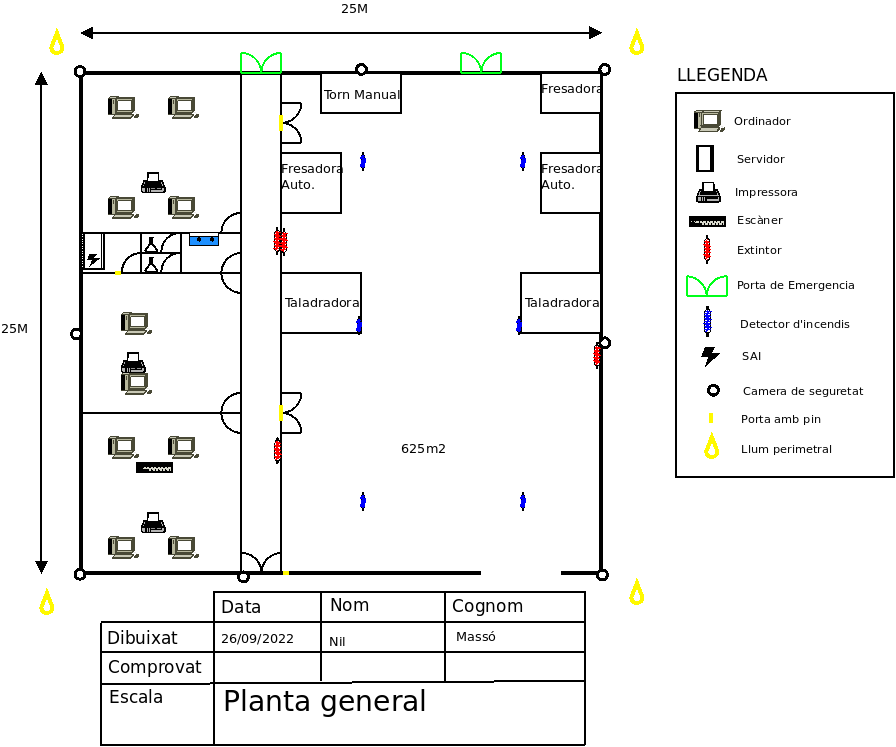
Indicar també les mides en metres de la nau i la superfície total de l'interior de la nau en m2.



## 2) Plànol de seguretat (2,5 punts)

**Investiga** i proposa de manera **justificada** possibles mesures de **seguretat física** (activa o passiva) que siguin proporcionades i que permetin rebaixar el risc al que estan sotmesos els equips informàtics d’aquesta empresa.

Al plànol anterior posa-hi els elements de seguretat física per tal de protegir a les persones i els béns de l'empresa. **Posar com a mínim 6 elements de seguretat física**.

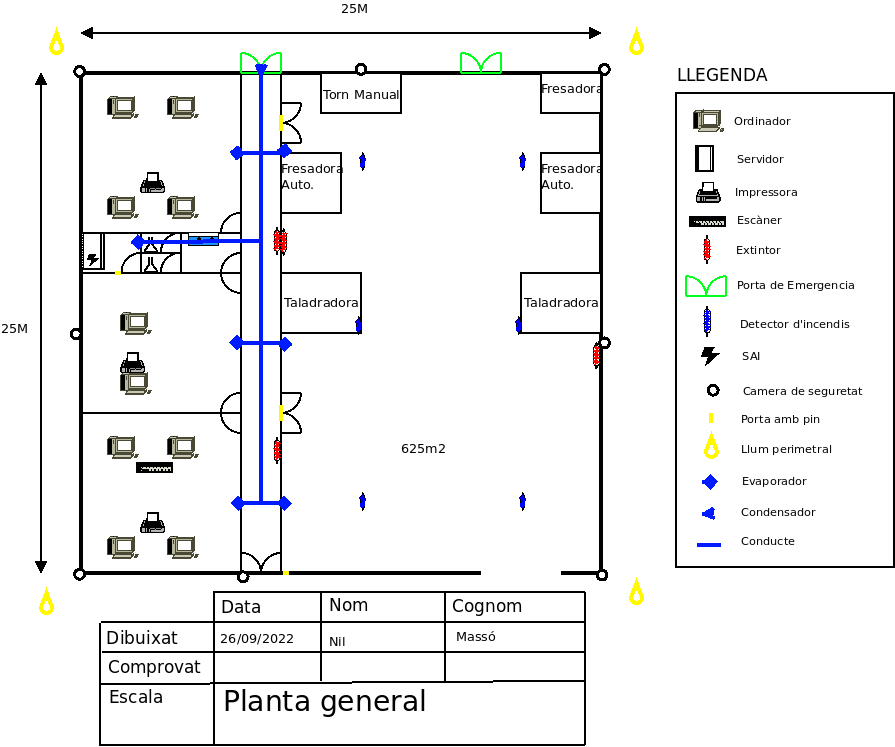
**Per a dibuixar els elements de seguretat utilitzar símbols representatius per a cada element i** **afegir-los a la llegenda.**

