RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Collège Jean Moulin
La norville

Ministère de l'Education nationale

Académie de Versailles

BILAN PROJET

doc 17

INTITULE du projet : CRYPTOGRAPHIE en 3e

Enseignant Organisateur du projet : Mme DE SOUSA CHULER

Enseignants impliqués : Mme MARTINS et Mme WULLEMAN (en français), M. DAUMET et Mme LEROY(en Histoire Géographie), Mme HEREDIA (en espagnol), Mme THORIN (en SVT)

Le projet a-t-il été réalisé ? : OUI
Nombre d'élèves participants : 60 élèves

Date de réalisation du projet : 2021-2023
Coût total : 0 euros

BILAN ET PERSPECTIVES

Ecueils (freins éventuels et condition de réussite du projet):

- Le manque de temps pour approfondir certaines notions mathématiques autour de la cryptographie
- Omission des différents codages vus en classe au mémo de l'oral de DNB pour éviter des questions pointues et développées des membres du jury.
- Organisation et dates communes avec le Collège Camus.
- Difficultés pour certains élèves d'échanger avec leur camarade du Collège Camus, prévoir une activité pour une meilleure cohésion.
- Beaucoup d'investissement des collègues pour aucune compensation financière, aucune heure HSE.

Points d'appui/ points forts :

- Ce projet inter-établissement a permis de tisser des liens entre les élèves et les enseignants des deux collèges de LA NORVILLE.
- Les élèves ont découvert la cryptographie et apprécié obtenir des points de Bonus lors des exercices demandés. Ils se sont rendu compte que cela ne concernait pas que les Mathématiques.
- Les élèves ont pu réfléchir, de façon ludique, aux fondements mathématiques, informatiques et logiques de la cryptanalyse et de les sensibiliser à la question importante de la sécurité de l'information. Pour certains élèves, cette notion a été compliqué.
- Améliorer l'expression écrite et orale en Français et en Espagnol.
- Les élèves ont regardé et travaillé sur le film The Imitation Game.
- Les élèves ont travaillé sur la pièce de théâtre « La machine de Turing » de Benoit Solés.
- Les élèves ont une meilleure connaissance du conteste historique et la vie d'Alan TURING.
- Les élèves ont été enthousiastes par ce projet.
- Reconnaissance et remerciement de parents notamment lors du conseil de classe.
- Présentation du projet à l'oral de DNB par certains élèves.
- Retour de collègues jury après l'Oral de DNB sur les points positifs et à améliorer.

Améliorations :

- Revoir la progression de 3e : déplacer le chapitre « Arithmétiques » avant les vacances de Toussaint et non en fin d'année.
- Retravailler le parcours réalisé pendant la formation ELEA.
- Faire appel à un chercheur (ou autre) qui aborderait la notion de la cryptographie.
- Intégrer plus de questions de Mathématiques dans le mémo Oral de DNB.
- Donner le mémo avant l'épreuve (ou pas ?)

Perspectives Reconduire le projet

Objectifs fixés pour ce projet	**atteint**	**non atteint**
Participation des élèves aux deux tours du concours « ALKINDI »	x	
Visualisation du film « The Imitation Game » au cinéma d'ARPAJON	x	
Les élèves impliqués et intéressés par le projet	x	
Exploitation d'une erreur du film pour le calcul sur les puissances		x
Les élèves soient capables de faire le lien entre les nombres premiers et la cryptographie		x

Date : 11 Juin 2023 Nom et signature du professeur référent : Mme De Sousa Chuler

CRYPTOGRAPHIE
En 2022-2023

La Norville
Collège Albert Camus
Collège Jean Moulin

I – PRINCIPE

Quatre classes de 3ème, deux de chaque établissement, sont inscrites au concours « Alkindi – Découvrez la cryptographie », celles de Mme DE SOUSA CHULER et Mme VIOLETTE.
Pour les deux premiers tours, les élèves sont réunis en salle informatique dans deux salles et disposent de 45 minutes pour résoudre 8 défis en binôme, à horaire décalé. Chaque binôme est composé d'un élève de 3ème de chaque établissement. Un classement est établi à l'issue de chaque tour et des diplômes peuvent être imprimés. Aucun prérequis en cryptanalyse n'est nécessaire.

