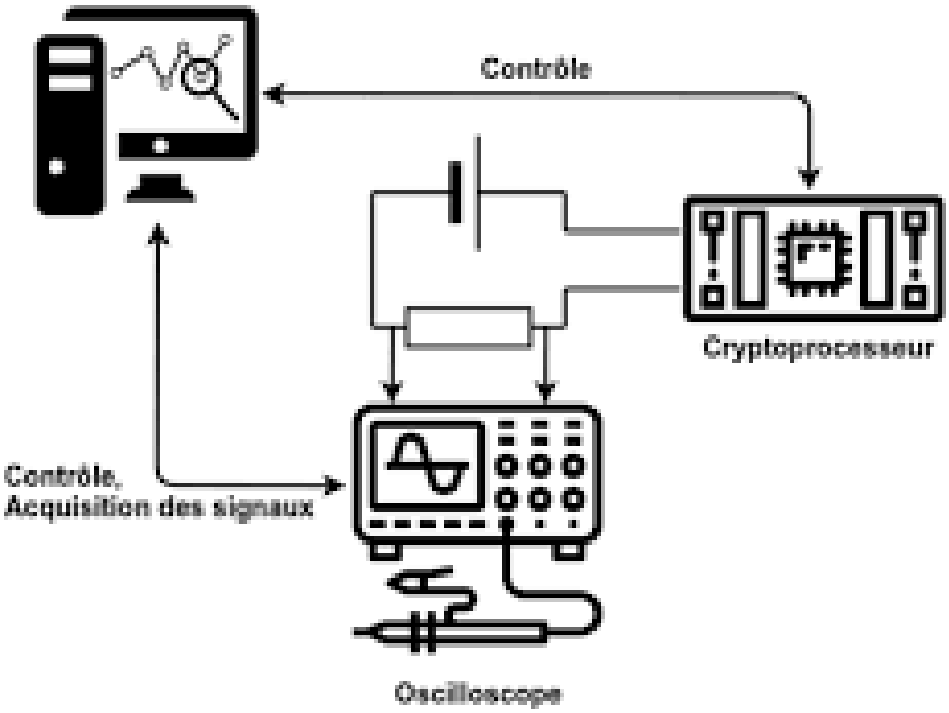
# Cryptographie asymétrique : Attaque par canal auxiliaire

