Introduction :

Eureka, j'ai trouvé le code ! Est une phrase qu'aurait pu prononcer Alan Turing. En fait, Alan Turing est une personnalité si riche et si modeste, tant cachée puis tant exposée aujourd'hui, tellement ouverte et tout aussi hermétique que tout un chacun cherche à donner du sens à tous ces faits et gestes. Alan Turing est désormais dans un processus d'idéalisation. Il est actuellement la source d'inspiration de groupes sociaux et d'artistes.
Beaucoup lui ont prêté des intentions qu'il ne pouvait pas avoir eues.
Ces dernières années, on dénombre un film, plusieurs documentaires, un oratorio, différentes fictions au théâtre, une bande dessinée, des romans, une chanson, des bandes-sons de musique électronique en son hommage.
En 2009, des associations de défense des droits de l'homme dénoncent le traitement dégradant que l'État anglais lui a infligé à cause de son homosexualité. Ces démarches militantes aboutissent à un « pardon royal » de la Reine d'Angleterre en 2013, ce qui efface de facto sa condamnation pour « outrage à la pudeur »de 1952.
Alan Turing est un symbole.
Alan Turing est aussi une icône populaire, à qui on a attribué la création du logo d'Apple, la pomme croquée, car ce serait une pomme qui l'aurait empoisonné en 1954, sans que personne ne puisse le certifier. L'histoire de cet homme nourrit donc son mythe, la réalité de l'individu se transforme en de multiples images, alimentées par les découvertes quotidiennes sur l'Intelligence Artificielle.

Pour bien comprendre qui fut Alan Turing, je m'appuierai sur son biographe Andrew Hodges qui intitula l'ouvrage qu'il lui consacra en 1983 « Alan Turing : the Enigma ». Un lecteur y trouvera la polysémie du terme plus que pertinente ; Enigma, en tant que nom propre, est la machine à coder nazie qu'Alan Turing déchiffra si facilement ; quant au nom commun Enigma il a en anglais le même sens, qu'en Français le mot énigme. Sans doute est-ce ce mystère Alan Turing qui stimule l'imagination de nombreux intellectuels et artistes. Cette biographie d'un mathématicien d'Oxford fit entrer Turing dans la lumière, il devint dès lors un personnage public.

Par ailleurs, afin de situer Alan Turing dans l'histoire des mathématiques, j'ai utilisé les travaux du philosophe Jean Lassègue, notamment le numéro 29 du magazine « Pour la science » de janvier 2008 ainsi que le numéro 476 de ce même magazine de juin 2017 sur l'Intelligence Artificielle.

Enfin, le numéro 8115 de la Documentation Photographique de Stéphane Van Damme intitulé « Science en société » permet de donner une perspective historique aux mathématiques.

Pour la partie pédagogique, je me suis appuyé sur les travaux du chercheur du Computer Laboratory de Cambridge, Sam Aaron.

Cambridge, son université, et voici la boucle bouclée. Alan Turing y étudia et enseigna, dans le climat si favorable à l'émergence de nouvelles idées. Cambridge, cette université avant la seconde guerre mondiale, c'est aussi l'université de Kim Philby, recrue de l'Union Soviétique, et Alan Turing , s'il est difficile d'établir pour ce qui le concerne, des options politiques tranchées, était un homme de son temps et un citoyen engagé.

La problématique à laquelle je répondrai est une reformulation de celle proposée par les RVH de Blois, à savoir « les sciences filles de la guerre ? Ou la guerre fille des sciences ? ».
Cela revient à se demander si Alan Turing était un génie isolé, un pur esprit ou au contraire si sa théorie a éclos grâce à la guerre mondiale ? L'ordinateur et le code sont-ils les enfants naturels de la guerre ?

Une thèse, qu'on trouve aujourd'hui sur You Tube et aussi dans un documentaire diffusée sur Arte , serait qu'Alan Turing aurait gagné la guerre grâce à son esprit mathématique. Les mathématiques seraient-ils plus forts que les bombes ? Travailler sur ces questions en classe amène à étudier le codage informatique. Turing a inventé un langage , qui , aujourd'hui, nous permet de faire fonctionner des machines, de créer des programmes. Ce codage peut s'étudier en cours d'histoire, en collaboration avec un enseignant de français, de mathématiques ou bien de musique.

