

# CONCOURS ALKINDI

*Épreuve finale – Paris – 18 mai 2022*



Vous avez un message de la part des organisateurs. Ce message a été chiffré par une substitution en conservant les espaces. Le message est composé de lettres de A à Z et d'espaces entre les mots. On a enlevé le reste de la ponctuation. On a associé à chaque lettre (et au caractère "espace") un nombre entre 00 et 26. Chaque occurrence de cette lettre (ou de l'espace) a été remplacée par ce nombre. Par exemple ALICE ET BOB aurait pu être chiffré 15 23 02 11 08 21 08 19 21 00 13 00 si on avait choisi A=15, B=00, C=11, etc. et "espace"=21. Dans ce message, la correspondance entre lettres et nombres a été choisie au hasard et est différente de l'exemple.

15 10 20 13 07 20 13 12 20 00 25 00 08 25 00  
05 10 13 25 08 20 00 21 12 00 23 14 13 23 14  
12 01 18 00 25 08 02 10 13 21 10 00 13 14 12  
18 00 20 18 19 20 01 14 13 18 00 26 12 20 00  
08 20 18 00 20 11 20 01 23 10 23 20 18 00 21  
20 00 23 20 04 04 20 00 25 13 13 20 20 00 07  
14 13 04 00 07 14 12 18 00 19 08 25 10 01 20  
00 15 14 13 13 20 00 23 17 25 13 23 20 00 08  
20 00 23 14 21 20 00 20 18 04 00 15 20 10 07  
18 05 08 04

Pourrez-vous retrouver le code secret caché dans ce message ?

---

Réponse attendue : 8 lettres (ce n'est pas un mot français).

# CONCOURS ALKINDI

Épreuve finale – Paris – 18 mai 2022



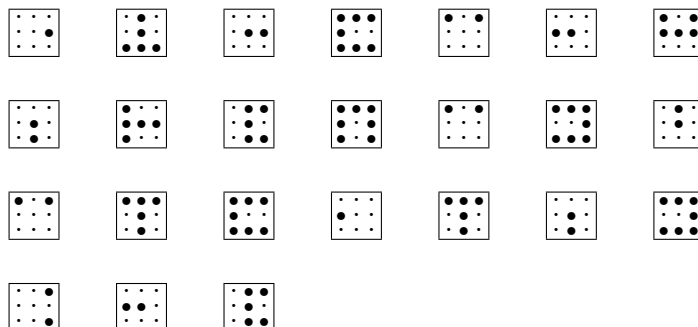
Chaque lettre est chiffrée de la manière suivante :

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				

Alice a trouvé un message chiffré, mais chaque symbole a fait l'objet d'une rotation aléatoire de 0, 90, 180 ou 270 degrés.

**Exemple :** BOB a pu devenir .

Le message contient un code à six chiffres, écrits en toutes lettres (par exemple UNDEUXTROISQUATRECINQSIX). Pouvez-vous le déchiffrer ?



Réponse attendue : 6 chiffres.

# CONCOURS ALKINDI

Épreuve finale – Paris – 18 mai 2022



On reprend le système de chiffrement étudié lors du tour trois.

## Rappel du système de déchiffrement :

On a regroupé les lettres de l'alphabet en trois ensembles appelés cercles. Pour chaque paire de cercles, on a fixé un nombre, appelé le décalage.

Pour déchiffrer un mot, on procède par bigramme (groupe de deux lettres). Pour chaque bigramme, on regarde à quels cercles appartiennent les deux lettres et on note  $d$  le décalage correspondant à cette paire de cercles. On remplace alors chaque lettre du bigramme par la lettre qui est  $d$  positions plus loin sur le cercle.

## Exemple :

Ici **QG** a pour décalage 2, donc on déchiffre **Q** en **C** et **G** en **O**, ce qui donne **CO**. De même, **CK** a pour décalage 1, donc on déchiffre **C** en **N** et **K** en **C**, ce qui donne **NC**. Finalement, **QGCKHSNV** se déchiffre en **CONCOURS** avec cette clé.