II – DATES

Le concours se prépare tout au long de l'année :

1. Septembre/Octobre 2022: Les élèves s'entrainent à la maison
2. Le 18 Novembre 2021 : Une séance d'entrainement est organisée en salle informatique.
3. Le vendredi 9 décembre 2022 : 1er tour au collège Jean.Moulin
4. Du mardi 7 février 2023 : 2ème tour au collège Albert.Camus avec gouter.

III – OBJECTIFS

Ce concours a pour objectif de faire découvrir aux élèves la cryptographie, application très concrète des mathématiques, qui joue un rôle fondamental dans leur vie quotidienne. Il a pour but de les faire réfléchir, de façon ludique, aux fondements mathématiques, informatiques et logiques de la cryptanalyse et de les sensibiliser à la question importante de la sécurité de l'information.

Ce projet est également porté par des enseignants en Anglais, de Français, d'Espagnol, d'Anglais, Histoire Géographie et de SVT. Il va permettre la liaison entre les collèges mais aussi la collaboration entre collègues.

IV- PLANNING

- Une réunion d'équipe est prévue le Jeudi 17 novembre 2022 en salle de réunion.
- Le Mardi 21 Mars 2023, une sortie pédagogique est prévue pour les quatre classes au cinéma d'Arpajon autour de film The Imitation Game.

Français – Mme MARTINS et Mme WULLEMAN	Dates
Travail d'écriture	
Histoire des Arts , « La machine de Turing » de Benoit Solés	
Espagnol – Mme HEREDIA	
Vidéo de présentation.	Décembre 2022
Travail sur le langage Inca, les mayas	Juin 2023
Histoire- M. DAUMET (les élèves de 3e3)	
Connaitre le contexte historique : la Seconde Guerre mondiale (causes, grandes étapes de la guerre, événements majeurs) et intégration des éléments sur Alan Turing et la cryptographie dans le cours sur le tournant de la guerre et les débarquements alliés.	Fin Janvier -début Février
Mettre en lumière l'évolution de la société française entre les années 1950 et 80.	Avril -Mai
Histoire Mme LEROY (les élèves 3e6, 3e1 et 3e2)	
Connaitre le contexte historique : la Seconde Guerre mondiale (causes, grandes étapes de la guerre, événements majeurs) et intégration des éléments de la cryptographie dans le cours	
L'homophobie	
Mathématiques- Mme DE SOUSA CHULER	
- Donner la définition de la cryptographie. A quoi sert-elle ? - Recueillir des informations sur Alan Turing et Elizebeth Smith Friedman. - Présenter et organiser ces informations de manière synthétique en utilisant un diaporama.	Le Lundi 14 novembre
S'entrainer aux épreuves des années précédentes du **concours Alkindi** : https://epreuve.concours-alkindi.fr/	Le vendredi 18 novembre
1er tour au collège Jean.Moulin	Le vendredi 9 Décembre
Découvrir différents types de messages secrets, et leur fiabilité : le chiffrement de César, le chiffrement presque allemand et le codage affine, issues du livre « 25 énigmes ludiques pour s'initier à la cryptographie » et extrait d'un document du Lycée Bertran de Born, Périgueux.	Le vendredi 6 Janvier + codage affine en mai
Découvrir le codage de la carte Vitale pendant la semaine des Mathématiques, une activité réalisée par **Mme AZIZA**, professeur de Mathématiques	Le lundi 6 au mercredi 15 mars 2023
Codage avec le logiciel « Scratch »	En Janvier 2023
2ème tour au collège Albert.Camus	Du mardi 1er février au lundi 28 février 2023
Exploitation d'une erreur du film pour le calcul sur les puissances	Non réalisé
SVT- Mme THORIN	
Le code génétique : lecture de la molécule d'ADN pour « fabriquer » des protéines	