## 3) Plànol de climatització (2,5 punts)

**Al plànol físic del punt 1**, ara afegeix-hi a cada zona de la nau la temperatura i humitat recomanada.

|  |  |  |
| --- | --- | --- |
| Tipologia | Temperatura | Humitat |
| Oficines | 27 | 50% |
| Taller | 24 | 55% |
| Sala servidor | 22 | 50% |

Dibuixar els evaporadors i els condensadors necessaris. **Especifica clarament en el plànol la posició de l’evaporador i del condensador (interior o exterior). Posa-hi una llegenda, també.**



## 4) Realitzar un pressupost aproximat del pla de seguretat física. Inclou en el pressupost els elements de seguretat que has descrit anteriorment. (2,5 punts)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Descripció de l’element (amb un enllaç) | Quantitat | Preu/unitat | Total | Gran  Total |
| 1 | https://www.amazon.es/dp/B06XCKMNT4?tag=mariocasas-21&linkCode=ogi&th=1&psc=1 | 4 | 54 | 216 | 2089 |
| 2 | https://servimaxi.casa/instalar-puerta-de-emergencia-precio-y-presupuestos/ | 2 | 420 | 840 |
| 3 | https://www.amazon.es/Detector-Incendios-Silencio-Dormitorios-Pasillos/dp/B08LSVJ9JR | 6 | 20 | 120 |
| 4 | https://www.amazon.es/Salicru-Advance-Line-Interactive-senoidal-Rack/dp/B079FX9P9L/ref=sr\_1\_16?\_\_mk\_es\_ES=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=25SHUAIGLSRY6&keywords=ups&qid=1664228033&sprefix=ups%2Caps%2C150&sr=8-16 | 1 | 243 | 243 |
| 5 | https://www.amazon.es/SANNCE-n48pau/dp/B07FCJ7X6H/ref=sr\_1\_132?\_\_mk\_es\_ES=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=3DKV3LM0QRRXD&keywords=sistema%2Bcamara%2Bexterior&qid=1664228175&sprefix=sistema%2Bcamara%2Bexterior%2Caps%2C112&sr=8-132&th=1 | 1\*8 | 370 | 370 |
| 6 | https://www.amazon.es/Retekess-Retroiluminado-Num%C3%A9rico-Laboratorio-Edificio/dp/B07CYNLF96/ref=sr\_1\_40?keywords=cerradura+puerta+con+codigo&qid=1664228280&sr=8-40 | 4 | 50 | 200 |
| 7 | https://www.amazon.es/Impermeable-Brillante-Iluminacion-Iluminaci%C3%B3n-Seguridad/dp/B09Y8C44BT/ref=sr\_1\_12?\_\_mk\_es\_ES=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=20X9I6BKJVIWK&keywords=foco+exterior&qid=1664228484&sprefix=ex%2Caps%2C200&sr=8-12 | 4 | 25 | 100 |

## 5) CPD (Tasques opcionals)

a) Buscar informació sobre què és un CPD. (0,5 punts)

|  |
| --- |
| Es una instalacio que enmgatzema i processa les dades i aplicacions de una o diverses empreses |

b) Anomena cinc elements informàtics que es poden trobar en un CPD. (0,5 punts)

