

FEUILLE D'EXERCICES n° 3

Cryptographie classique 1

On rappelle la numérotation des lettres de l'alphabet :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Exercice 1 –

- 1) Coder le message **Rendez-vous à la cafétéria** à l'aide du chiffrement par décalage et de la clé $K = 5$.
- 2) Décoder le message **RGNEIDVGPEWXTRAPHHXFJT** sachant qu'il a été créé par un chiffrement par décalage.

Exercice 2 – Les lettres les plus fréquentes dans un message codé sont K et O. En français les lettres les plus fréquentes sont A (8.4%) et E (17.26%). Sachant que le message est en français, codé en utilisant un chiffrement par décalage, déterminer la clé et déchiffrer le début du message : **SVOXFYIKNKXCVKVSQEB SOKMRODOBNOCYV NKDC**.

Exercice 3 –

- 1) Coder le message **Rendez-vous à la cafétéria** à l'aide du chiffrement par substitution et de la clé
- | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T | S | F | L | R | C | V | M | U | E | K | J | D | I |
- 2) Est-il possible de décoder le message **YHVMQVVMH** codé par un chiffrement par substitution sans connaître la clé. Décoder ce message sachant qu'il a été créé avec la clé précédente.

Exercice 4 –

- 1) Coder le message **Rendez-vous à la cafétéria** à l'aide de la méthode de Vigenère et de la clé **POULE**. Même question pour **Chiffre de Vigenere** et la clé **BACHELIER**.
- 2) Est-il possible de décoder le message **DSJWPHYRSSUHPAJXVQV** codé par un chiffrement de Vigenère sans connaître la clé. Décoder ce message sachant qu'il a été créé à l'aide de la clé **BORDEAUX**.

Exercice 5 – Le cryptogramme suivant a été codé en utilisant le chiffrement de Vigenère et on sait que le message en clair contient le mot **ATTAQUE**. La clé est un mot français ; retrouver la et déchiffrer le message : **BILKOPFFGMLTWOEWJCFDSHKWONKSEOVUSGRLWH**.

Exercice 6 –

- 1) Coder le message **Rendez-vous à la cafétéria** à l'aide d'un chiffrement par permutation, pour la clé $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$.
- 2) Décoder le message **MELSEGESEADESCTPTREY** à l'aide de la clé $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$.