CRYPTOGRAPHIE
Le chiffrement de César

Séance 2
GROUPE 1

Objectifs	1) Découvrir différents types de messages secrets, et leur fiabilité 2) Mener collectivement une investigation en sachant prendre en compte le point de vue d'autrui. 3) Extraire d'un document les informations utiles, les reformuler, les organiser, les confronter à ses connaissances. 4) Expliquer à l'oral ou à l'écrit (sa démarche, son raisonnement, un calcul, un protocole de construction géométrique, un algorithme), comprendre les explications d'un autre et argumenter dans l'échange. 5) Réaliser un panneau / une affiche

Exercice : Parcours orange

1) Une énigme à résoudre (*Un extrait du livre « 25 énigmes ludiques pour s'initier à la cryptographie »)* :

Dans la cave d'un bâtiment de l'U.S. Navy, des brouillons de lettres, certaines chiffrées et d'autres en clair, ont été retrouvés dans un vieux carton d'archives de la Seconde Guerre mondiale. A l'aide de la lettre de la figure 1, saurez vous décrypter celle de la figure 2 ?

Le 26 avril 1942 à Washington D.C.,

A qui de droit,

J'ai fait des découvertes importantes sur la cryptanalyse de la machine ENIGMA. J'ai utilisé mes connaissances en cryptographie antique pour protéger mes travaux des curieux, mais je n'ai aucun doute qu'un expert en cryptographie saura y accéder.

Elizebeth Smith Frieman.

Figure 1 - Un brouillon en clair retrouvé dans la cave.

