

## Contrôle Continu

# Sécurité Informatique

**Réalisé par**  
**EL ASRI Ayoub**

**Groupe**  
**4A SAGI TD1**

## A- Cryptographie

Le message déchiffré ainsi que le programme utilise :

```
def inverseMod(a,m):
    _a = 0
    for i in range(0, m):
        if (a*i)%m ==1:
            return i
    return str(str(a) + " et 26 ne sont pas premiers entre eux")

def dechiffrementAffine(chiffre, a, b):
    _a = inverseMod(a,26)
    if(type(_a) is int):
        message = ""
        for lettre in chiffre:
            rang = ord(lettre) - ord('A')
            rang = (_a * (rang - b)) % 26 + ord('A')
            message += chr(rang)
        return message
    else:
        return "L-inverse Inexistant!"

for i in range(0,21):
    for j in range (0,21):
        if(dechiffrementAffine("VRDTFJJ DV RGPSLQTKJTCCLKKLDGPDUTUFJ",
i, j)[1] != '-'):
            print("a = " + str(i) + " b = " + str(j))

print(dechiffrementAffine("VRDTFJJ DV RGPSLQTKJTCCLKKLDGPDUTUFJ", i,
j));
```

```
RTNFZXXNRTSHMJAFQXFUJJQQJNSHNYFYZX
a = 11 b = 17
YAUMGEEUYAZOTQHMXEMBBQXXQUZOUFMFGE
a = 11 b = 18
FHBTNLLBFHGVAXOTELTIIXEEXBGVBMTMNL
a = 11 b = 19
MOIAUSSIMONCHEVALSAPPELLEINCITATUS
a = 11 b = 20
TVPHBZZPTVUJOLCHSZHWWLSSLPJPAHABZ
a = 15 b = 0
RPVDJLLVRPQBWZIDSLD00ZSSZVQBVKDKJL
```

Pour  $a = 11$  et  $b = 19$ , on trouve le message déchiffré:

MOIAUSSIMONCHEVALSAPPELLEINCITATUS

MOI AUSSI MON CHEVAL S'APPELLE **INCITATUS**

## B- OSINT



Rechercher un film, u



Se connecter

S'inscrire



## Nevada



1 membre(s) intéressé(s). Se connecter pour gérer son agenda

Réalisé par Laure De Clermont-Tonnerre avec Matthias Schoenaerts, Bruce Dern, Josh Stewart... - Genre : **Drame** - Sortie cinéma : **19 juin 2019**

Incarcéral dans une prison du Nevada, Roman n'a plus de contact avec l'extérieur ni avec sa fille. Il vit reclus avec sa rage et sa violence comme seule compagnie. Pour essayer de sortir de son isolement, il intègre un programme de réhabilitation...



## Tolkien



6 membre(s) intéressé(s). Se connecter pour gérer son agenda

Réalisé par Dome Karukoski avec Nicholas Hoult, Lily Collins, Craig Roberts... - Genre : **Drame, Biopic** - Sortie cinéma : **19 juin 2019**

TOLKIEN revient sur la jeunesse et les années d'apprentissage du célèbre auteur. Orphelin, il trouve l'amitié, l'amour et l'inspiration au sein d'un groupe de camarades de son école. Mais la Première Guerre Mondiale...



## Nouriev



3 membre(s) intéressé(s). Se connecter pour gérer son agenda

Réalisé par Ralph Fiennes avec Oleg Ivenko, Adèle Exarchopoulos, Raphaël Personnaz... - Genre : **Drame, Biopic** - Sortie cinéma : **19 juin 2019**

Jeune prodige du célèbre ballet du Kirov, Rudolf Nouriev est à Paris en juin 1961 pour se produire sur la scène de l'Opéra. Fasciné par les folles nuits parisiennes et par la vie artistique et culturelle de la capitale, il se lie d'amiti...