Je vais développer un plan en trois parties. Tout d'abord, les mathématiques avant la seconde guerre mondiale et le rôle d'Alan Turing dans leur développement. Deuxièmement, la machine Enigma et Alan Turing durant la guerre. On examinera le génie d'un homme dans l'incubateur périlleux des années d'affrontement total avec le nazisme. Troisièmement, le legs d'Alan Turing : l'informatique, le codage, partie dans laquelle nous proposerons des pistes pédagogiques pour créer des programmes à partir du logiciel « Sonic pi » de Sam Aaron.

1. Le parcours intellectuel d'Alan Turing (1931-1935)

1.1. La perte de son alter ego : Christopher Morcom

En février 1930, à 17 ans, Alan Turing est un lycéen anglais vivant à Sherborne, une petite ville du sud. Il perd son meilleur ami, Christopher Morcom. La mort de Christopher Morcom affecte Alan Turing. Non seulement, il l'aimait, mais de plus, il partageait avec lui la même passion pour les sciences. La douleur conçue par l'adolescent donne naissance à une façon de raisonner dans deux dimensions. Pour Alan Turing adolescent, la perte de cet alter ego dans le monde réel s'atténue lorsqu'il imagine qu'il peut encore communiquer avec lui. Il écrit à la mère de l'adolescent en 1932 « Je crois personnellement que l'esprit est éternellement lié à la matière, mais sûrement pas systématiquement par le biais d'un même corps. Je ne sais pas ce qui peut se passer quand le corps est endormi, toutefois quand il meurt, le « mécanisme » qui retient l'esprit s'éteint aussi et ce dernier se voit contraint de trouver tôt ou tard, peut-être immédiatement, un nouveau corps » Dans l'intelligence d'Alan Turing, on retrouve une part de sentimentalisme. Il mène une quête de l'inexploré. Cette blessure d'adolescent ne se referme pas, elle agit comme un stimulus pour explorer des zones inconnues et invisibles. Toute sa courte vie, Alan Turing monte des systèmes alliant la mécanique si prévisible du corps et des machines à celle infinie et indéfinissable de l'esprit. Alan Turing meurt en 1954. Il va passer durant ces 25 années, de l'âge de 17 ans à l'âge de 42 ans, sans cesse entre ces deux dimensions. Ce qui fait qu'on peut parler d'un véritable destin à la fois tragique, scientifique et magique.

1.1.1. L'entrée à Cambridge

Lorsqu'il rejoint l'université en 1931, au King's College de Cambridge, les mathématiques pures absorbent Alan. Elle lui offre une véritable échappatoire au réel. La mécanique quantique est le champ d'investigation des mathématiciens de cette université. La difficulté réside pour eux dans l'indétermination du trajet des particules, leur manière aléatoire de se diriger. Comment les mathématiques peuvent décrire les parcours des électrons ? Il s'agit de trouver un modèle mathématique pour rendre visible et compréhensible les trajets des particules. Les travaux d'Eddington, un des professeurs d'Alan, l'amènent à réfléchir sur cette dualité entre la matière et l'esprit. Pour Eddington, le déterminisme n'a plus cours. Les notions de présent et de passé, la différence entre le corps et l'esprit ne sont plus pertinentes pour définir le mouvement de ces particules. Si on veut cerner l'invisible, il faut trouver d'autres façons de voir.

1.1.2. La 2ème année : 1932

En 1932, Alan Turing obtient son passage en deuxième année du cursus sans briller encore particulièrement. Il part en vacances d' été en Irlande avec un de ses amis. Il semble sortir de sa dépression. Ses amis notent sa soif de comprendre tout ce qui l'entoure. Il capture des mouches pour étudier leur reproduction. Il amuse son entourage par son enthousiasme et sa joie de vivre.
A Noël, il rencontre le père d'un de ses amis, Monsieur Beuttell, persuadé que le cerveau fonctionne par impulsion électrique. Monsieur Beuttell lui demande de l'aide pour effectuer des calculs sur l'éclairage électrique des nouveaux locaux de la franc-maçonnerie à Sherborne. Monsieur Beutell lui interdisait cependant d'entrer dans la loge, car Alan n'était pas franc-maçon. Il imagina donc la salle et fit sur papier tous les calculs nécessaires pour obtenir les bons éclairages.

Ces rencontres amicales et familiales approfondissent les intuitions d'Alan Turing sur la jonction possible entre l'invisible et sa formalisation mathématique par le biais du calcul. Alan Turing ne se nourrit cependant pas que de calculs aveugles et de cours théoriques.