Ben Amira Rawia Khebtani Dorsaf

13 mars 2023




Université de Toulon, UFR Sciences et Techniques

M1 DID

2022-2023

# Table des matières

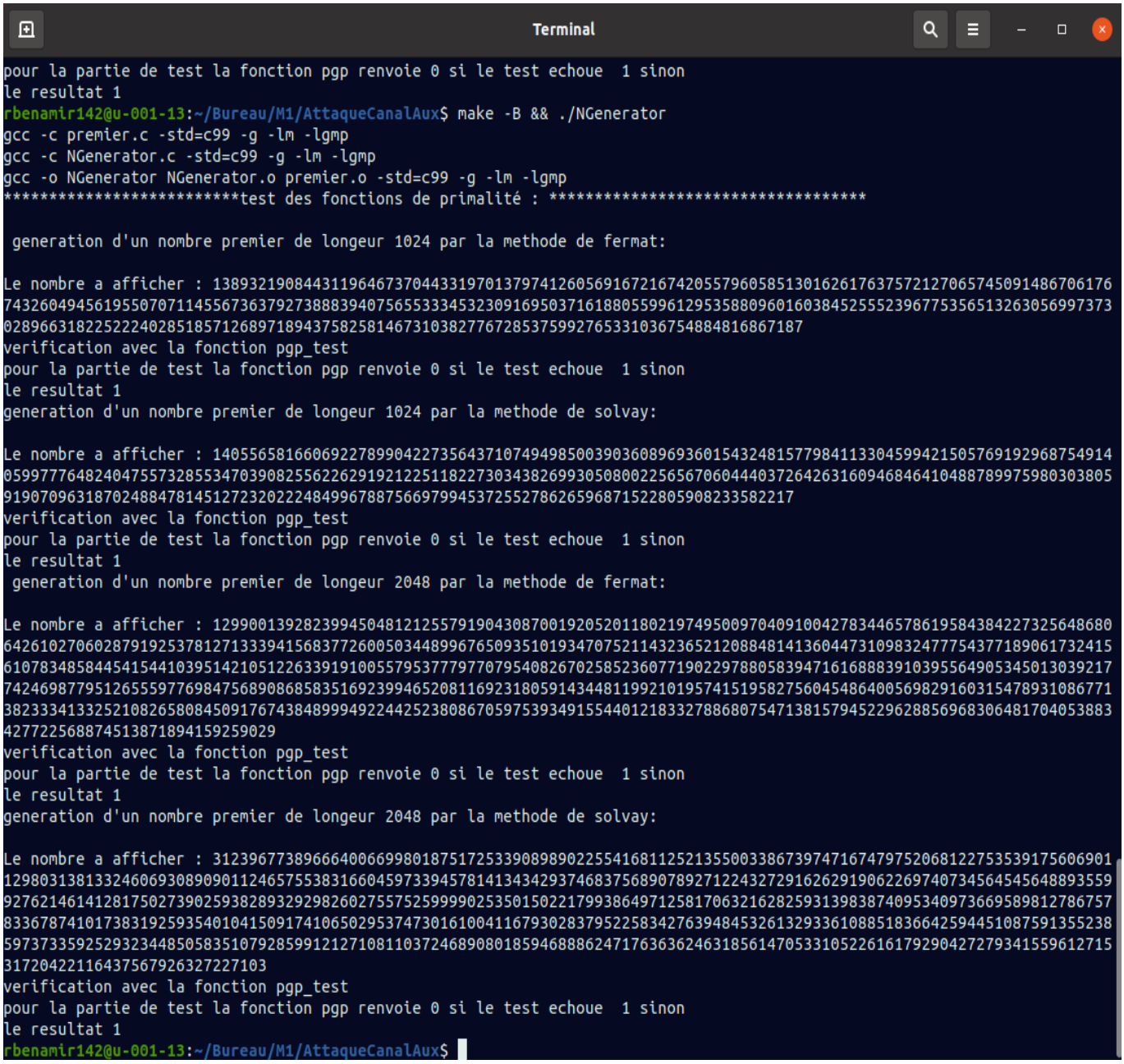
# 1 Generation nombres premiers

Dans cette partie, nous avons ecrits des fonctions de genrations de nombres premiers avec differentes methodes ainsi que des test de primalité pour verifier si les nombres qu'on a generer sont bien premiers.

Pour lancer le programme il suffit juste de tapper la ligne de commande suivante sur un terminal :

make -B && ./NGenerator

une fois cette ligne de commande tapée, vous aurez un affichage de plusieurs fonctions testées :




ici on vient bien que le resultat des test est toujours à 1, donc les nombres premiers qu'on a generé sont PROBABLEMENT premiers.