Nevada / Tolkien / Nouriev

Lyon Bastille

Le Crémieux

2019

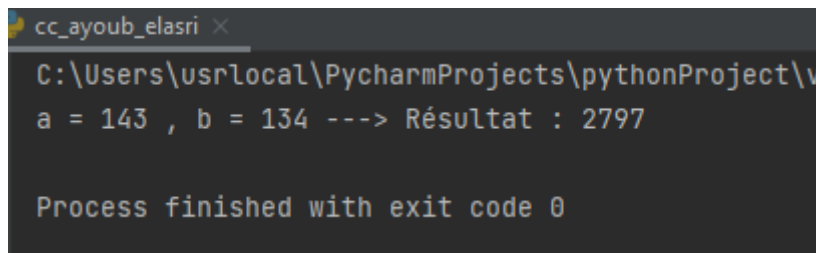
19 06

## C- Programmation

le nombre porte-bonheur ainsi que le programme utilisé :

```
n= 1000000

for i in range (0,n):
    for j in range(0, n):
        if(13*i + 7*j == 2797):
            if(abs(i - j) < 10):
                print("a = " + str(i) + " , b = " + str(j) + " --->
Résultat : " + str(13*i + 7*j))
```



```
cc_ayoub_elasri x
C:\Users\usrlocal\PycharmProjects\pythonProject\venv
a = 143 , b = 134 ---> Résultat : 2797

Process finished with exit code 0
```

A = **143**

B = **134**

Donc le nombre porte-bonheur : **AB = 143134**

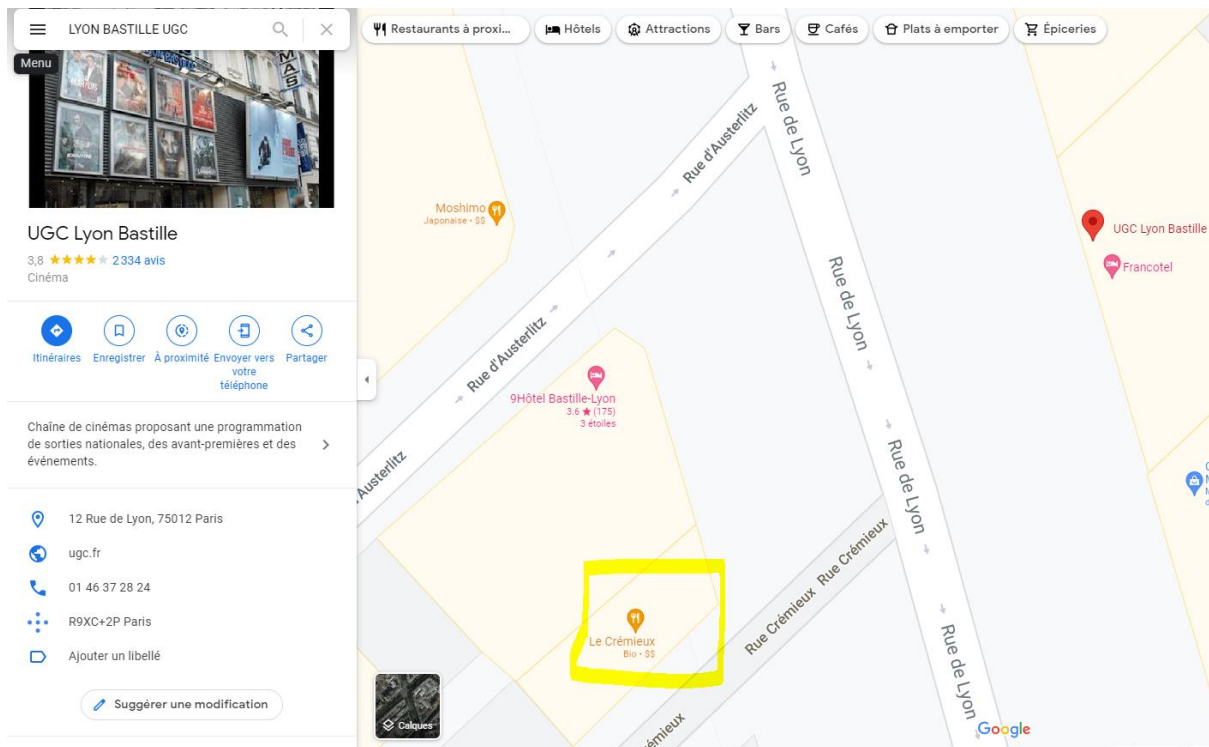
## D- Mise en Commun

On sait que le mot de passe de Martin est composé de **chiffres**, de **lettres minuscules sans accent**, et **une fois du symbole arobase(@)**.