	Décalages
Cercle 1 : G H O J D	> 3
Cercle 2 : N E B Z X R Q K C	> 1
Cercle 3 : F A Y S P I L M T U V W	> 4
	$\left. \begin{array}{l} 3 \\ 1 \\ 4 \end{array} \right\} \begin{array}{l} 2 \\ 5 \end{array} \right) 6$

Ici, on ne connaît pas le nombre de lettres dans chacun des trois cercles, ni les décalages. Mais on connaît les messages suivants lorsqu'ils sont chiffrés et en clair (c'est-à-dire déchiffrés) :

chiffré	EVSBRJQ	chiffré	UHHKHREI	chiffré	DTUAKFC
clair	REFDOQVS	clair	RLPALGJM	clair	BNBBCAEA
chiffré	ZXXXPFWA	chiffré	UCVAQGJI	chiffré	UYBKMOKE
clair	IYYYHEIK	clair	RAOKSJDM	clair	STQCWUCD
chiffré	HPXEKXZX	chiffré	SYYSCLHU	chiffré	UWKJFRHE
clair	PLYJCTIY	clair	RTTRKHLR	clair	SZCBUQLD
chiffré	CETBHOYI	chiffré	HDMKPUBJ	chiffré	MUEWLPFH
clair	ADNFLSTM	clair	LFZCHROV	clair	WSJZHLEL
chiffré	OKYBKXKU				
clair	SCTFCTCR				

Déchiffrez le message : PZNNKHDCEDQY.

Réponse attendue : 12 lettres (ce n'est pas un mot français).

# CONCOURS ALKINDI

Épreuve finale – Paris – 18 mai 2022



Alice utilise le système de chiffrement suivant.

D'abord, elle construit une grille 5x5 contenant toutes les lettres de l'alphabet (sauf W). Pour cela, elle commence par choisir une clé de 8 lettres au hasard (toutes différentes). Elle remplit le début de la grille avec ces lettres, puis complète avec le reste de l'alphabet dans l'ordre.

Par exemple, si la clé est LXPOTHDE, la grille sera :

L	X	P	O	T
H	D	E	A	B
C	F	G	I	J
K	M	N	Q	R
S	U	V	Y	Z

Ensuite, Alice prend le message qu'elle veut chiffrer, par exemple BONJOUR. Elle remplace chaque lettre par les deux coordonnées de la lettre dans la grille. B = 25, O = 14, N = 43, etc. Elle obtient 25144335145245.

Puis, elle prend chaque groupe de deux chiffres en commençant par le deuxième de la liste et elle remplace par la lettre correspondante. Ici, 51 = S, 44 = Q, 33 = G, etc. jusqu'à 52 (le dernier et le premier chiffre) qui donne U.

B	O	N	J	O	U	R
2	5	1	4	4	3	3
5	1	4	4	3	3	5
S	Q	G	S	R	A	U

Le message obtenu en chiffrant BONJOUR avec la clé LXPOTHDE est donc SQGSRAU.

Alice a utilisé une clé de huit lettres (différente de l'exemple). Avec sa clé, le message JOYEUXANNIVERSAIREBOB est chiffré en :

QCRNNGPUXKDHJQRJILGMI.

Alice vous indique que dans sa grille, le U est dans le coin en bas à gauche, c'est-à-dire que U = 51.

Quelle est la clé utilisée par Alice ?

Réponse attendue : 8 lettres (ce n'est pas un mot français).

Le chiffrement de Vigenère fonctionne de la façon suivante.

La clé est composée d'une liste de nombres, tous compris entre 0 et 25. Il peut y avoir plusieurs fois le même nombre.

Pour chiffrer un texte, on applique à la première lettre un décalage dans l'alphabet correspondant au premier nombre de la clé. Puis on applique à la deuxième lettre un décalage correspondant au deuxième nombre de la clé. Et ainsi de suite. Lorsqu'on a dépassé la longueur de la clé, on recommence avec un décalage égal au premier nombre de la clé.

**Exemple :** On veut chiffrer le message BONJOUR avec la clé [2,12,5]. D'abord la lettre B est décalée dans l'alphabet de 2 positions, ce qui donne D. Ensuite la lettre O est décalée de 12 positions, ce qui donne A. Puis la lettre N est décalée de 5 positions ce qui donne S. Pour la lettre J, comme la clé est ici de longueur 3, on ne peut pas utiliser la valeur suivante de la clé, donc on boucle et on utilise à nouveau la première valeur de la clé. Le J est décalé de 2 positions, ce qui donne L. Et on continue ainsi. On obtient le message DASLAZT.

Lorsqu'on chiffre un message avec des espaces et signes de ponctuation, seules les lettres sont chiffrées. Les espaces et signes de ponctuation ne comptent pas dans les positions de la clé. Par exemple, si on chiffre J'AIME LA CRYPTO ! avec la clé [2,12,5] on obtient L'MNOQ QC OWABYQ !.

Ce texte a été chiffré avec un chiffrement de Vigenère avec une clé de longueur 10.