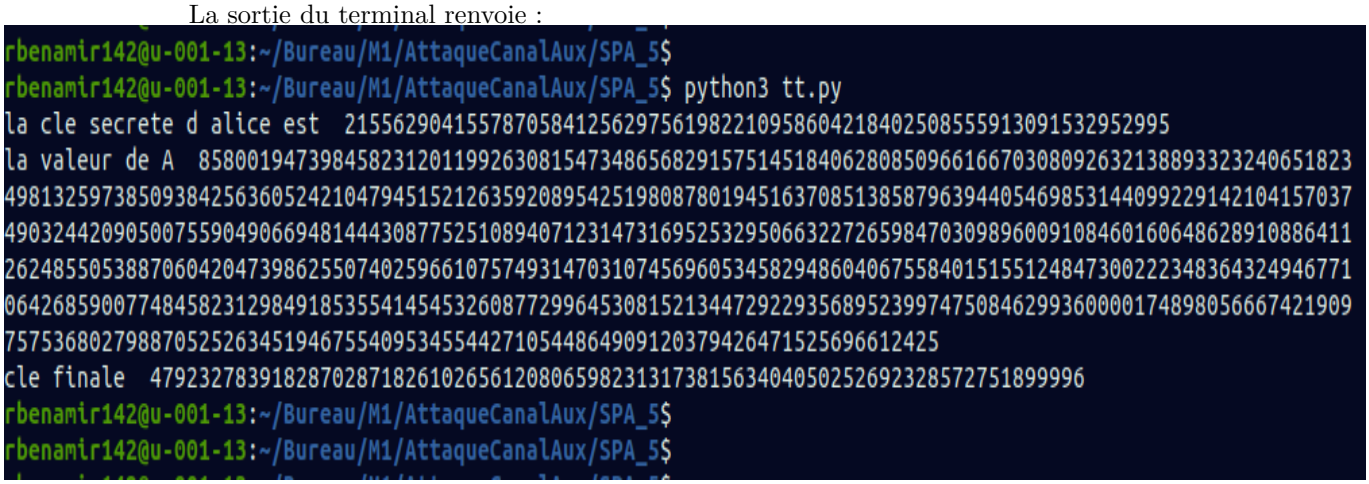
## 2 Attaque SPA

Pour analyser les traces, on a ecrit le script python suivant :

```
def moy(tab):
        """
        tab : liste d entiers
        retourne la moyenne du tab
        """
        return sum(tab)//len(tab)

def calcul_a(fichier):
        """
        fichier : contient les donnees a analyser
        retourne la valeur probable de la cle secrete d Alice
        """
        file = open(fichier, "r")
        lines = file.readlines()
        file.close()
        content = []
        for line in lines:
                content.append(int(line.strip()))
        i, n = 0, len(content)
        k = ""
        while i+55 < n:
                tmp = content[i:i+55]
                if moy(tmp) >= 65 :
                        i += 100
                        k+="1"
                else :
                        i += 45
                        k+="0"
        k = "".join(reversed(k))
        return int(k, 2)



if __name__ == "__main__":

        g=14789793378077042242120521274037173391261010897636027265546123991563081831117275602
        p=24614092481603675731022075504383970335861830446883656936098962383938382597155724410

        B=25223945747495863032358764904561433098045408795808991275832188309706519935701206243

        a = calcul_a('SPATrace.dat')
```

```
        print("la cle secrete d alice est " , a)
        A = pow(g, a, p)
        print("la valeur de A " , A)
        k = pow(B, a, p)
        inv = k% (2**256)
        print("cle finale ",inv)

        f = open('SecretKey.dat','w')
        f.write(str(hex(inv)))
        f.close()
```

La sortie du terminal renvoie :




pour analyser la fonction calcul_a, on a du faire des calculs pour arriver a trouver la longeur probable des trames pour la multiplication et celle du carré :

x = ( 149*(1+9/11)+75*9/11) = 16995(longeur du fichier SPATrace.dat)

pour arriver à conclure que les longeurs respectives 55 et 45.

On aurait pu utiliser à la place de POW de python des fonctions qu'on a ecrite :

***Pour cette premiere fonction on fait du left to right :

```
def left_to_right(g, e, N):
    binary = bin(e)[2:]
    t = 1
    n = len(binary)
    x = g
    while(t < n):
        x = (x**2)%N
        if binary[t] == '1' :
            x = (x*g)%N
        t = t + 1
    return x
```

***et pour cette deuxieme fonction on fait du right to left :

```
def expo_mod(g,e,n) : #right_to_left
    eb = bin(e)[2:]
    x = 1
    for i in range(len(eb)):
        if eb[i]=='1':
            x = (x*g)%n
        g = (g**2)%n
    return x
```