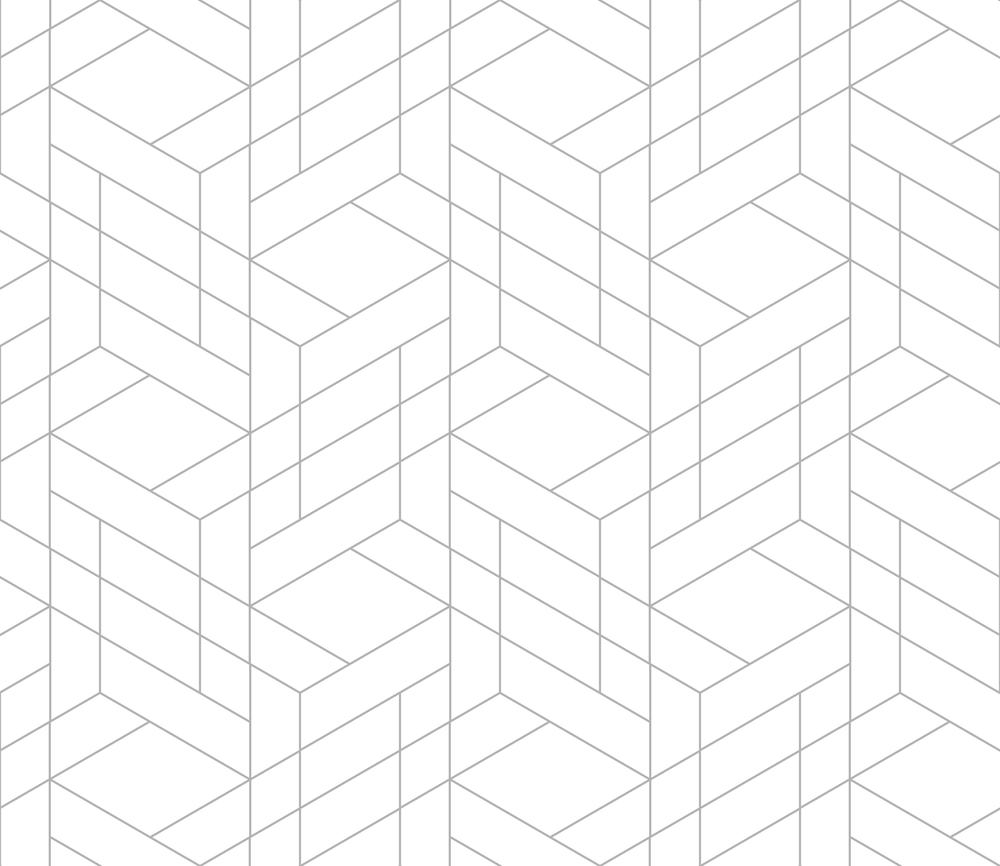
|  |
| --- |
| Servidors, erutadors, sais, |

c) Indica quina és la temperatura i la humitat relativa en un CPD. (0,5 punts)

|  |
| --- |
| 20 graus, 50% humitat |

d) Busca informació sobre quin tipus de extintor és més recomanable per a un CPD. (0,5 punts)

|  |
| --- |
| un de Co2 ja que els incendis seràn de tiupus electric |

­

**M11 – Seguretat Informàtica – UF1**

Pràctica 2 – SEGURETAT LÒGICA: FUNCIÓ HASH CRIPTOGRÀFICA

Nil Massó

**Table of Contents**

[Pràctica 2 – SEGURETAT LÒGICA: FUNCIÓ HASH CRIPTOGRÀFICA 3](#__RefHeading___Toc5320_2677517219)

[Pràctica 4](#__RefHeading___Toc5322_2677517219)

[md5sum 4](#__RefHeading___Toc5324_2677517219)

[sha256sum 5](#__RefHeading___Toc5326_2677517219)

[Exercici 1 (mostra les captures de pantalla i explicacions del procés) (1,5 punts) 5](#__RefHeading___Toc5328_2677517219)

[Exercici 2 (mostra les captures de pantalla i explicacions del procés) (1,5 punts) 6](#__RefHeading___Toc5330_2677517219)

[hashlib for Python 7](#__RefHeading___Toc5332_2677517219)

[Exercici 3 (mostra les captures de pantalla i justifica correctament el procés) (4 punts) 7](#__RefHeading___Toc5334_2677517219)

[Exercici 4: Xifratge i signatura digital (en parelles) (3 punts) 9](#__RefHeading___Toc5336_2677517219)

• Contesteu cada exercici raonant I posant-hi captures de pantalla quan es demani o considereu que es necessari.