Oh 28 dyulo 1945 d Zdvklqjwrq G.F.,

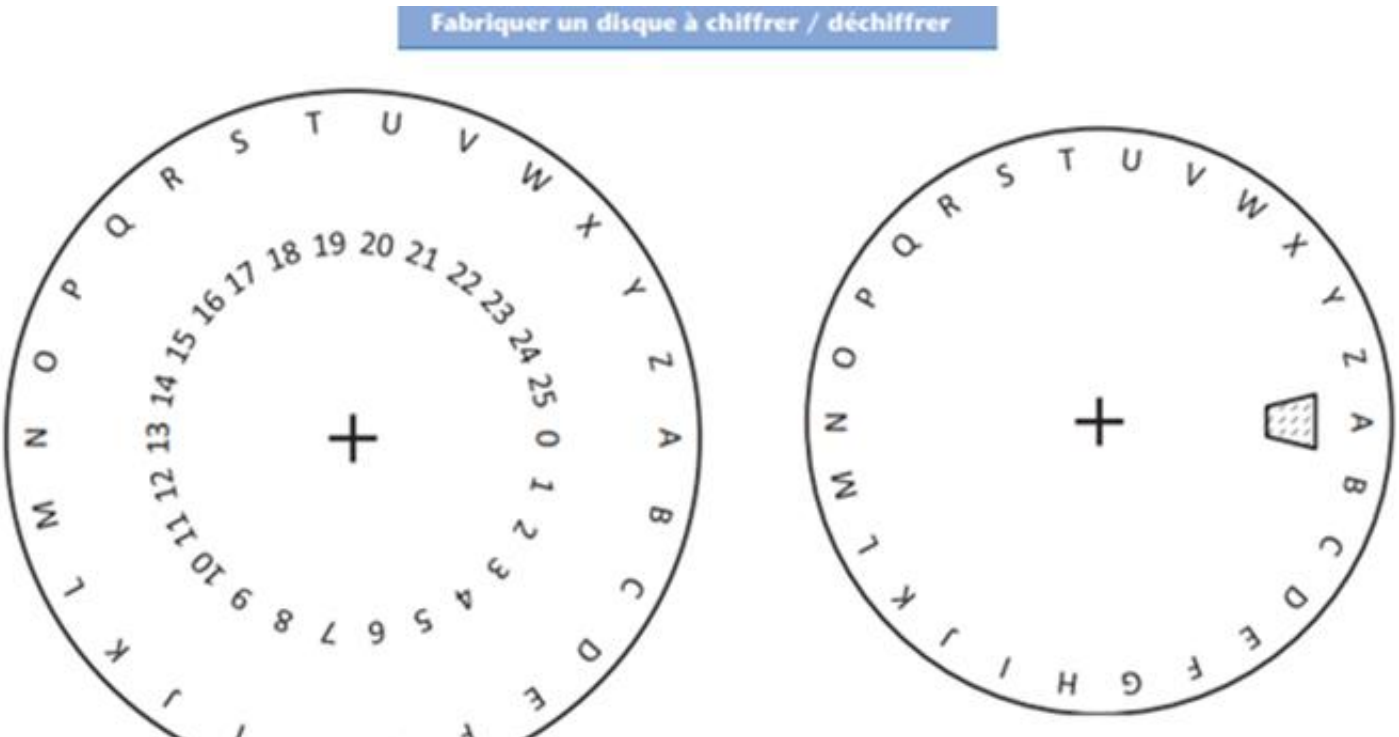
D txl gh gurlw,

Pd ghfrxyhuwh sruwh vxu od vwuxfwxuh gh od pdfklqh HQLJPD. Hooh shuphw gh idluh ghv vxffhvvlrqv gh vxevwlwxwlrqv hw gh shupxwdwlrqv. M'dl dxvvl o'lpsuhvvlrq txh od vwuxfwxuh ghv phvvdjhv hfkdqjhv hvw vrxyhqw od phph, fh txh qrxv doorqv hvvdhu g'hasorlwhu.

Holchehwk Vplwk lulhgpdq.

Figure 2 - Un brouillon chiffré retrouvé dans la cave.

2) Réaliser un panneau / une affiche pour expliquer le chiffrement de César (qui l'a inventé, quand, en quoi ça consiste, quelques exemples ...) Vous pouvez également réaliser des objets permettant d'animer cette technique.
Par exemple,



CRYPTOGRAPHIE
Un chiffrement presque allemand

Séance 2
GROUPE 2

Objectifs

1) Découvrir différents types de messages secrets, et leur fiabilité
2) Mener collectivement une investigation en sachant prendre en compte le point de vue d'autrui.
3) Extraire d'un document les informations utiles, les reformuler, les organiser, les confronter à ses connaissances.
4) Expliquer à l'oral ou à l'écrit (sa démarche, son raisonnement, un calcul, un protocole de construction géométrique, un algorithme), comprendre les explications d'un autre et argumenter dans l'échange.
5) Réaliser un panneau / une affiche

Exercice : Parcours Jaune

1) Une énigme à résoudre *(un extrait du livre « 25 énigmes ludiques pour s'initier à la cryptographie »)* :

Dans la cave d'un bâtiment de l'U.S. Navy, des brouillons de lettres, certaines chiffrées et d'autres en clair, ont été retrouvés dans un vieux carton d'archives de la Seconde Guerre mondiale.
A l'aide de la lettre de la figure 1, saurez-vous décrypter celle de la figure 2 ?

Le 27 avril 1942 à Bletchley Parc,

A qui de droit,

Nous avons obtenu une machine ENIGMA et sommes en bonne voie pour en percer les secrets.

Alan Turing.

Figure 1 - Un brouillon en clair retrouvé dans la cave.

DX AV VX VF AA GG FX DF DX VG XX XA VV AA AD DX AV GD AF DD DX
AV VA FG AA FX DV ,

AA FV GF DF AG AV AG FX FF DF GD,
FA AV FX AF DF FG FF GF FX AF AV GA FD FF GF GG AV DX DX AV GA,
FD FF GF GA AA GG FF FD GA FX AV GF GA GA DF AA AG AV AF DD DF
AX AX FX AV FX FV GF AV DX FV GF AV GA FA AV GA GA AA DA AV GA
AV FD GG FF VA AV GA FG AA FX DX AV GA AA DX DX AV FA AA FD AG
GA.