La clé ecrite dans le fichier SecretKey.dat est la suivante :
0x69f39d45b884225ed76e6d0ee843ba33939c6b16d1552149c3401b11046aed5c
Pour faire l'attaque on utilise la commande openSSl suivante : openssl aes-256-cbc -d -in output.cph -out output -pbkdf2 -pass file :SecretKey.dat
Cette commande prend en parametre le fichier output.cph, dechiffre avec la cle et ecrit le message en clair dans le fichier output.
Pour tester cette partie SPA il suffit de :
cd SPA_5/
python3 tt.py
ensuite on execute la commande openssl ci-dessus et on a l'image dans le fichier output :

```
 1 xxxxddddxxkkdc;:::::::ccllllllllllooollloooollllllllllollllllllllc:codxxddddddddddddxx0XXk::ccclccllllllllcoo
 2 xxddddddxkkxoc;;:::::::ccllllllllllllllllllllllllllllllllllllllllllcc:codxxdxxxddddddddx0XKxccccccccllllllll:'.
 3 dxxxdxxxxxxoc;;:::::::ccclllllllllllllllllllllllllllllollllllllllllcc::lddxxxxxxxddddddddx0XXOl:ccllllllll:'...
 4 xxxxxxxxxxxdc;;:::::::ccllllllllllllllllllllllllllllllllllllllllllccc:lodxxxxxxxddddddddOKX0occcllll;......
 5 xxxxxxxxxxxoc,;:::::::ccclllllllllllllllllllllllllllllllllllllllllccc:codddddddddddddddddodOKXKo:ccc;........
 6 xxxxdodxxxxdc,;;:::::::ccccllllllllllllllloodxxkkkkkxxdlcllllllllcccc:coodddddddddddddoooookKXXxc;..........
 7 xkxocldxxxxdc,,;;:::::::ccccllllllllollloooodxxkkOOOO00kdlcccccccc::codddddddddooooooooooooxKXK;...........
 8 kxo;,cdxxxxo:,,;;:::::::ccccccclllcccclllloooodxkkOOOOOOOOkoc:cc::::codddooooddoddooooddddxo'............
 9 dl;,;cdxxxxo:,,;;:::::::ccccccccllccccclllloooooodxOOOOOOOOKKKXk:;::::codddddl:;codddooooddddl'..........'';d
10 c;;;;cdxxxxo:,,;;:::::::ccccccllccccccccllooooooodxkkkO0KKK0KKKKXKl,;;;:oddddo;.'coddooodddc...........,:ldd
11 ;;;;;coxxxxo:,,;;:::::::ccccll:ccccccccllooooooooxkO0000000KKKKKKX0d,,:oddddo;..':odooodo,...........;lodxx
12 ;;;;;cdxxxxoc,,;;:::::::ccccx:::cccccllooooollldkOOOOO0000K0KKKKKKKX0;;lddddo:....:xkkkl...........'coodxxx
13 ;;;;;coxxxxo:,,;;;:::::::c:xd:::ccclllllllcoxkkkkkOOO0000000000K00KKKKXO:lddddo;..:d0KKXXk..........,oddxxxxx
14 ;;;;;coxxxxd:,,;;;:::::::ccc0l::::ccllllllloxxxxkkkOkOOOkOO000000000000KKK0xddddlloO00KKKKXK.........:dddxxxxdd
15 :::::coxkkkdc,,;;::::::::dOl::::ccclcloddodxxkkkkkkkkkkkOOOOOOO000000000OxkO000KK0K0KKXx.......'cddxxxxxddd
16 ::;;:coxkkkdc,,;;::::::::;kOdlc::ccclodooodddddxxxkkkkkkkkkkkOOOOOOkkkkkOO000000000K0k0KK;......'lddxxxxxxxdx
17 ;;;;:cdxkkkdc,,;:::;;::::;Okxooc::clolllododdddxxxxxxxxxxxkkkkkkkxkkkO000000000KKOxxdOl......,oddxxxxxxxxxx
18 ;;;;:ldxkkkdc,,;;;;;;;;;;0OkddocllllloollooddoolllddoddddddldxxkOO00OOO00000KKKOollxx......,oddxxxddxddddd
19 :::::ldxkkkdc,,;;::::::;;O0Odlocccloollllooolllc:,;lc;;;,'..;dkO0000000000KOxoc::oxo......'oddxxxxxddddddd
20 :::::ldxkkkdc,,;;;;:;;;;oK0xoolclllllllloocc;,'..;;';;'''':dxOOOOOOOOO0OxoocCloxkl.......'lddxxxxxxddddddd
21 :::::cdxkkkdc,,;;;;;;:::;xKOkocllclllll;;,'.''.,..,,,,:dkOOOOkkkOOOOc,;ccdxkxc.........codxxxxxxxxxxdddd
22 ::::;coxkkkxc,,;;;;;;;;c:;kKOolccllcc,'',',.,,....',;ldOOOkkkkkOO000x;,;cod;.........'cloxxxxxxxxxxxxddd