• A l’hora d’avaluar i qualificar el treball es tindran en compte els aspectes estètics, de correctesa lingüística (sintàctica i ortogràfica) a més del que s’hagi comentat al cicle formatiu sobre la redacció de documentació tècnica i manuals.

• El mòdul professional pertany a uns estudis orientats al món laboral, cosa que fa que un cop complerts els requisits mínims la nota resultant serà condicionada per la quantitat i qualitat del treball individual realitzat per cada alumne.

# Pràctica 2 – SEGURETAT LÒGICA: FUNCIÓ HASH CRIPTOGRÀFICA

Una **funció de hash criptogràfica** és una classe especial de funció matemàtica també anomenada ***funció digest o funció resum***, que té certes propietats que el fan adequat per al seu ús en la criptografia. Aquest algoritme matemàtic:

• **mapeja dades de mida arbitraria a una cadena de bits d'una mida fixa** (funció resum) i

• està dissenyat per a ser també una funció d'un sol sentit, és a dir, una funció que és **impossible d'invertir**.

Les dades d'entrada es diu sovint el **missatge**, i la sortida (el valor de resum o hash) és sovint anomenat el **resum del missatge** o simplement el producte de digestió.

La funció hash criptogràfica ideal té quatre propietats principals:

• **Ràpid** de calcular el valor hash per a qualsevol missatge donat.

• **No** és factible per **generar el missatge a partir del seu valor hash**.

• Un **petit canvi** en un missatge ha **de canviar el valor del resum** de manera tan extensiva que el nou valor re-sum no pot aparèixer correlacionat amb l'antic hash.

• **No** és factible trobar **dos missatges diferents amb el mateix valor hash**.

La funció hash criptogràfica tenen **moltes aplicacions** de seguretat de la informació, sobretot en:

• Per a signatures digitals.

• Per a codis d'autenticació de missatges.

• Per altres formes d'autenticació.

• Per a les dades d'índex en les taules hash.

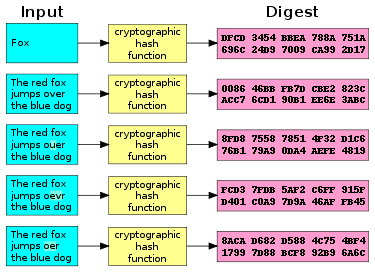
• Per *fingerprinting* (empremta dactilar, eina per tal de defensar els drets d'autor i combatre la pirateria).

• Per detectar dades duplicats.

• Per identificar de forma exclusiva els arxius.

• Per sumes de comprovació per detectar corrupció de dades accidental.

Figura 1: A una funció *hash* un petit canvi en l'entrada (a la paraula "over") canvia dràsticament la sortida (digest). Aquest és l'anomenat efecte allau.



# Pràctica

Aquesta activitat es pot fer des d'una màquina real o des d'una màquina virtual amb sistema operatiu ***Linux*** **Ubuntu Desktop** i accés a *Internet*.

## md5sum

Recordar que l'algoritme MD5 **ja no es considera segur**. Per tant, mentre que *md5sum* és molt adequat per a la identificació d'arxius coneguts en situacions que no estan relacionats amb la seguretat, *md5sum* no ha de ser invocat si hi ha una possibilitat que els arxius han estat intencionalment i maliciosament manipulat, en aquest últim cas, es recomana l'ús d'una eina de hash més recents, com ***sha256sum***.

## sha256sum

***sha1sum*** és un programa informàtic que calcula i verifica hash ***SHA-1***. S'acostuma a fer servir per a verificar la integritat dels arxius. Es troba instal·lat per defecte en la majoria dels sistemes operatius basats en Unix. Les variants inclouen ***shasum, sha224sum, sha256sum, sha384sum i sha512sum***, que fan servir una funció específica ***SHA-2*** de hash, i sha3sum (que permet ***SHA-3*** a través de ***SHA3-512***). També hi ha versions per a Microsoft Windows i la distribució Acti-vePerl inclou una implementació de Perl de shasum. En FreeBSD aquesta utilitat es diu sha512 i amb característiques addicionals.

