cryptanalyse chiffrement affine

'lqdmadtfkahuhqutadnkxxutesdstqutrqmadtfkalsrpqumqdtmq
psstnawulsfswrpulsxkatmlshsfmstladsqtwkmrnsfsmaudtqdtsd
kdrpamyaadtfkamsedamqxpkddsavmqdmfusdrkafmqmmskufd
umafyakuwqdgsfestqutadtfkalsnkxxutesyauuwrpuyaspsekdzkf
tbfftkpiusdxupxkpsnkxxut'

Cryptanalyse

On cherche la clé $(\boldsymbol{a}, \boldsymbol{b})$ *qui a permis de transformer chaque lettre de rang* $\boldsymbol{i}$ *en une lettre de rang j par la formule :* $\boldsymbol{j} = (\boldsymbol{ai} + \boldsymbol{b})[\mathbf{26}]$

Cryptanalyse

On cherche la clé $(\boldsymbol{a}, \boldsymbol{b})$ *qui a permis de transformer chaque lettre de rang* $\boldsymbol{i}$ *en une lettre de rang j par la formule :* $\boldsymbol{j} = (\boldsymbol{ai} + \boldsymbol{b})[\mathbf{26}]$

Nous avons surtout besoin de décoder le message c'est-à-dire d'exprimer $\boldsymbol{i}$ en fonction de $\boldsymbol{j}$:

$$\boldsymbol{j} = (\boldsymbol{ai} + \boldsymbol{b})[\mathbf{26}] \Longrightarrow \boldsymbol{i} = \boldsymbol{a}^{-\mathbf{1}}(\boldsymbol{j} - \boldsymbol{b})[\mathbf{26}] = (\boldsymbol{a}^{-\mathbf{1}}\boldsymbol{j} - \ \boldsymbol{a}^{-\mathbf{1}}\boldsymbol{b})[\mathbf{26}]$$

$$\boldsymbol{i} = (\boldsymbol{\alpha j} + \boldsymbol{\beta})[\mathbf{26}] \quad \text{avec} \quad (\boldsymbol{\alpha}, \boldsymbol{\beta}) = (\mathbf{a}^{-\mathbf{1}}, -\mathbf{a}^{-\mathbf{1}}\mathbf{b})$$

$\mathbf{a}^{-\mathbf{1}}$ étant l'inverse de a dans $\mathbb{Z}/\mathbf{26}\mathbb{Z}$

Analyse fréquentielle

```
from collections import Counter
c=Counter(cryptogramme)
freq=c.most_common(10)
freq
```

```
[('s', 27),
 ('d', 22),
 ('a', 22),
 ('t', 21),
 ('u', 20),
 ('k', 18),
 ('m', 17),
 ('f', 15),
 ('q', 14),
 ('x', 10)]
```

E	A	I	S	T	N	R	U	L	O	D	M	P	C	V	Q
15,9%	9,4%	8,4%	7,9%	7,3%	7,2%	6,5%	6,2%	5,3%	5,1%	3,4%	3,2%	2,9%	2,6%	2,2%	1,1%

On suppose que la lettre la plus fréquente ‘s’ correspond à ‘e’
(cela marche souvent, mais pas toujours…)

Rang(‘s’) = 18
Rang(‘e’) = 4

```
[('s', 27),
 ('d', 22),
 ('a', 22),
 ('t', 21),
 ('u', 20),
 ('k', 18),
 ('m', 17),
 ('f', 15),
 ('q', 14),
 ('x', 10)]
```

On suppose que la lettre la plus fréquente ‘s’ correspond à ‘e’
(cela marche souvent, mais pas toujours…)

Rang(‘s’) = 18
Rang(‘e’) = 4

$$\boldsymbol{i = (\alpha j + \beta)[26] \implies 18\alpha + \beta = 4\ [26]}$$

```
[('s', 27),
 ('d', 22),
 ('a', 22),
 ('t', 21),
 ('u', 20),
 ('k', 18),
 ('m', 17),
 ('f', 15),
 ('q', 14),
 ('x', 10)]
```

On suppose que la lettre la plus fréquente ‘s’ correspond à ‘e’ (cela marche souvent, mais pas toujours…)

Rang(‘s’) = 18
Rang(‘e’) = 4

$$i = (\alpha j + \beta)[26] \implies 18\alpha + \beta = 4\ [26]$$

```
[('s', 27),
 ('d', 22),
 ('a', 22),
 ('t', 21),
 ('u', 20),
 ('k', 18),
 ('m', 17),
 ('f', 15),
 ('q', 14),
 ('x', 10)]
```

Pour ‘d’, la deuxième lettre la plus fréquente, nous pouvons tester les lettres suivantes : ‘a’, ’i’, ’s’, ’t’,’n’

