Jeu d'initiation à la cryptologie : Sauvez Jean Jaurès

Ce jeu d'énigmes vous est proposé par CyberINSA. L'objet de CyberINSA est de développer la recherche, la formation et la sensibilisation autour de la cybersécurité en région Centre-Val de Loire.

Les supports conçus par l'équipe de CyberINSA sont distribués gratuitement pour une utilisation pédagogique non-commerciale. Nous vous remercions de bien vouloir indiquer la provenance de ces supports lors de vos utilisations.

Dans le but de suivre l'évolution du projet et de mesurer son impact, nous vous remercions de bien vouloir nous faire remonter les indicateurs du nombre d'élèves et/ou de participants touchés par ce jeu d'énigmes à amandine.lefebvre@insa-cvl.fr.

Ce projet bénéficie d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre de France 2030.

ANR-23-CMAS-0019

Paris, le 20 mai 1914

Cher ami,

J'ai eu vent de rumeurs me concernant. Ma vie est en danger ! Pouvez-vous mener l'enquête ?

L'un de mes informateurs me communique régulièrement des messages concernant cette affaire, mais ceux-ci sont chiffrés.

Fort heureusement, je sais que la cryptographie est l'une de vos passions. Je vous transmettrai chaque message intercepté. Je compte sur vous pour essayer de déjouer ce complot.

Amicalement,

Jean Jaurès

Paris, le 21 mai 1914

Cher ami,

Voici le premier message intercepté par mes informateurs

Il me semble que nos ennemis n'ont pas choisi la méthode de chiffrement la plus robuste. Si vous réussissez à identifier la lettre qui remplace le « e » vous devriez casser ce message sans aucun problème.

Amicalement,

Jean Jaurès

Paris, le 21 mai 1914

Rtsxnjzw,

Stzx ijatsx jqnrnsjw Ojfs Ofzwjx.
Rfnx hjy mtrrj jxy ywjx rfqns,
rjx rjxxfljx xjwtsy hmnkkwjx.

Anaj qf Kwfshj!

Paris, le 22 mai 1914

Cher ami,

Merci pour votre aide dans le déchiffrement du code César. Voici un nouveau message.

Si mes lointains souvenirs sont encore vivaces, il s'agit d'un carré de Polybe. Je suis certain que cela ne vous posera aucune difficulté.

Amicalement,
Jean Jaurès

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

Paris, le 22 mai 1914

33 35 34 44 24 15 51 43

25 11 51 43 15 44 44 15 33
15 21 24 15 14 15 34 35 51
44 21 11 24 44 35 34 44 52
24 45 15