Transition : Alan Turing vit en effet une époque de remises en cause. Le capitalisme est en crise depuis quelques années. Le système intangible de l'économie de marché s'écroule face à celui de la planification socialiste de l'Union Soviétique. Le capitalisme semble dépassé, beaucoup d'anglais estime qu'il faut une alternative pour l'Angleterre, quelque chose qui n'a encore jamais été tenté, une

économie qui ferait entrer la société dans une nouvelle civilisation.

1.1.3. les idées au King's College de Cambridge (1933)

En 1933, un vent favorable à l'Union Soviétique souffle donc sur Cambridge comme sur l'Angleterre en général. Les « comités anti-guerre » se développent mêlant des communistes, des pacifistes et des internationalistes. Alan se sent proche de ce mouvement, surtout parce que c'est pour lui un moyen de s'opposer au pouvoir. Il déclare vouloir adhérer et partir pour l'URSS, ce qu'il ne fit pas. Les idées politiques d'Alan Turing sont finalement plus proches du journal libéral le « New Statesman », qui prône à la fois le partage des richesses et l'individualisme. L'université de Cambridge baignait davantage dans ces idées progressistes. L'homosexualité n'y était pas réprimée. Les lois anglaises contre les homosexuels n'étaient pas appliquées. Il existait même des sections de l'université pour les filles, ce qui n'était pas le cas de Princeton aux USA, par exemple. Le climat de tolérance permettait de discuter très librement de tout. Aussi, on imagine difficilement Alan Turing en Union Soviétique, qui avait soumis la mécanique quantique à des critères politiques. Alan Turing fuyait la rigidité et s'épanouissait dans ce microcosme libertaire de Cambridge. A Cambridge, dans les années 1930, on pouvait être un hérétique. Personne n'avait l'idée de vous blâmer pour votre originalité ou votre différence.

Transition : En fait, ce qui va enflammer Alan Turing, ce ne sont donc pas les communistes de Cambridge, c'est une série de rencontres avec ses professeurs et les différents intervenants de Cambridge.

1.2 Les Maths à Cambridge (1933-1935)

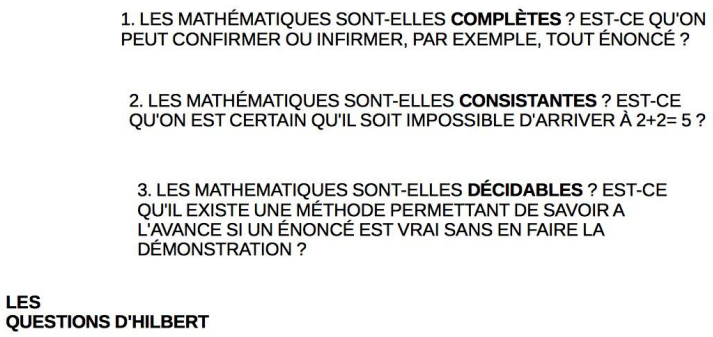
1.2.1. Von Neumann : la mécanique quantique et Hilbert : l'imaginaire et l'infini

Sa rencontre avec les concepts de Von Neumann, chercheurs de particules invisibles, les électrons et les atomes, le fascine bien plus que l'alternative socialiste. Alan Turing inaugure alors une odyssée dans le monde de l'invisible et pousse les frontières au-delà de toutes limites. En octobre 1933, il a terminé « Les fondements mathématiques de la mécanique quantique » de Von Neumann. La théorie de Von Neumann est l'inverse de celle d' Eddington. Pour Von Neumann, les particules obéissent à des lois mécaniques et déterministes. Le hasard est introduit par celui qui observe. L'observateur extérieur aux particules introduit un hasard absolu et déterminé. Il n'y a aucun moyen de savoir ce qui se passe tant que nous n'avons pas de bonnes lunettes.

Cette idée renverse les conceptions d'Alan. Cette approche est d'abord celle d'un physicien. Mais Von Neumann s'appuie sur des modèles crées par des mathématiciens pour appréhender les particules.
Il reprend ainsi la théorie de l'espace d'Hilbert selon laquelle l'espace contient un nombre infini de dimensions. Il n'a rien à voir avec l'espace physique. Cet espace correspondrait à un schéma reproduisant les sons des instruments de musique. Chaque son de base se démultiplierait en une quantité considérable d'autres sons dérivés , donnant une dimension nouvelle à chaque fois et chaque instrument serait lui-même une dimension. Pour Von Neumann, ce modèle donnerait la possibilité d'observer l'état d'un électron dans un atome d'hydrogène. Ces états observés pourraient s'additionner comme les sons, et les états des particules seraient ainsi infinis comme les sons de l'espace d'Hilbert.

