TD1 - cryptologie

Exercice 1

1.

2.

3.

4.

5.

6.

Type	Accès
France	Libre
Fr $\leftrightarrow$ UE[1]	Libre
Fr $\leftrightarrow$ UE[2]	Déclaration préalable
Fr $\leftrightarrow$ UE[3]	???

Exercice 2

1.

$31 \bmod 26 = \{31 + 26k, k \in \mathbb{Z}\}$. Il représente l'ensemble des entiers ayant pour reste 5 lors de la division euclidienne par 26

2.

$\star$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	0	0	0	0	0	0	0	0	0	8	0
3	0	0	0	0	0	0	0	0	0	0	6	0
4	0	0	0	0	0	0	0	0	0	0	4	0
5	0	0	0	0	0	0	0	0	0	0	2	0
6	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0

À finir yipeeeeeeee

[1] Authentification
[2] Intégrité
[3] Confidentialité

Exercice 3

1. Ensemble muni d'une loi de composition interne associative, avec un élément neutre et dont tout élément est inversible

2. Soit $n \in \mathbb{N}$, soit $k \in \mathbb{Z}/n\mathbb{Z}$

3. Un groupe est cyclique s'il est monogène fini.

4. Soit $n \in \mathbb{N}$, soit A un groupe de cardinal n Comme $\text{card}(\mathbb{Z}/n\mathbb{Z}) = \text{card}(A) = n$, il existe une bijection $A \to \mathbb{Z}/n\mathbb{Z}$ Par conséquent, les groupes sont isomorphes

5. Un groupe $(A, +, e)$ est commutatif si
$\forall (a, b) \in A^2, a + b = b + a$

Exercice 4

1. On encode le texte en permutttant chaque caractère avec une lettre du même alphabet. Pour ce faire, on utilise les permutations. la clé est l'alphabet d'arrivée

2.

Exercice 5

1. **2.** VOUSAVEZDEJAQUELQUESPOINTS **3.** NIIAEHWMTZXGTMKBIGQCGKIDCQC **4.**

Exercice 6

1. $\text{IC} = \sum_{q=A}^{Z} \frac{n_q(n_q-1)}{n(n-1)}$ **2.**

```
def IC(nqs : list) -> float:
  n = len(nqs)
  return sum(nq*(nq-1) / (n*(n - 1)) for nq in nqs)

print(IC([8.08, 1.67, 3.18, 3.99, 12.56, 2.17, 1.80, 5.27, 7.24, 0.14, 0.63, 4.04,
2.60, 7.38, 7.47, 1.91, 0.09, 6.42, 6.59, 9.15, 2.79, 1.00, 1.89, 0.21, 1,65,
0.07,]))

>>> 6.7234367521367515
```

3. Preuve:
l'addition est commutative

Exercice 7

1. Consister à deviner la clé grâce aux répétions de motifs présents dans le texte chiffré

2.

BEAV: décalage de 5
YEA: décalage de 29
JOO: décalage de 108

Pas de diviseur clair, on ne peut pas conclure

3.

Exercice 8

1. Couper le texte en bloc de 4
On calcule les ICM (déjà donnés dans le tableau). On a alors:

$$\begin{cases} d_0 = d_1 + 1 \\ d_0 = d_2 + 11 \\ d_0 = d_3 + 3 \\ d_1 = d_2 + 10 \\ d_1 = d_3 + 2 \\ d_2 = d_3 + 18 \end{cases} \Rightarrow \begin{cases} d_1 = d_0 - 1 \\ d_2 = d_0 - 11 \\ d_3 = d_0 - 3 \end{cases}$$

On veut déterminer d0. On fait comme pour Cesar, sur le texte composé de la première colonne. C et T sont les lettres les plus fréquentes $\Rightarrow d_0 = 24 \mid d_0 = 15$

Après test $d_0 = 15$, la clé est donc “POEM”

Exercice 9

Exercice 10

Exercice 11

Exercice 12

Exercice 13

1.

Clé $K_3 = K_1 + K_2$

2. $e = e_0$ où 0 est la clef qui déplace pas $e_K \circ e_{-K} = e_0$ avec e_{-K} l'application qui déplace de l'opposé de e_K
1. commutatif et associatif car + a ces propriétés dans $\mathbb{Z}/26\mathbb{Z}$

3. Elle doit chiffrer une dernière fois

4. $S_2 = S_1 + K_2$ donc $K_2 = S_2 - S_1$. On peut refaire ça avec toutes les clefs

5. Il faut qu'on ne puissse pas déduire la clé d'un couple de clair / chiffré

6. C'est un chiffrement parfait incassable. Pas possible car pour chiffrer et déchiffrer la même clef est utilsée, contraire au règles de OTP

7.

Exercice 14

Exercice 15

1.

$a = 170 = 17 \times 10 = 13 \times 9 \times 2 \times 5 = 2 \times 3^2 \times 5 \times 13$
$b = 330 = 33 \times 10 = 11 \times 3 \times 5 \times 2$

...

$D(330) \cap D(1170) = \{1, 2, 3, 5, 6, 10, 15, 30\}$

2. $\text{pgcd}(a,b) = \max(D(330) \cap D(1170)) = 30$

3. après calculs 53

4. après calculs 53

5. $\text{pgcd}(a,b) = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}, au + bv = 1$

6. $\text{pgcd}(a,b) \times \text{ppcm}(a,b) = ab$

Exercice 16

1. $\min(\{k, k \in \mathbb{N}, [k]g = [0]g\}) = | < g > |$

2. Utiliser formule question 4.

3.

4.

Exercice 17

1. Supposons que a est inversible et diviseur de 0.
a est inversible, on note a^-1 son inverse.
a est diviseur de 0, donc on dispose de $b \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ tq $ab = 0$
$a^{-1}ab = (a^{-1}a)b = b$

$= a^{-1}(ab) = 0$

Or $b \neq 0$, impossible

Soit a divisieur de 0. On dispose de $b \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ tq $ab = 0$

blablabla

$b = \frac{n}{\text{pgcd}(a,n)}$

2. apparemment $\left\lfloor \log_{\varphi(1014)} \right\rfloor = 14$

$O(\log(1014)\log(5005))$ opérations

(deux dernières colonnes du tableau plutot fausses)

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
−1					1	0
0			5005	1014	0	1
1	5005	4	1014	949	1	−4
2	1014	1	949	65	−1	5
3						
4						
5						
6						

$$u_i = u_{i-2} - q_i \times u_{i-1}$$
$$v_i = v_{i-2} - q_i \times v_{i-1}$$

ici $\text{pgcd}(5005, 1014) = 13$
et $31 \times 5005 - 153 \times 1014 = 13$

de plus $r_i = u_i \times a + v_i \times b$

3.

D'autre part comme $au + bv = 1$, u est l'inverse de a modulo b et v l'inverse de b modulo a

à la dernière ligne, on obtient les diviseurs de 0

4. Algo d'euclide étendu, si PGCD > 1, il existe un diviseur de 0. $O\big((\log(n))^2\big)$