Théorie des nombres et application à la cryptographie: Midterm

Joris LIMONIER

Le 30 Avril 2021

1 Exercice 1

1.1 Partie (a)

Nous applicons l'algorithme d'Euclide:

$$\begin{aligned} 495 &= 7 * 68 + 19 \\ 68 &= 3 * 19 + 11 \\ 19 &= 1 * 11 + 8 \\ 11 &= 1 * 8 + 3 \\ 8 &= 2 * 3 + 2 \\ 3 &= 1 * 2 + 1 \\ 2 &= 2 * 1 + 0 \end{aligned}$$

Puis nous remontons la chaine d'inégalité

$$\begin{aligned} 1 &= 3 - 1 * 2 \\ &= 3 - 1 * (8 - 2 * 3) \\ &= 3 * 3 - 1 * 8 \\ &= 3 * (11 - 1 * 8) - 1 * 8 \\ &= 3 * 11 - 4 * 8 \\ &= 3 * 11 - 4 * (19 - 1 * 11) \\ &= 7 * 11 - 4 * 19 \\ &= 7 * (68 - 3 * 19) - 4 * 19 \\ &= 7 * 68 - 25 * 19 \\ &= 7 * 68 - 25 * (495 - 7 * 68) \\ &= 182 * 68 - 25 * 495 \end{aligned}$$

Nous avons donc que

$$\begin{aligned} & 182 * 68 - 25 * 495 = 1 \\ \implies & -25 * 495 \equiv 1 \mod 68 \\ \implies & 43 * 495 \equiv 1 \mod 68 \end{aligned}$$

Ainsi, 43 est l'inverse de a dans $\mathbb{Z}/68\mathbb{Z}$

1.2 Partie (b)

Ce problème revient à trouver la quantité suivante

$$3^{1607} \equiv 187 \mod 100$$

D'abord nous avons que

$$\varphi(100) = 2^{2-1} * (2-1) * 5^{2-1} * (5-1) = 40$$

Nous invoquons le théorème d'Euler. Nous avons

$$1607 = 1600 + 7 = 40 * 40 + 7 \equiv 7 \mod 40$$

Donc, par l'identité d'Euler, on a

$$3^{1607} \equiv 3^7 = 2187 \equiv 187 \mod 100$$

2 Exercice 2

2.1 Partie (a)

L'élément en position 3 passe en position 5, le 5 passe en 1, le 1 en 3 d'une part. D'autre part, le 2 passe en position 4 et le 4 en 2.

$$ralepibtyamoencecmen$$

2.2 Partie (b)

On procède similairement à la partie (a) pour obtenir

$$cestlemidtermparty$$

3 Exercice 3

3.1 Partie (a)

Voilà le nombre d'apparition de chaque lettre dans le message chiffré.

Lettre	Fréquence
c	1
g	3
h	2
j	1
l	1
m	1
p	1
q	2
r	4
s	6
u	1
v	2
w	4
x	2
y	8

Les autres lettres n'apparaissent pas. Le y est le plus fréquent, ensuite c'est le s. Si nous identifions le y avec le E, nous avons une clef de 20, ce qui signifie que les s, qui sont également très nombreux, seraient chiffrés en Y. Cela paraît peu probable.

Mais nous savons que les clefs trop courtes peuvent ne pas être représentatives des fréquences de lettres dans la langue française. Nous estimons donc qu'il n'est pas possible de déchiffrer ce message avec si peu d'information.

3.2 Partie (b)

Avec ces informations supplémentaires, nous avons que les O ont été chiffrés en s, c'est à dire une clef de 4. De même, U ont été chiffrés en y.

En conservant cette même clef, nous avons que les quatre premières lettres du message chiffré nous donnent:

$$r \to N$$
$$s \to O$$
$$y \to U$$
$$w \to S$$

Ainsi, les quatre premières lettres du message déchiffré sont

$$NOUS$$

L'exercice est terminé mais dans un élan d'engouement, nous déchiffrons le texte entier, qui est:

$$NOUSCROYONSTOUSQUILFUTUNDUCHORSDUCOMMUN$$

4 Exercice 4

4.1 Partie (a)

Nous voulons exprimer α^{10} dans la base $1, \alpha, \alpha^2, \alpha^3$.
Comme $\mathbb{F}_{81}$ est de degré 4 sur $\mathbb{F}_3$, on cherche un polynôme irréductible de dergré 4, qui admettra nécessairement une racine dans ce corps.
Puisque α est une racine de f dans $\mathbb{F}_{81}$, on a que

$$\alpha^4 + \alpha^3 - 1 = 0 \tag{1}$$

D'où

$$\alpha^5 = 1 - \alpha^3$$

Ainsi,

$$\begin{aligned} \alpha^{10} &= \left(\alpha^5\right)^2 \\ &= \left(1 - \alpha^3\right)^2 \\ &= 1 + \alpha^6 - 2\alpha^3 \end{aligned}$$

Nous devons évaluer α^6. Pour cela nous multiplions (1) par α^2 pour obtenir

$$\alpha^6 = \alpha^2 - \alpha^5$$

Alors nous avons

$$\begin{aligned} \alpha^{10} &= 1 + \alpha^6 - 2\alpha^3 \\ &= 1 + (\alpha^2 - \alpha^5) - 2\alpha^3 \\ &= 1 + \alpha^2 - (1 - \alpha^3) - 2\alpha^3 \\ &= \alpha^2 - \alpha^3 \end{aligned}$$

4.2 Partie (b)

Nous savons que $\mathbb{F}_{81}^{\times}$ est un groupe cyclique d'ordre $3^4 - 1 = 80$, donc l'ordre de θ est un diviseur de 80. Or, comme $\theta = \alpha^2 - \alpha^3$ ...

4.3 Partie (c)