CHIFFREMENT AFFINE [CORRECTION]

A. Chiffrer

… ikgun

B. Déchiffrer

1. Un exemple

On cherche x tel que $4 \equiv 11x + 8$ [26], c'est-à-dire tel que $11x + 4 \equiv 0$ [26].
$11x \equiv -4$ donc $11x \equiv 22$ donc i=2 convient

2. Cas général

On cherche x tel que $11x + 8 \equiv y$ [26], autrement dit tel que $11x \equiv y - 8$ [26].

a) $u_0 = -7$ et $v_0 = -3$ avec l'algorithme d'Euclide (coefficients de Bézout).
On a donc : $11u_0 \equiv 1[26]$.

b) $11x \equiv y-8[26]$ donc $11xu_0 \equiv (y-8)u_0[26]$ donc $11 \equiv (y-8)u_0[26]$

c)

```
def decodage(message):
    mescode = ""
    for c in message:
        if c==" ":
            mescode=mescode + " "
        else:
            x=(num(c)-8)*(-7) % 26
            mescode=mescode + lettre(x)
    return mescode
```

d) « ehgegzij » corespond à « chocolat »
Le texte à déchiffrer donne :

> un zoologiste qui en afrique a observe de pres les gorilles s etonne de l uniformite de leur vie et de leur grand desoeuvrement des heures et des heures sans rien faire ils ne connaissent donc pas l ennui cette question est bien d un homme d un singe occupe loin de fuir la monotonie les animaux la recherchent et ce qu ils redoutent le plus c est de la voir cesser car elle ne cesse que pour etre remplacee par la peur cause de tout affairement l inaction est divine c est pourtant contre elle que l homme s est insurge lui seul dans la nature est incapable de supporter la monotonie lui seul veut a tout prix que quelque chose arrive n importe quoi par la il se montre indigne de son ancetren le besoin de nouveaute est le fait d un gorille fourvoye emil cioran

ce qui donne :

> Un zoologiste qui, en Afrique, a observé de près les gorilles, s'étonne de l'uniformité de leur vie et de leur grand désœuvrement. Des heures et des heures sans rien faire... Ils ne connaissent donc pas l'ennui?
> Cette question est bien d'un homme, d'un singe occupé. Loin de fuir la monotonie, les animaux la recherchent, et ce qu'ils redoutent le plus c'est de la voir cesser. Car elle ne cesse que pour être remplacée par la peur, cause de tout affairement.
> L'inaction est divine. C'est pourtant contre elle que l'homme s'est insurgé. Lui seul, dans la nature, est incapable de supporter la monotonie, lui seul veut à tout prix que quelque chose arrive, n'importe quoi. Par là, il se montre indigne de son ancêtre: le besoin de nouveauté est le fait d'un gorille fourvoyé. [Emil CIORAN]

C. Clés possibles

1. Si a et 26 sont premiers entre eux, on peut trouver u_0 comme précédemment et donc en déduire que $x \equiv (y-8)u_0\,[26]$.

2. Si a et 26 ne sont pas premiers entre eux, alors il existe $d > 1$ tel que d divise a et 26.
Or les diviseurs de 26 sont 1, 2, 13 et 26.
Donc $d = 2$ ou $d = 13$ puisque $a < 26$.

Si $d = 13$ alors $a = 13$ et en posant $x = 7$ et $x' = 5$ (par exemple) on a :
$ax+b = 13\times 7+b \equiv b\,[26]$ et $ax'+b = 13\times 5+b \equiv b\,[26]$
donc x et x' sont codés par la même lettre, ce qui pose problème.

Si $d = 2$ alors a est pair, $a = 2k$ et en posant $x = 23$ et $x' = 10$ (par exemple) on a :
$ax+b = 2kx+b = 46k+b \equiv 20k+b\,[26]$ et $ax'+b = 2kx'+b = 20k+b$
donc x et x' sont codés par la même lettre, ce qui pose problème.

3. Il n'existe que 12 entiers compris entre 0 et 26 et premiers avec 26 (1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 et 25). Il n'existe donc que 12 × 26 = 312 clés de chiffrement possibles.
Si l'on sait qu'un chiffrement affine a été utilisé, on peut casser le code par force brute en essayant les 312 clés.

```
def bezout(a,b):
    r1, u1, v1 = a, 1, 0
    r2, u2, v2 = b, 0, 1
    while r2 != 0:
        q = r1//r2 # quotient de r1 par r2
        rt, ut, vt = r1, u1, v1 # rt = r_temporaire; etc.
        r1, u1, v1 = r2, u2, v2
        r2, u2, v2 = (rt-q*r2), (ut-q*u2), (vt-q*v2)
    return u1,v1

def num(caractere): #pour convertir les caractères en nombres
    return ord(caractere)-65-32 #les majuscules commencent à 65, les minuscules à 32

def lettre(n):
    return chr(n+65+32)

def decodage(message, a, b, u0):
    mescode = ""
    for c in message:
        if c==" ":
            mescode=mescode + " "
        else:
            x=(num(c)-b)*u0 % 26
            mescode=mescode + lettre(x)
    return mescode

message = " " #écrire le message à décoder dans cette variable

listea = [1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25]

for a in listea:
    for b in range(0,25):
        u0 = bezout(26,a)[1]
        message_decode = decodage(message, a, b, u0)
        print("a=",a," et b=",b,'\n',message_decode,'\n')
```