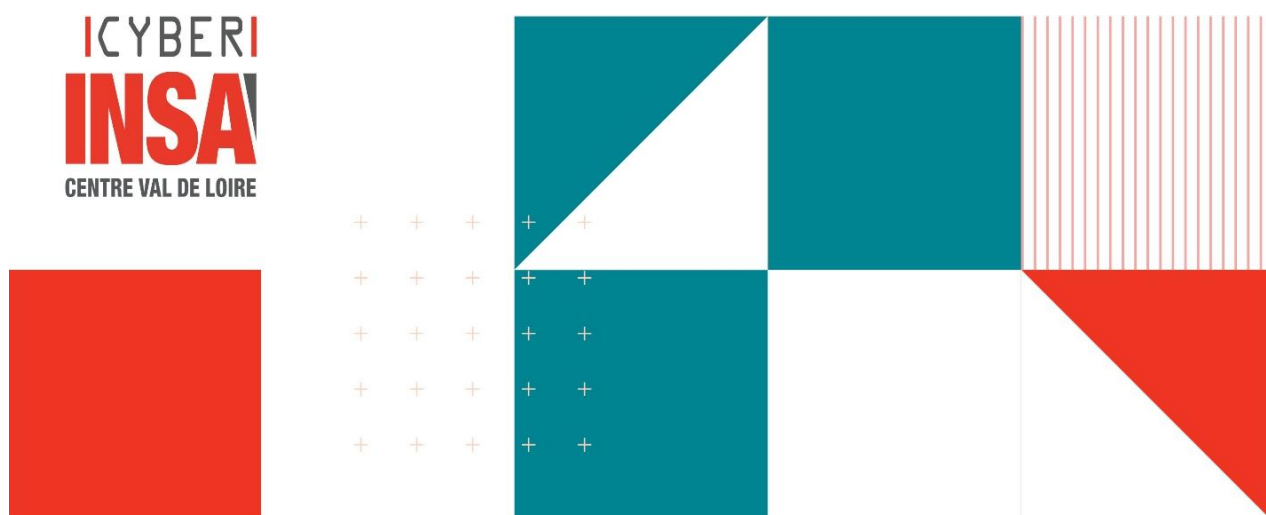




Jeu d'initiation à la cryptologie : La machine Enigma

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

Avant-propos :

Ce jeu d'énigmes nécessite l'utilisation d'une maquette de machine Enigma conçue pour s'adapter à une boîte de pringles.

Les différentes parties à imprimer sont disponibles ici : <https://franklinheath.co.uk/wp-content/uploads/2012/05/pringlesenigma3a4.pdf>

Attention, veuillez à imprimer ces plans à l'échelle 100% pour qu'ils s'adaptent parfaitement à la boîte.



Londres le 20 mai 1940

Chère Mrs Clarke,

Je vous remercie pour votre proposition d'aide concernant le déchiffrement des messages allemands.

L'heure est grave, les nazis progressent de jour en jour et nous devons impérativement les arrêter.

Pour cela, toute aide est la bienvenue. Je pense que vos compétences seront très utiles à nos travaux.

Afin de m'assurer qu'aucun œil malicieux ne viendra espionner nos échanges, je chiffrerai mes prochaines lettres dans le but de vous communiquer les informations les plus importantes. Et pour commencer, pensons comme les romains.

Bien à vous,

A. Turing



Londres le 23 mai 1940

Inkxk Sxy Irgxqk,

Rky ykxboiky ykixkzy tuay utz iutloxsk r'azoroygzout
j'atk kzxgtmk zkinturumok vgx rky grrksgtjy, rkax
vkxskzzgtz at inollxksktz zxky xuhayzk. Pk bgoy
kyygekx j'kt ygbuox vray.

Sg vxuingotk rkzzxk azoroykxg atk yahyzozazout.