52 24 52 15 32 11 21 43 11
34 13 15

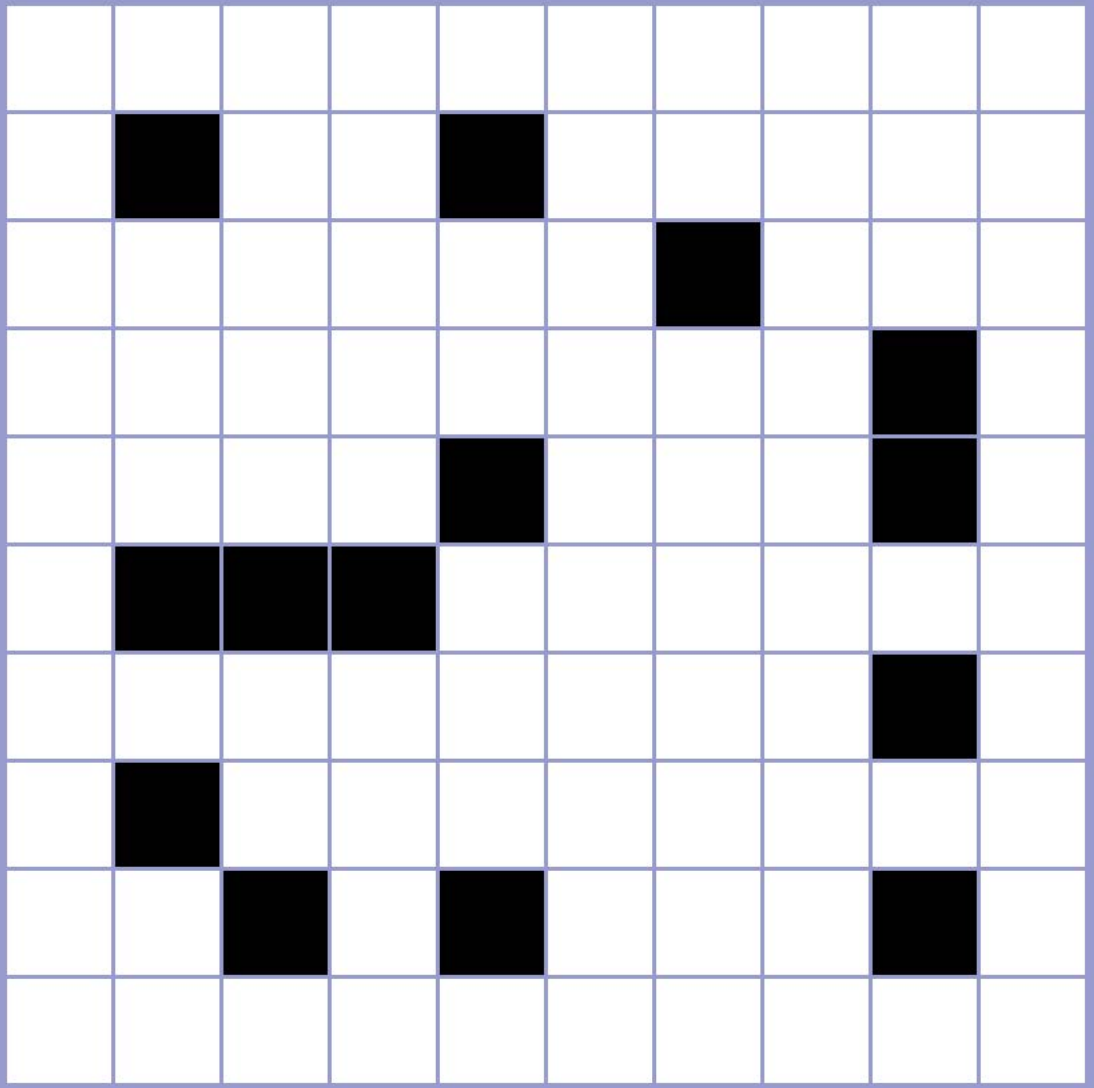
Paris, le 23 mai 1914

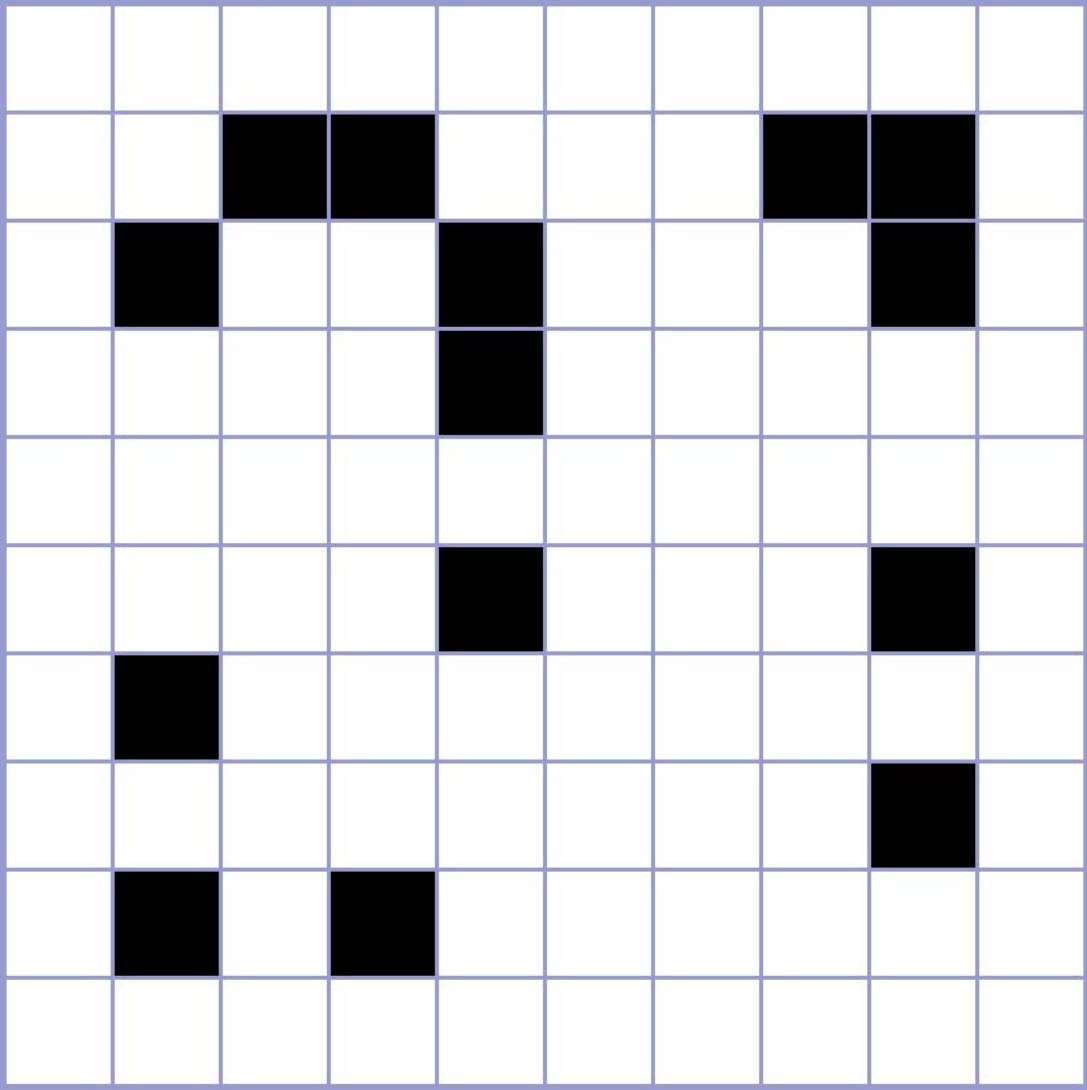
Cher ami,

Je m'inquiète, ma vie semble en grand danger. Voici un nouveau message. J'espère que vous réussirez à le déchiffrer. Le temps presse !

Amicalement,

Jean Jaurès





Paris, le 24 mai 1914

Cher ami,

Les informations que vous avez brillamment déchiffrées m'inquiètent de plus en plus ! Il semble que vous ayez trouvé l'heure de l'attaque !

Nos opposants gagnent du terrain. Voici un nouveau message. Si je ne m'abuse, nous sommes face à une substitution de caractères !

Faites vite !

Amicalement,

Jean Jaurès

Paris, le 23 mai 1914

K F A S Y N D U

V Z D U N S S N M U F D O N U
Z Z K F A M K Z U M U N , Z D
R Z X N B D R U F Y S S Z A M
. G N W U F R L Z Y A K N S S
Z J N S N U Z R L Y X X U N S
N G F A D A N R N U M Z Y A N
W N U K D M Z M Y F A .

O Y O N G Z X U Z A R N

Paris, le 25 mai 1914

Cher ami,

Je suis impressionné par vos talents. Malheureusement l'heure n'est pas aux réjouissances. Voici un nouveau mystère à éclaircir!

Amicalement,

Jean Jaurès

Paris, le 25 mai 1914

Monsieur,

uoNsa novsu lanli otéut ortuv opéur tecte câthe aR.ou iVlll niaou irvra feleu rusJa èrus.

Vive la France!

Paris, le 26 mai 1914

Cher ami,

Nos informateurs m'ont transmis ceci... Avez-vous une idée de ce que cela siginifie?

Amicalement,

Jean Jaurès

A G S L » A !	O O S I A F E N	P M U I R	L I E E E	P R E T L « V A	U C S L E C	E N Z F V F	R H A I C U L E

Paris, le 27 mai 1914

Cher ami,

Nous avons le lieu, l'heure et même le nom de celui qui souhaite attenter à ma vie.

