

M11 – Seguretat Informàtica – UF1

Pràctica 2 – SEGURETAT LÒGICA: FUNCIO HASH CRIPTOGRÀFICA

Nil Massó



ASIX 2			
M11 – Seguretat Informàtica – UF1		Tipus	Individual
Cognoms, Nom:	Massó Cabaña, Nil	Curs	2022-23
Observacions:			

Table of Contents

Pràctica 2 – SEGURETAT LÒGICA: FUNCIO HASH CRIPTOGRÀFICA.....	3
Pràctica.....	4
md5sum.....	4
sha256sum.....	5
Exercici 1 (mostra les captures de pantalla i explicacions del procés) (1,5 punts).....	5
Exercici 2 (mostra les captures de pantalla i explicacions del procés) (1,5 punts).....	6
hashlib for Python.....	7
Exercici 3 (mostra les captures de pantalla i justifica correctament el procés) (4 punts).....	7
Exercici 4: Xifratge i signatura digital (en parelles) (3 punts).....	9



ASIX 2			
M11 – Seguretat Informàtica – UF1		Tipus	Individual
Cognoms, Nom:	Massó Cabaña, Nil	Curs	2022-23
Observacions:			

- 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: FUNCIO 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 arbitrària 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**.

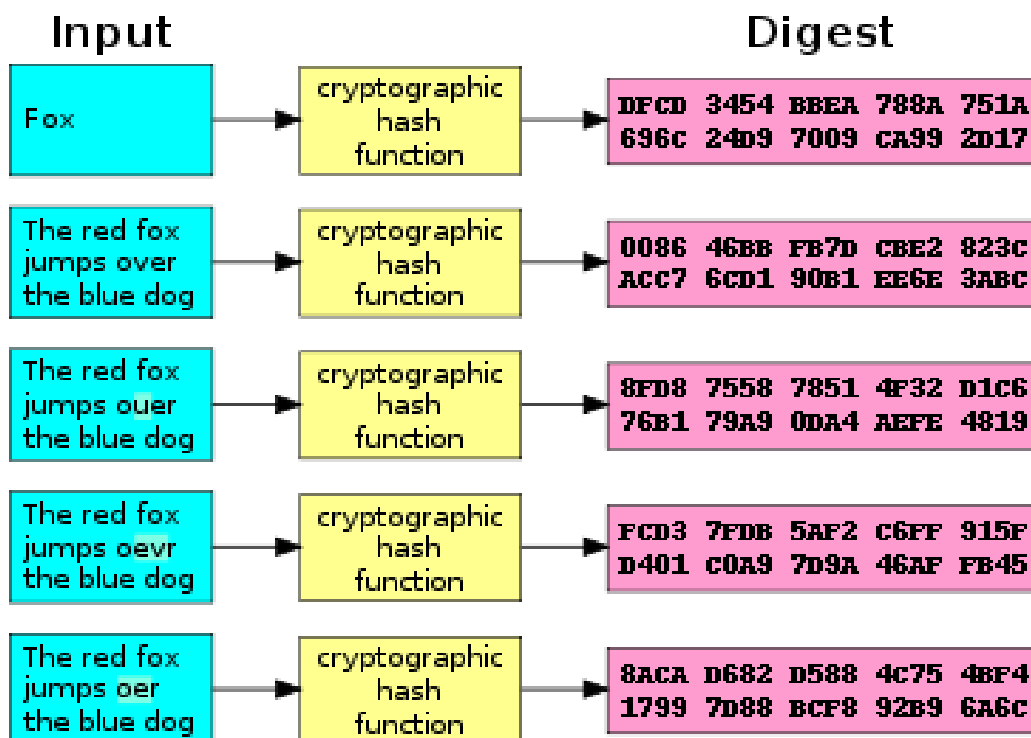
La funció hash criptogràfica tenen **moltes aplicacions** de seguretat de la informació, sobretot en:

- 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.

ASIX 2			
M11 – Seguretat Informàtica – UF1		Tipus	Individual
Cognoms, Nom:	Massó Cabaña, Nil	Curs	2022-23
Observacions:			

- 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



ASIX 2			
M11 – Seguretat Informàtica – UF1		Tipus	Individual
Cognoms, Nom:	Massó Cabaña, Nil	Curs	2022-23
Observacions:			

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)