Avec :

**Son biopic préféré :**

**Le restaurant où il a dîné (sans article) :** **Le Cremieux**



Un empereur romain qu'il copie : Caligula

## Incitatus

Incitatus est le nom du cheval favori de l'empereur romain Caligula, qui régna de 37 à 41.

Son nombre porte-bonheur : 143134

*Le seul symbole @ se trouve quelque part dans ce mot de passe, n'importe où, même au milieu d'un mot.*

SHA1 du mdp: **9c85de01b4319238a77cd63d40566f482393b062**

On a les mots-clefs:

143134

Le

Crémieux

@

Caligula

Martin

*Je ne suis pas sur du film, donc je vais faire tous les noms des films qui ont eu la sortie cinema le 19 juin 2019 :*

Nevada

Tolkien

Noureev

Jeanne

Juno

Jenny

```
-----
-----Section A: Main Subject Information-----
-----
> Enter The Main Subject's Full Name, separated by spaces - or as much as you have >:martin
-----
> Enter an additional number, or simply press enter to move on >:143134
> Enter an additional number, or simply press enter to move on >:
-----
--- Get Additional Words ---

Want to add any other additional words?
This is the time to add any information you
might have that was not asked about previously.
If you wish to add numbers in HEXIDECIMAL, you must do so here.

If you are guessing the password for a given domain or purpose,
consider entering its name here.

Inputs containing spaces will have variations generated
that do NOT include spaces.

> Enter an additional word here, or simply press enter to move on >:le
> Enter an additional word here, or simply press enter to move on >:cremieux
> Enter an additional word here, or simply press enter to move on >:@
> Enter an additional word here, or simply press enter to move on >:caligula
> Enter an additional word here, or simply press enter to move on >:nevada
> Enter an additional word here, or simply press enter to move on >:tolkien
> Enter an additional word here, or simply press enter to move on >:noureev
> Enter an additional word here, or simply press enter to move on >:jeanne
> Enter an additional word here, or simply press enter to move on >:juno
> Enter an additional word here, or simply press enter to move on >:jenny
> Enter an additional word here, or simply press enter to move on >:
-----

GNU nano 3.2 hashcc
9c85de01b4319238a77cd63d40566f482393b062
```

*Aperçu sur le dictionnaire :*

mMartinNOUREEV  
mMartinCremieux  
mMartincremieux  
mMartincaligula  
mMartinCREMIEUX  
mMartinCALIGULA  
mMartinCaligula  
mNEVADA@  
mNEVADAM  
mNEVADALe  
mNEVADALE  
mNEVADAl e  
mNEVADAJUNO  
mNEVADAJuno  
mNEVADAJuno  
mNEVADAJenny  
mNEVADAJENNY  
mNEVADAJenny  
mNEVADAnevada  
mNEVADAJEANNE  
mNEVADAMARTIN  
mNEVADAJeanne  
mNEVADAMartin  
mNEVADAJeanne  
mNEVADAmartin  
mNEVADANevada  
mNEVADA143134  
mNEVADATolkien  
mNEVADANoureev  
mNEVADATOLKIEN  
mNEVADAnoureev  
mNEVADATolkien  
mNEVADANOUREEV  
mNEVADACremieux  
mNEVADAcremieux  
mNEVADAcaligula  
mNEVADACREMIEUX  
mNEVADACALIGULA  
mNEVADACaligula  
mjeanne@  
mjeanneM  
mieannel e



```

Thank you for using BEWGor!
elasriayoub4159@sshbox:~$ nano hashcc.txt
elasriayoub4159@sshbox:~$ john hashcc.txt --wordlist=elasri.txt
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-LinkedIn"
Use the "--format=Raw-SHA1-LinkedIn" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "has-160"
Use the "--format=has-160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=6
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2022-01-12 11:56) 0g/s 3241Kp/s 3241Kc/s 3241KC/s CaligulaCALIGULAjuno..CaligulaCALIGULAjuno
Session completed.

```

*Avec  $n=2$ , il n'a pas r uss    le trouver, on augmente  $n$ .*