Cette thèse est alors enseignée à Cambridge, par le professeur Newmann. Pour Alan Turing, un mur s'écroule entre le réel d'une part et d' autre part, en face de celui-ci, l'infini des calculs. Aux espaces infinis d'Hilbert, se double les questions d'Hilbert soumises aux étudiants et mathématiciens. Hilbert interroge la valeur et la réalité même des mathématiques. Il pose les questions suivantes, qui sont

autant d'énigmes à résoudre. La première question est « les mathématiques sont-elles **complètes**, au sens où chaque énoncé (comme par exemple « tout nombre entier est la somme de quatre carrés ») peut être confirmé ou infirmé ? Les mathématiques sont-elles **consistantes**, au sens où il est impossible d'arriver par une suite d'étapes correctes à l'énonce 2+2+=5 ? » Les mathématiques sont-elles **décidables**, c'est-à-dire existe-t-il une méthode permettant de décider à l'avance, sans en faire la démonstration, si un énoncé mathématique est vrai ? «
Hilbert est persuadé que toutes les réponses seront positives. Mais il lance le débat. Rapidement, des mathématiciens répondent. Le premier est le tchèque Kurt Gödel. Il prouve que certaines propositions en mathématiques ne se démontrent pas. Les mathématiques sont donc incomplètes. Il montre également que toute opération logique est par nature arithmétique, c'est-à-dire qu'il ne s'agit que d'une succession d'opérations de calculs et de comparaisons. Il invente un codage, chaque nombre correspondant à une opération logique. Il affirme ensuite que ce codage ne peut être vérifié comme vraie ou fausse tout comme on ne peut vérifier si une personne qui dit « je mens » ment effectivement ou dit la vérité. On peut interpréter la phrase dans les deux sens, il n'existe donc aucune vérité. Les mathématiques sont donc pas consistantes. On peut arriver à n'importe quel résultat car tout est symbole et codage.



1.2.2. La machine de Turing : été 1935

Alan Turing répond, lui, à la troisième question d'Hilbert : peut-on dire, si toute assertion, peut être démontrée ou non ? Est-ce qu'on peut savoir à l'avance, sans le réaliser, si un calcul est faisable ou pas. Les mathématiques sont-elles **décidables ?**

C'est en faisant un footing qu'il a une intuition : créer une entité physique pour capter l'abstraction des calculs. Il imagine une machine à écrire, d'un type particulier.
Il lui donne les attributs de la logique et de la cohérence des mathématiques de son époque.
Dans cette machine imaginaire, le ruban est infini. Celui-ci n'a pas de couleurs rouge et noir mais des cases. Le papier est supprimé. La machine ne va jamais à la ligne. Le ruban est pré-imprimé et contient des symboles : soit des barres horizontales soit le vide , dans ce cas, le symbole est la case elle-même) , personne n'actionne le clavier, il agit tout seul. Il suffit juste de l'enclencher pour qu'il parte.