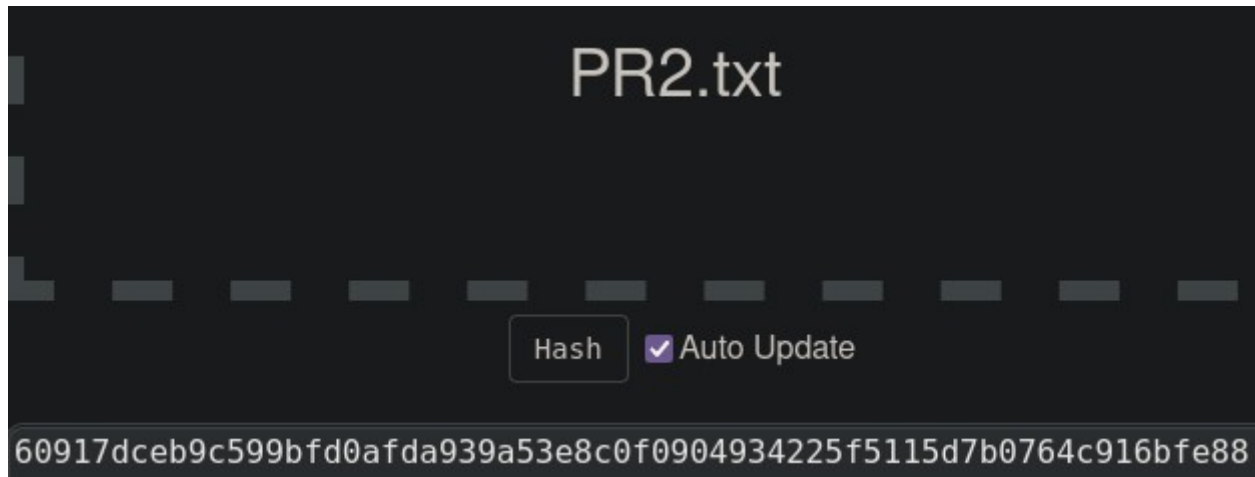
Selecciona qualsevol fitxer (un de text per exemple) i fes el seu resum (digest) mitjançant el programari sha256sum. Fes dues operatives:

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

```
tursu@localhost:~/Documents/ASIX-DAW/M11 - Seguretat$ sha256sum PR2.txt  
60917dceb9c599bfd0afda939a53e8c0f0904934225f5115d7b0764c916bfe88 PR2.txt
```

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

ASIX 2			
M11 – Seguretat Informàtica – UF1		Tipus	Individual
Cognoms, Nom:	Massó Cabaña, Nil	Curs	2022-23
Observacions:			



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 empremta de les claus sigui de ubuntu amb la seguen comanda:

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

```
tursu@localhost:~$ gpg --keyid-format long --list-keys --with-fingerprint 0x46181433FBB75451 0xD94AA3F0EFE21092
pub   rsa4096/D94AA3F0EFE21092 2012-05-11 [SC]
      Key fingerprint = 8439 38DF 228D 22F7 B374  2BC0 D94A A3F0 EFE2 1092
uid   [ unknown] Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.com>

pub   dsa1024/46181433FBB75451 2004-12-30 [SC]
      Key fingerprint = C598 6B4F 1257 FFA8 6632  CBA7 4618 1433 FBB7 5451
uid   [ unknown] Ubuntu CD Image Automatic Signing Key <cdimage@ubuntu.com>
```



ASIX 2			
M11 – Seguretat Informàtica – UF1		Tipus	Individual
Cognoms, Nom:	Massó Cabaña, Nil	Curs	2022-23
Observacions:			

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

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

```
tursu@localhost:~/Downloads$ gpg --keyid-format long --verify SHA256SUMS.gpg SHA256SUMS
gpg: Signature made Thu 11 Aug 2022 13:07:33 CEST
gpg: using RSA key 843938DF228D22F7B3742BC0D94AA3F0EFE21092
gpg: Good signature from "Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 8439 38DF 228D 22F7 B374 2BC0 D94A A3F0 EFE2 1092
```

Mirem que ens digui que la signatura es vàlida

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

```
tursu@localhost:~/Downloads$ sha256sum -c SHA256SUMS 2>&1 | grep OK
ubuntu-22.04.1-desktop-amd64.iso: OK
```

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:



ASIX 2			
M11 – Seguretat Informàtica – UF1		Tipus	Individual
Cognoms, Nom:	Massó Cabaña, Nil	Curs	2022-23
Observacions:			

- hello
- hola
- 12345
- El teu nom
- La teva data de naixement en format de 6 dígit (2 per al dia, 2 per al mes, 2 per a l'any)
- Una frase

```
26 import hashlib
27
28 def hash_sha256(text):
29     return hashlib.sha256(text.encode('utf-8')).hexdigest()
30
31 print(hash_sha256("hello"))
32 print(hash_sha256("hola"))
33 print(hash_sha256("12345"))
34 print(hash_sha256("El teu nom"))
35 print(hash_sha256("04/07/2003"))
36 print(hash_sha256("Una frase inventada per mi"))
37
38
39
```

PROBLEMS 12 OUTPUT TERMINAL GITLENS DEBUG CONSOLE

```
tursu@localhost:~/Documents/ASIX-DAW$ /bin/python3 "/home/tursu/Documents/ASIX-DAW/M11 - Seguretat/Ex3.py"
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
b221d9dbb083a7f33428d7c2a3c3198ae925614d70210e28716ccaa7cd4ddb79
5994471abb01112afcc18159f6cc74b4f511b99806da59b3caf5a9c173cacfc5
635e97331827735fdbf1309204221f209dda039dcc669e280f7add14f6719e33
f7e87569561d7af3f6420989c7fd1f609b452b145af2120522bc89003f49e72c
b283516a554dafa18b6639ffe828649a97524f6874ff996e1c2c3c1dd0919dbb
tursu@localhost:~/Documents/ASIX-DAW$
```

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?

ASIX 2			
M11 – Seguretat Informàtica – UF1		Tipus	Individual
Cognoms, Nom:	Massó Cabaña, Nil	Curs	2022-23
Observacions:			

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](#) o [Windows](#). **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 extraïble, 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**