AA DX AA FD GD GF FX DF FD DA.

FG FF GA GD – GA AF FX DF FG GD GF FA : AD GF GG AV VD AG AV AF
AV GV DD DF GA DV VA FV GF AV DX AV FG AA GD FX FF FD DG GF DA
AV AX AA FA AV GF GX.

Figure 2 - Un brouillon chiffré retrouvé dans la cave.

2) Réaliser un panneau / une affiche pour expliquer ce chiffrement (qui l'a inventé, quand, en quoi ça consiste, quelques exemples ...) Vous pouvez également réaliser des objets permettant d'animer cette technique.

Par exemple,

	A	D	F	G	V	X
A	a					
D						
F						
G						
V						
X						

CRYPTOGRAPHIE
Le codage affine

Séance 2
GROUPE 3

Objectifs

1) Découvrir différents types de messages secrets, et leur fiabilité
2) Mener collectivement une investigation en sachant prendre en compte le point de vue d'autrui.
3) Extraire d'un document les informations utiles, les reformuler, les organiser, les confronter à ses connaissances.
4) Expliquer à l'oral ou à l'écrit (sa démarche, son raisonnement, un calcul, un protocole de construction géométrique, un algorithme), comprendre les explications d'un autre et argumenter dans l'échange.

Exercice : Parcours Vert

Extrait d'un document du Lycée Bertran de Born – Périgueux

Principe

A chaque lettre est associée un nombre entier n selon son rang dans l'alphabet de 0 pour la lettre A à 25 pour la lettre Z.

Deux nombres a et b sont choisis comme clés.

Méthode :

- Au nombre n de départ, on associe le nombre $m = an + b$.
- Ce nombre m n'étant pas toujours compris entre 0 et 25, il ne permet pas de chiffrer une lettre.
- Pour résoudre ce problème, le codage se fait en associant au nombre de départ n le nombre entier p, reste de la division euclidienne de m par 26.
- Puis, on retranscrit p en lettres.

Par exemple, si on prend $a = 4$ et $b = 1$.

La lettre Z est remplacée par $n = 25$.

Puis $m = 4 \times 25 + 1 = 101$.

Or 101 n'est pas compris entre 0 et 25, on effectue donc la division euclidienne de 101 par 26 ce qui donne :

$101 = 3 \times 26 + 23$.

Donc $p = 23$ qui correspond à la lettre X. Z est donc codée par X.

Questions

On prend $a = 3$ et $b = 7$, compléter les tableaux suivants :

Lettre décodée	A	B	C	D	E	F	G	H	I
n									
m									
p									
Lettre décodée									

Lettre décodée	J	K	L	M	N	O	P	Q	R
n									
m									
p									
Lettre décodée									

Lettre décodée	S	T	U	V	W	X	Y	Z
n								
m								
p								
Lettre décodée								

1. Coder une phrase de votre choix avec la clé $(3; 7)$.
2. Décrypter la phrase RXF HPJJF avec la clé $(3; 7)$ ainsi que celle de votre voisin.
3. On prend maintenant pour clé le couple $(2; 13)$. Coder alors le mot ENTIER. Quel problème apparaît dans ce codage ?

MEMO DNB CRYPTOGRAPHIE

3e6 et 3e1-2-3 de Mme De Sousa Chuler En 2022-2023

« Comment les mathématiques ont contribué à la victoire des alliés pendant la seconde guerre mondiale ? »

I- Biographie courte d'Alan Turing

Né le 23 juin 1912 à Paddington, en Angleterre. Très tôt, il montre des signes de génies en apprenant notamment à lire seul en trois semaines.