Mes hommes ont pu intercepter un autre message. Saurez-vous en tirer quelque chose? La clef que vous venez de trouver vous sera sans doute fort utile !

Amicalement,

Jean Jaurès

Paris, le 27 mai 1914

Rshxmyzv,

Htym fkcwshx py yvysxy jx os nonpfjx.

Pnzy qe Zwehhi.

Paris, le 28 mai 1914

Cher ami,

Grâce à votre aide précieuse, me voici sain et sauf. Je serai éternellement reconnaissant.

Mais la route est encore longue, le monde sombre petit à petit dans le chaos, et nous devons essayer d'empêcher l'assemblée de voter l'entrée en guerre.

Retrouvons-nous dans l'hémicycle.

Amicalement,

Jean Jaurès

Solutions

1 - Code césar : décalage de 5

Monsieur ,

Nous devons éliminer Jean Jaurès. Mais cet homme est très malin, mes messages seront chiffrés.

Vive la France !

2- Carré de Polybe

Monsieur,

Jaurès se méfie de nous, faisons vite.

Vive la France

3- Pixels

La superposition des pixels donne le chiffre 21 (correspondant à l'heure).

4- Substitution

Les informations en clair (toutes les lettres commencent par MONSIEUR et terminent par VIVE LA FRANCE) dans les précédentes lettres permettent d'obtenir la substitution suivante :

Monsieur

Jaurès se trouvera à Montmartre, au Café du Croissant. Le prochain message sera chiffré selon une certaine permutation.

Vive la France

5- Permutation

Selon la séquence 3 2 1 4 5. Les signes de ponctuations font partie de la permutation. :

Nous avons un allié tout trouvé pour cette tâche. Raoul Villain ouvrira le feu sur Jaurès.

Vive la France

6- Bandelettes

A remettre dans l’ordre pour obtenir

P M U I R	P R E T L « V A	O O S I A F E N	U C S L E C	R H A I C U L E	 A G S L » A !	L I E E E	E N Z F V F

7- Vigenère

Avec la clef « FEU »

Monsieur,

Nous agirons le trente et un juillet.

Vive la France