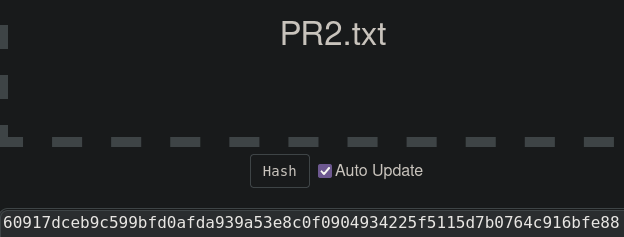
Les variants ***SHA-1 es consideren vulnerables als atacs de col·lisió***, i els usuaris han d'utilitzar per exemple una variant SHA-2 com ara ***sha256sum*** en el seu lloc si es fa servir amb el propòsit de prevenir la manipulació d'arxius per part d'un adversari.

## Exercici 1 (mostra les captures de pantalla i explicacions del procés) (1,5 punts)

Selecciona qualsevol fitxer (un de text per exemple) i fes el seu resum (digest) mitjançant el programari sha256sum. Fes dues operatives:

1.1. Des de la línia d'ordres invoca el programa i aconsegueix el resum d’aquest fitxer.



1.2. Des d'una calculadora en línia *Checksum sha256* fes la mateixa operació. Pots trobar una al següent enllaç: <https://emn178.github.io/online-tools/sha256_checksum.html>

1.3. Compara el resum obtingut des de la línia d'ordres i la calculadora web.

Dona el mateix resultat ja que el metode per a crear el hash a estat el mateix

1.4. Què passa si modifiquem el contingut del fitxer?

Que el hash canviara completament

## Exercici 2 (mostra les captures de pantalla i explicacions del procés) (1,5 punts)

Ara provarem una altra aplicació del Hash: **identificar de forma exclusiva els arxius**.

Fes tot els passos per a assegurar la integritat de les dades i l'autenticitat de la descàrrega d'una ISO d'Ubuntu.

Tots els passos que s'han de fer es poden veure documentats en el següent enllaç: <http://www.ubuntu.com/download/how-to-verify>

Descarreguem la iso juntament amb el seu checksum i les signatures.

Primer executem aquesta comanda per verificar que els nostres arxius estan firmats per ubuntu:

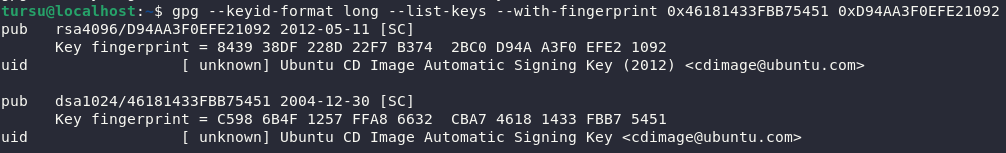
gpg --keyid-format long --verify SHA256SUMS.gpg SHA256SUMS

En cas de no estar ja en un ubuntu haurem de descarregar les claus publiques de ubuntu per verificarho, ho fem amb:

gpg --keyid-format long --keyserver hkp://keyserver.ubuntu.com --recv-keys 0x46181433FBB75451 0xD94AA3F0EFE21092

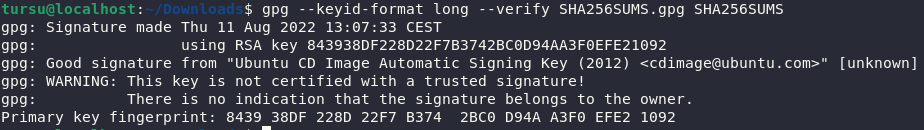
Ara s’hauran afegit clauer del nostre linux

Verifiquem que la emprempta de les claus sigui de ubuntu amb la seguen comanda:

gpg --keyid-format long --list-keys --with-fingerprint 0x46181433FBB75451 0xD94AA3F0EFE21092