E	A	I	S	T	N	R	U	L	O	D	M	P	C	V	Q
15,9%	9,4%	8,4%	7,9%	7,3%	7,2%	6,5%	6,2%	5,3%	5,1%	3,4%	3,2%	2,9%	2,6%	2,2%	1,1%

Deuxième lettre

Rang(‘d’) = 3

Si choix de ‘a’ : Rang(‘a’) = 0 $\Longrightarrow \cdots \alpha + \cdots \beta \equiv \cdots \ [26]$

Si choix de ‘i’ : Rang(‘i’) = 8 $\Longrightarrow$

Si choix de ‘s’ : Rang(‘s’) = 18 $\Longrightarrow$

Si choix de ‘t’ : Rang(‘t’) = 19 $\Longrightarrow$

Si choix de ‘n’ : Rang(‘n’) = 13 $\Longrightarrow$

Deuxième lettre

Rang(‘d’) = 3

- **Si choix de ‘a’ : Rang(‘a’) = 0** $\Longrightarrow 3\alpha + \beta = 0\ [26]$
- **Si choix de ‘i’ : Rang(‘i’) = 8** $\Longrightarrow 3\alpha + \beta = 8\ [26]$
- **Si choix de ‘s’ : Rang(‘s’) = 18** $\Longrightarrow 3\alpha + \beta = 18\ [26]$
- **Si choix de ‘t’ : Rang(‘t’) = 19** $\Longrightarrow 3\alpha + \beta = 19\ [26]$
- **Si choix de ‘n’ : Rang(‘n’) = 13** $\Longrightarrow 3\alpha + \beta = 13\ [26]$

Exemple de résolution d’un système ?

$$\begin{cases} 18\alpha + \beta = 4\ [26] \\ 3\alpha + \beta = l\ [26] \end{cases}$$

Exemple de résolution d'un système

$$\begin{cases} 18\alpha + \beta = 4\ [26] \\ 3\alpha + \beta = l\ [26] \end{cases} \Longrightarrow 15\alpha = (4 - l)\ [26] \Longrightarrow \alpha = 15^{-1}(4 - l)\ [26]$$

Exemple de résolution d'un système

$$\begin{cases} 18\alpha + \beta = 4\ [26] \\ 3\alpha + \beta = l\ [26] \end{cases} \Longrightarrow 15\alpha = (4 - l)\ [26] \Longrightarrow \alpha = 15^{-1}(4 - l)\ [26]$$

$$15^{-1} = 7[26] \Longrightarrow \alpha = 15^{-1}(4 - l)[26] = 7(4 - l)[26]$$

$$\alpha = 28 - 7l\ [26] = 2 - 7l\ [26]\ \ ou\ \ 2 + 19l[26]$$
$$\beta = 4 - 18(2 - 7l)[26] = -32 + 105l\ [26] = 20 + 22l[26]$$

Exemple de résolution d'un système

$$\begin{cases} 18\alpha + \beta = 4\ [26] \\ 3\alpha + \beta = l\ [26] \end{cases} \Longrightarrow 15\alpha = (4 - l)\ [26] \Longrightarrow \alpha = 15^{-1}(4 - l)\ [26]$$

$$15^{-1} = 7[26] \Longrightarrow \alpha = 15^{-1}(4 - l)[26] = 7(4 - l)[26]$$

$$\alpha = 28 - 7l\ [26] = 2 - 7l\ [26]\ \ ou\ \ 2 + 19l[26]$$
$$\beta = 4 - 18(2 - 7l)[26] = -32 + 105l\ [26] = 20 + 22l[26]$$

Lettre	'a'	'i'	's'	't'	'n'
l	0	8	18	19	13
(α, β)	(2,20)				
Début du décodage	qaasuageou				

Exemple de résolution d'un système

$$\begin{cases} 18\alpha + \beta = 4\ [26] \\ 3\alpha + \beta = l\ [26] \end{cases} \Longrightarrow 15\alpha = (4 - l)\ [26] \Longrightarrow \alpha = 15^{-1}(4 - l)\ [26]$$

$$15^{-1} = 7[26] \Longrightarrow \alpha = 15^{-1}(4 - l)[26] = 7(4 - l)[26]$$

$$\alpha = 28 - 7l\ [26] = 2 - 7l\ [26]\ \ ou\ \ 2 + 19l[26]$$
$$\beta = 4 - 18(2 - 7l)[26] = -32 + 105l\ [26] = 20 + 22l[26]$$

Lettre	'a'	'i'	's'	't'	'n'
l	0	8	18	19	13
(α, β)	(2,20)	(24,14)	(6,0)	(25,22)	(15,20)
Début du décodage	qaasuageou	siiqoiceuo	ossuaskeia	lgtkwtdrmw	dansuntrou

Message décodé

'dansuntrouvivaitunhobbitcenetaitpasuntroudeplaisantsaleethumidere
mplideboutsdeversetduneatmospheresuintantenonplusquuntrousecnu
sablonneuxsansrienpoursasseoirnisurquoimangercetaituntroudehobbit
cequiiimpliqueleconfortjrrtolkienbilbolehobbit'