Lorsqu'il a 13 ans, il se lie d'une grande amitié pour un certain **Christopher Morcom,** un brillant étudiant en sciences et en mathématiques. Son ami meurt de la tuberculose bovine. Effondré par cette nouvelle et persuadé que l'esprit de Morcom continue d'exister, il se fait la promesse d'accomplir le destin scientifique de son ami. Il se spécialise très rapidement dans **la cryptographie, c'est-à-dire en déchiffrage de code secret.**

Au début de **la seconde guerre mondiale,** il rejoint les services secrets afin de déchiffrer **la machine Enigma** des nazis réputée comme incassable. Pour la décrypter, il faudrait trouver le bon réglage parmi 159 000 000 000 000 000 000 de combinaisons par jour. Il décide alors de créer la nouvelle « BOMBA » **capable d'interpréter les messages en se basant sur un raisonnement binaire**. Il vient tout simplement **d'inventer l'ordinateur.**

Son invention a permis aux Anglais de décrypter 85 000 messages allemands par mois et est notamment à l'origine de la réussite du débarquement en Normandie. Son invention a permis de raccourcir la guerre de 2 ans et sauver 14 millions de personnes.

Après la guerre, il développe les premiers ordinateurs et explore la **théorie de l'intelligence artificielle.** Il fait le pari que dans 50 ans, on ne pourra plus différencier une réponse humaine d'un ordinateur. Aujourd'hui, avec l'arrivée de CHAT GPTcela lui donne raison.

Si **son homosexualité** l'a empêché d'être reconnu de son vivant à sa juste valeur, aujourd'hui il est considéré comme **un héros.** Il a été gracié par la reine Elisabeth II. Un prix est décerné tous les ans au même titre qu'un prix Nobel.

Il se suicide le 7 juin 1954 à Wilmslow. Selon la thèse officielle, il a commencé à manger une pomme imbibée de cyanure. Certains y voient un symbole, **le logo de l'entreprise Apple.**

II- Un film retrace la vie d'Alan Turing

Depuis les années 2000 et la révélation du rôle d'Alan Turing durant la Seconde Guerre mondiale, les hommages destinés au scientifique se multiplient. Ainsi, en 2014, le réalisateur norvégien Morten Tyldum conçoit le film **Imitation Game** avec Benedict Cumberbatch dans le rôle d'Alan Turing. Il relate la façon dont Alan Turing, soumis à une intense pression, contribua à changer le cours de la Seconde Guerre mondiale et de l'Histoire. C'est aussi le portrait d'un homme qui se retrouva condamné par la société de l'époque en raison de son homosexualité et en mourut.

D'autres films, mais aussi des **pièces de théâtre notamment « La machine de Turing- Benoit Solés »** (4 molières) et des ouvrages divers saluent l'incroyable vie d'Alan Turing.

III- Biographie courte d'Elizebeth Smith Friedman

Elizebeth Smith Friedman est née le 26 aout 1892 à Huntington, dans l'Indiana et morte le 31 octobre 1980. Elle est reconnue pour être la première femme dans le domaine de la cryptologie. Elle était mariée à un autre cryptanalyste, William Friedman qui a déchiffré la célèbre machine japonaise Purple lors de la Seconde Guerre mondial.

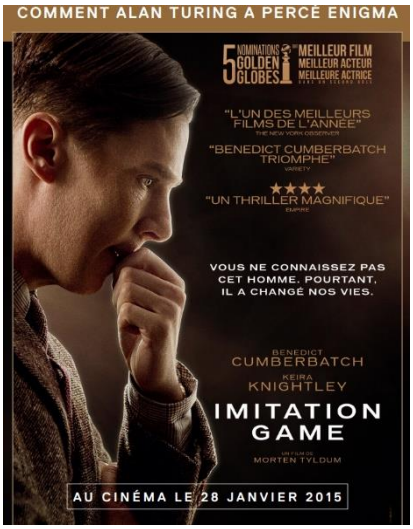
Contrairement à Alan Turing, sa vie n'a pas fait l'objet de films… Elle a pourtant autant de mérite que lui, puisqu'elle est parvenue à déchiffrer les codes nazis de la Seconde Guerre mondiale, contribuant de fait à sauver des milliers de vies.