Hokt g buay,

G. Zaxotm



Londres le 25 mai 1940

H I T W T J W L H B V W D T ,

H T E E T J V H I F X T L T X C J J T T X F U J V
. T B B T L T J N B T A C X H E F C X X T W L T B
C X O X G W F X H F G T R T W C E C W L V B F J
T X E T L G V W O X T G F B T T B T H E W F M O T

N F T X V Y C O L ,

V . E O W F X U



Londres le 28 mai 1940

Chère Mrs Clarke,

N'hésitez pas à agir directement sur ce morceau de papier.

Bien à vous,

A. Turing

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



Londres le 2 juin 1940

Chère Mrs Clarke,

Voici d'autres informations concernant le fonctionnement de la machine.

Cu qrw1zhi wirtnmfhrv wsdgi cyw klszm
ezayzfpvm h' lhi dirkli.

Civjkyv fi glidcii lskiv r zezn ye
nsll gfgtcyx, cy wvwsex emurty h'lh
giur. Civjkyv fi jygfhh r zezn ye
nsll gfgtcyx, cy xiimjcidy emurty
h'lh giur.

Bien à vous,

A. Turing



Londres le 6 juin 1940

Chère Mrs Clarke,

Empruntons le code de la plus célèbre des sociétés secrètes.

7E<F C J F F O
C C O L > F C O O O F L J
J L N F O O , < > F L F V O A
L J L L O C U E U .

Bien à vous,

A. Turing



Londres le 6 juin 1940

Chère Mrs Clarke,

Vous avez la clef mais il vous reste à connaître la configuration des rotors de la machine.

Il y a un réflecteur indiqué par une lettre, et trois rotors numérotés .

Si vous savez jouer au mastermind, vous ne devriez pas rencontrer de problèmes.

Proposition	Bien placés	Mal placés
D 3 4 2	0	2
C 1 2 5	2	0
B 2 4 1	1	2
B 1 2 4	3	0
B 5 2 3	3	0
D 4 5 7	0	0

Bien à vous,

A. Turing



Londres le 9 juin 1940

Chère Mrs Clarke,

Vous disposez de toutes les informations nécessaires pour déchiffrer ce message grâce à la machine.

N'oubliez pas de bien configurer les rotors dans le bon ordre et d'effectuer une rotation du dernier rotor après chaque lettre déchiffrée.

Je m'explique, vous déchiffrerez la première lettre en utilisant la clef BOB. La seconde lettre sera déchiffrée en utilisant la clef BOC, etc.

Voici le message: IFIIC

Bien à vous,

A. Turing

La machine Enigma

Solutions

Lettre 1 : Pas d'énigme

Lettre 2 : César, décalage de 6

Chère Mrs Clarke,

Les services secrets nous ont confirmé l'utilisation d'une étrange technologie par les allemands, leur permettant un chiffrement très robuste. Je vais essayer d'en savoir plus.
Bien à vous,

A. Turing

Lettre 3 : Substitution selon l'alphabet suivant (retrouvable grâce aux informations glanées en clair connu dans les lettres précédentes).

1	A	V	12	L	B
2	B	N	13	M	J
3	C	H	14	N	X
4	D	R	15	O	C
5	E	T	16	P	G
6	F	A	17	Q	M
7	G	U	18	R	W
8	H	I	19	S	L
9	I	F	20	T	E
10	J	S	21	U	O
11	K	D	22	V	Y
12	L	B	23	W	P
24	X	Z			
25	Y	Q			
26	Z	K			

Chère Mrs Clarke,

Cette machine se nomme enigma. Elle semble fonctionner selon un principe de rotors alimentés par une pile électrique.

Bien à vous,

A. Turing

Lettre 4 : Il faut imaginer un principe de bandelettes à remettre dans l'ordre.

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

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

Lettre 5 : Vigenere :

Avec la clef « RUE »

La machine fonctionne comme les trois aiguilles d'une montre. Lorsque le premier rotor a fait un tour complet, le second avance d'un cran. Lorsque le second a fait un tour complet, la troisième avance d'un cran.

Lettre 6 : Pig Pen (code des francs-maçons)

Pour faire fonctionner la machine, utilisez la clef « BOB »

Lettre 7 : Déchiffrement de la machine Enigma avec la clef « BOB »

BRAVO