Ara ja podem verificar que el checksum sigui legitim, ho fem amb:

gpg --keyid-format long --verify SHA256SUMS.gpg SHA256SUMS

Mirem que ens digui que la signatura es valida

Ara anem al directori on tinguem la ISO en el nostre cas Downloads:

cd ~/Downloads

I executem la comanda per a verificar el hash de la ISO



## hashlib for Python

***hashlib*** és una llibreria per a Python que es permet utilitzar diferents funcions de hash.

El següent codi codifica la paraula ‘hello’ utilitzant les funcions sha512, sha256 i sha1:

*import hashlib*

*paraula=”hello”*

*paraula8=paraula.encode(‘utf8’)*

*hexhash = hashlib.sha512(paraula8).hexdigest()*

*print (hexhash)*

*hexhash = hashlib.sha256(paraula8).hexdigest()*

*print (hexhash)*

*hexhash = hashlib.sha1(paraula8).hexdigest()*

*print (hexhash)*

Encara que les funcions de Hash intenten ser indesxifrables, amb diccionaris de paraules habituals, podem arribar a trobar ràpidament la paraula encriptada.

## Exercici 3 (mostra les captures de pantalla i justifica correctament el procés) (4 punts)

4.1. Amb Python, obté el codi SHA256 de les següents paraules:

• hello

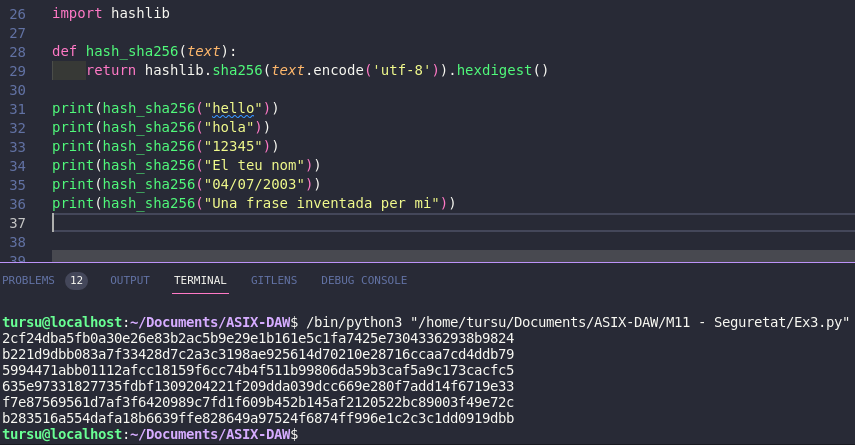
• hola

• 12345

• El teu nom

• La teva data de naixement en format de 6 dígits (2 per al dia, 2 per al mes, 2 per a l’any)

• Una frase



4.2. Utilitza el següent codi Python <https://github.com/Starwarsfan2099/Python-Hash-Cracker> per provar la força de les contrasenyes anteriors. Quan temps tarda en desxifrar cadascuna? N’hi ha alguna que no trobi?

4.3. En el cas de la data de naixement, prova a rebentar-la mitjançant la opció numèrica del codi Python anterior. L’aconsegueix trobar? Quan temps ha necessitat?

4.4. En lloc del diccionari Wordlist.txt que ve per defecte, busca altres diccionaris que s’acostumin a utilitzar per rebentar contrasenyes. Fes una llista dels més habituals i prova almenys un. Quina diferència hi ha entre ells?

## Exercici 4: Xifratge i signatura digital (en parelles) (3 punts)

5.1. Utilitza l’eina GnuPG i la seva eina Kleopatra per a xifrar i desxifrar fitxers. Ho podeu provar amb [Linux](https://apps.kde.org/kleopatra/) o [Windows](https://gpg4win.org/download.html). **Realitza i documenta (tna el procés com el resultat) les tasques següents**:

• Crea’t una parella de claus (ja es creen les dues: pública i privada)

• Puja la teva clau al servidor i baixa't la del teu company. Si no et funciona la interfície del Kleopatra, ves directament a <https://keys.openpgp.org/>

• El servidor et servirà per intercanviar les claus. També pots fer servir altres mètodes (emmagatzemament extraible, correu electrònic,...)

• Xifra i signa un fitxer de text. **Ja saps quina clau has de fer servir.**

• Envia fitxers signats i xifrats al teu company.

• Desxifra els fitxers rebuts del teu company i comprova'n la signatura. **Ja saps quina clau has de fer servir**