KL D'QKUWVC IBUC OB BWHPWJLB YLM KBBJ. KL  
CGFR AHP VVL DG XQZVTJSHC M ID ZRAZQLBQO.  
KM PMIF LCF JXITHZ. K'LCBBQM DSJ UB XQ  
QQIUGWBZ ZMP LI PMSGPKZZD.

Déchiffrez le texte et retrouvez le code caché.

---

Réponse attendue : 6 lettres (ce n'est pas un mot français).

Vous avez intercepté une lettre que Alice a envoyée à Bob. Voici le contenu de la lettre.

SALUT BOB,

J'ESPERE QUE TU PASSES UN BON MOIS DE JUJLLET. CE DXMANCHE JE VAIS FETER  
MON ANXIVERSAIRE. JE VAIS ORGANISER UN GOUTER DANS LE JARDIX AVEC TOUS  
MES AMIX ON POURRA MEME SE BAIXNER DANS LA PISCINE S'IL FAIT BEAX.  
J'ESPERE QUE TU POUXRAS ETRE LA ! ENVOIE MOI TA REXONSE RAPIDEMENT.

AMITIES,

ALICE

PS : AU MOIS D'AOUT JE VAIS PARTIR EN VOYAGE EN EUROPE : JE VAIS VISITER  
LA BELGXQUE, LES PXYS-BAS, L'ALLEXAGNE, LE DANEMARX, LA SUEXE ET LA  
NORVEGX! J'AI HATE !

Un message secret est caché dans la lettre. Le message commence par LE CODE ...  
Pourrez-vous trouver le code secret ?

---

Réponse attendue : 6 lettres (ce n'est pas un mot français).

Alice a un nouveau système de chiffrement qui permet de chiffrer les mots de 5 lettres. La clé est une liste de 5 nombres. Pour chiffrer, Alice procède de la manière suivante :

1. Elle convertit les lettres en nombres ( $A=0, B=1, \dots, Z=25$ ). Elle obtient une liste de cinq nombres.
2. Pour chaque nombre de la liste elle ajoute la valeur de la clé correspondante (le premier nombre avec la première valeur de la clé, etc.). Si un résultat est  $\geq 26$ , elle soustrait 26.
3. Elle déplace le premier élément de la liste pour le mettre à la fin.
4. Pour chaque nombre de la liste elle ajoute la valeur de la clé correspondante (le premier nombre avec la première valeur de la clé, etc.). Si un résultat est  $\geq 26$ , elle soustrait 26.
5. Elle déplace le premier élément de la liste pour le mettre à la fin.
6. Pour chaque nombre de la liste elle ajoute la valeur de la clé correspondante (le premier nombre avec la première valeur de la clé, etc.). Si un résultat est  $\geq 26$ , elle soustrait 26.
7. Elle convertit les nombres en lettres ( $A=0, B=1, \dots, Z=25$ ).

**Exemple :** pour chiffrer le mot ALICE avec la clé  $[1, 2, 3, 4, 5]$ , voici les étapes :

0. ALICE
1.  $[0, 11, 8, 2, 4]$
2.  $[1, 13, 11, 6, 9]$
3.  $[13, 11, 6, 9, 1]$
4.  $[14, 13, 9, 13, 6]$
5.  $[13, 9, 13, 6, 14]$
6.  $[14, 11, 16, 10, 19]$
7. OLQKT

Dans cet exemple, le mot ALICE devient OLQKT.

Alice a choisi une nouvelle clé au hasard, différente de celle de l'exemple. Avec cette clé, le mot ALICE est chiffré en UQWQA. Pouvez-vous déchiffrer le message ITNCM qui a été chiffré avec la même clé ?

---

Réponse attendue : 5 lettres (ce n'est pas un mot français).

Alice utilise à nouveau le système de chiffrement de l'exercice 4. Vous avez informé Alice que générer la grille à partir d'une clé de 8 lettres n'était pas une bonne idée car il était possible de retrouver facilement la clé. Alice a donc décidé de générer sa grille de manière totalement aléatoire, indépendamment de l'ordre alphabétique (ce qui revient à prendre une clé de taille 25).

Par exemple, Alice peut choisir la grille

P	E	I	F	Z
R	Y	D	J	U
G	N	H	L	S
M	B	X	C	T
O	Q	K	A	V

Alors, le mot **BONJOUR** est chiffré en **UIYTEQF**.

Alice a utilisé une nouvelle grille (différente de l'exemple). Avec sa clé, le message **RENDEZVOUSCESOIRAUPARC** est chiffré en :

**XKAVSFHBEZUKOBGAXIYGGQ.**

Pouvez-vous déchiffrer le message **EVYCURQH** ?

---

Réponse attendue : 8 lettres (ce n'est pas un mot français).