Mais **en raison du sexisme institutionnel de l'époque, de sa personnalité effacée et de ses homologues masculins**, Smith Friedman fut en grande partie rayée de l'histoire jusqu'en 2017.

Grace à l'ouvrage ***The Woman Who Smashed Codes*, de Jason Fagone**, nous apprenons que Smith Friedman a passé, plusieurs années :

- à chercher des **messages cachés dans les œuvres de Shakespeare** pour le compte d'un mystérieux millionnaire
- a **démantelé des réseaux de contrebande d'alcool sous la Prohibition**. Les trafiquants utilisaient des messages radio codés afin d'empêcher les garde-côtes de se renseigner sur leurs opérations.
- a **décrypter des codes nazis et de la machine Enigma** pour la Garde côtière des États-Unis pendant la Seconde Guerre mondiale. Son équipe démantèle ainsi tous les réseaux d'espionnage nazis présents sur le continent sud-américain.

IV – L ELEVE DOIT ËTRE CAPABLE DE…



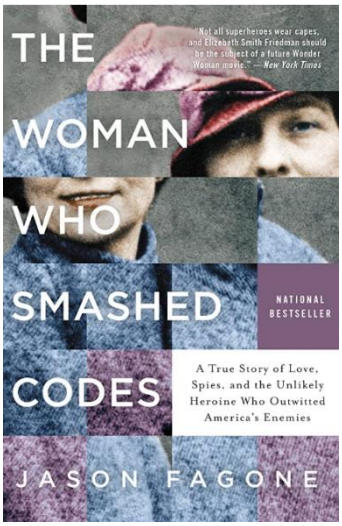
1) Donner la définition de la cryptographie. A quoi sert-elle ?
2) Faire la différence entre Décrypter / Crypter
3) Présenter Alan Turing : sa vie, son parcours, ses réalisations
4) Dire « comment Alan Turing a percé la machine Enigma ? »
Attention, les élèves ne doivent pas confondre la machine Enigma avec la machine inventée par Alan Turing pour déchiffrer la machine Enigma
5) L'impact sur le déroulement de la guerre
6) L'importance de la cryptanalyse pendant la guerre
7) Héritage et hommage à Alan Turing
8) Vous parler du film IMITATION GAME
9) Vous parler du contexte historique : la seconde guerre mondiale

Pour les élèves de 3e3,
- la Seconde Guerre mondiale (causes, grandes étapes de la guerre, événements majeurs) et intégration des éléments sur Alan Turing et la cryptographie dans le cours sur le tournant de la guerre et les débarquements alliés.
- Mettre en lumière l'évolution de la société française entre les années 1950 et 80.

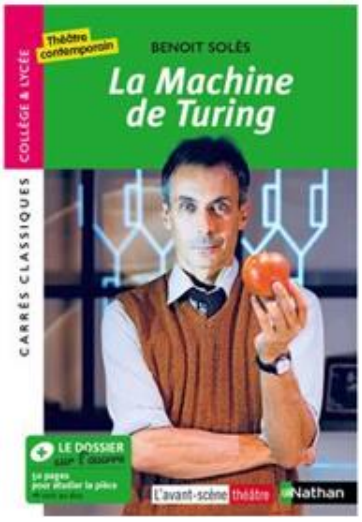
Pour les élèves de 3e6, 3e1 et 3e2,
- la Seconde Guerre mondiale (causes, grandes étapes de la guerre, événements majeurs) et intégration des éléments de la cryptographie dans le cours.

10) Vous parler de la pièce de théâtre « La machine de Turing » (pas pour les 3e6)

11) Présenter Elizebeth Smith Friedman.




An Enigma Machine.



Quelques photos lors du premier tour du Concours ALKINDI.