23 ::::;coxkkkxl,,;;:::::ccc:oKdccccccc:''....'.',,..'coddkOkxkkxkO000KKOl'.,ol..........cooddxxxxxxxxxxxxdd
24 :::;;coxkkkxl,,;::::::ccccckoclll;'..'......,',:dkOkdOOxxxxkO000KKKKx;..:o.........;ooxxxddddddddddddddd
25 :::;;:oxkkkxl,,;::::::ccc11:cllc,'.'..'....''.;lxxxOOxdodxkkkOO000KKKOc..'d,........,ooxxxxxxxxddddddooddd
26 :::::;oxkkkxl,,;::::::ccodc';l,','',......'..cdkOkkxolcl:;:oxkO0OOkdl:;...o:.'.....lodxxxxddxxddddddddooo
27 :;;;,:oxkkkxl,,;;:;;;cxoddl;.'',,;...'.''...lxk0Oo,....:;'clodk00l,';.....lc''....;odxxddddddddddddddoooo
28 :;;;,;oxkkkxl,,::::,,:xkl,'''.'';:........,lxO0xlc:,::ckOlccldOXd::cd,....cl,'...'loddddddddddddddooooodx
29 :;;,';oxkOOxl;;:::ccl::'.,:;..,,:c;......,lkOxccodddooodxxolloOXOdol:;,...:x;....coddddddddddddooooodkOOOO
30 ;,,,.,lxkOOxl,;:clll:;'',:;'..',:,:,....:okk:;clodxkkkkkkxdollkX0kdolc;...;x;...,odxddddddddoooooxO000000
31 ,,''.,lxkkkxl,;::lc;;;,,,c'.......:c,..:oOd'.;cloddxkkkkxdoollxKKxdoll,...,dc...loxxddddddoooook000000K0
32 ,,''.'lxkkkxl,,cll,;:,';;c,....',:c;'.;oOl..';clloddxxxxxollllldOXxdol:..'..do..;odxddddddddoook0000KKKKK
33 ,,''.,lxkkkxl;;::;,;:';';c:,....':...dxo;...,;clloodddxxdollcclx0xdoc...'..cd,.odxddddddddoook000KKKKKKK
34 ,,,'':oxkkkxo,,;cc',,,',;:cc.':..;:l:ol....'::clloooddddxddooddxOkdol'..',..,d;:ddddddddddooodO00KKKKKKK
35 '''''cdxkkkko,,:c:':'.''',,cc;.;cxxcc,......:;clloooooodddddkOOOxol'...'''..ocodddddddddooolx00KKKKKKKK
36 ..'.,cdxkkOko:::l;.'.'.::;;;;;lo0occ.......;,:llloooocccllllldolll,....',...loddddddddddooolkKKKKKKKKKK
37 ....,:oxkkOko;,c:';..',l;;;::loddo;.......'.'',:ccllooollllodddol'.....,,''.cddddddddddddoollOKKKKKKKKKK
38 ...'::oxkkkxo,;:,',.'.,l:l:;c::xo'..........'',;:clloooddxdddc'......,,''.cxddddddddddooll0XXKKKKKKKK
39 ...';coxkkkko,;;.,'.'.'l';cccocc'...'.........'.',:cllodxxxxdo'.......;,,''cxooddddddddooldKXKKKKK0kdl
40 ....,;lxkkkxoc:;.''....cc,;cccl:l;..'..........,;ccllooddddxkkdl:'...';,,,'ldcccccllloollckKKKKK0Oo,..'
41 l:,'..:dkkkko::...,'.;,.;:c:;:ccl;;''.'.........,:cllloooodxOO0000kl'.,,','loooollcc::::c;kKKKKOl,'',,,
42 lool,.:dkkkxxo,...'',''.;'',:coc;c:'.'......';.'ccllooooodxxkOOO00KKKd,.''.ooddooooolllclll0KKKk;';;;:;;
43 .cxxc.:xkkkxdc.......;...',,;;;col'lc........'c,.:llooooodddxxkkOO00KKX0;..,ddddooooolllodOKKKO:,;:::;::
44 .,xxc.;xkkkkdc......,;.....',:,:ol,lc.''.....;c;'clloooooodddxxkkOO0KKKXK,.:ddddoooollld0KKXKOl;;:c:;:::
45 .'dkl.;xkkkkd:.....,,.....''::ll::c,,,'....;cl;,clooooooooddxxxkOO00KKKXk.lodooooooolllkKKKX0o:;:c:;:::;;
46 ..oko.;dkkkkd:............'''':c::;,...''..,cll,:looooooooodddxxxkO00KKKKKlooooooooolloxO0XKdc:;;;;:::;;;
47 ..cxd,;dkkkkdc'.......'.....,:'',':;.....':cl,,looooooooooodddxxkkO00KKKK0l;;:ccllooddodKKkc;;;,;:;;;;'
48 ..ckx:,okkkko:'.......'.....;l:;;.......,:cc',looooooooooooodddxxkkO00KKKXx;;;,,'..,oOxOKO:'',,:;;;:;'.
49 ;;lkkl;okkOkl:........'.....',c:;.....,::,';llooooooooooooooddxxkkO0KKKKKl;::;;'..dKOko,.',;:,,;::;'.
50 ';cxko:okkOkl,.....'..,.;'.','::'.....',,;:clllooooooddooooooddxxkOO00KKKO;;:::::::lxl;,',,:;'';c:;''.
51 ..,x0klokkOkc.........,.;:',',';,...';:ccclllllloooooooddddddddddddxkkOO00KKKl,;:ccccc::c:;;;,',:cc;'...
```