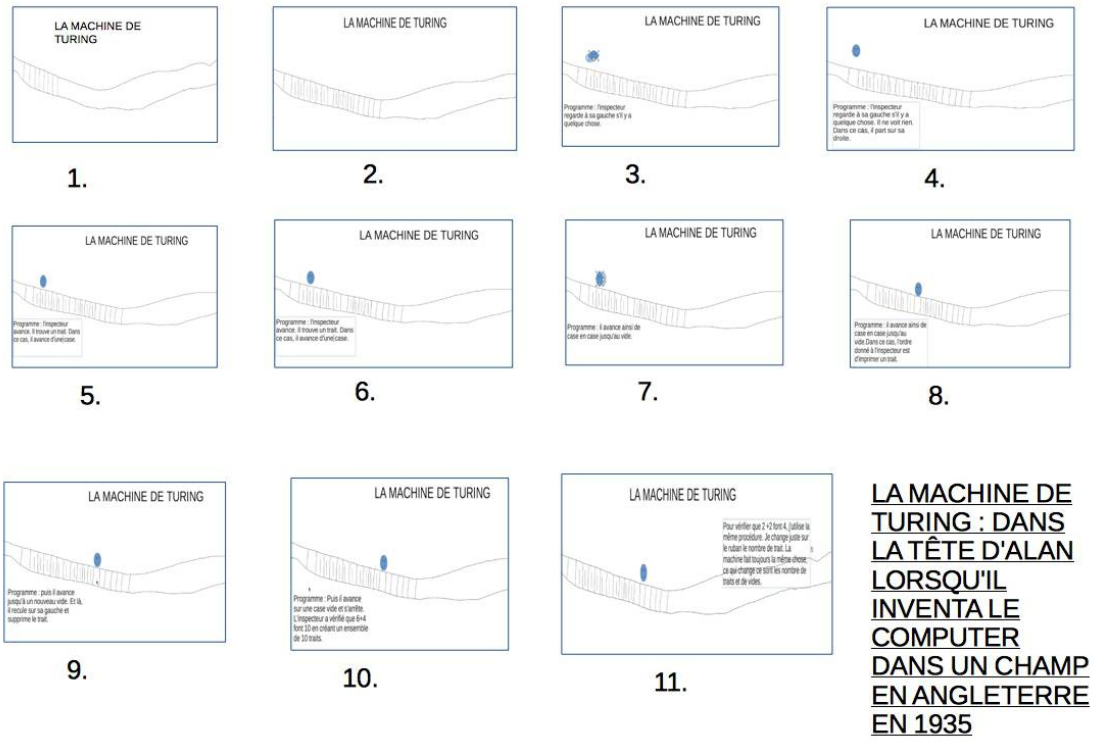
La machine inspecte les cases. Elle regarde si les symboles conviennent. Soit elle passe la case, soit elle imprime une barre, soit elle efface. Elle a donc trois fonctions.
Il ne reste plus qu'à la faire fonctionner. Alan Turing veut vérifier que 4 +6 font 10. Il crée donc sur

le ruban des cases.
La machine regarde les cases. Quand la case est vide, la machine avance sur sa droite. Quand il y a un trait, elle avance également. Mais si la case suivante est vide, elle imprime un trait. Elle continue à inspecter sur sa droite. A la case vide suivant un trait, elle recule sur sa gauche et supprime le trait. Puis elle avance sur une case vide et s'arrête.

A la fin, la machine a effectivement vérifié que 4+6 font 10 car elle a crée un ensemble de 10 traits.

En fait, la machine a toujours le même programme pour les additions : pour vérifier que 2+2 font 4 et pas 5, elle utilise la même procédure. Les instructions sont toujours les mêmes, ce qui change c'est la valeur des chiffres.
Il semble donc qu'Alan ait répondu à la question d'Hilbert : on peut savoir si un calcul est faisable, il suffit de lancer la machine, le « computer » et attendre. Les mathématiques sont donc décidables. Sauf que les chiffres sont infinis. Le computer ne va donc jamais s'arrêter. Et donc l'être humain attendra l'éternité. Il ne saura donc jamais si son opération est calculable. Alan Turing répond finalement que, dans l'absolu, il est impossible de dire à l'avance si un calcul vaut la peine d'être entrepris, c'est insoluble. Par contre, si l'être humain sait à l'avance quelle limite il donne au calcul (par exemple, le nombre de décimales après la virgule), s'il sait à quel moment le computer doit s'arrêter de certifier des additions pour passer à des multiplications, on peut laisser la machine tourner très longtemps . Il suffit de lancer le programme en code binaire, avec donc des zéros et des un. La machine calcule et pendant ce temps, le mathématicien peut partir courir le marathon, comme savait si bien le faire Alan Turing.

Alan Turing vient d'inventer le codage : avec un symbole, le trait, et une absence de symboles, l'absence de trait , il vérifie tous les autres calculs, basés eux-mêmes sur des symboles. Eureka, il a trouvé le code ! Il a inventé un système de signes qui vérifie les autres signes, de façon rigoureuse et logique. Le problème est que peu de personne comprenne son intuition. D'ailleurs, Hardy, un de ses professeurs estimait que « seuls des idiots croient que les mathématiciens font leur découvertes en tournant la poignée de quelque machine miraculeuse ». C'est pourtant ce que vient d'imaginer Alan, une machine magique à calculer, presqu'à l'infini.



2. La machine Enigma : le jeu d'énigmes d'Alan Turing (1936-1954)

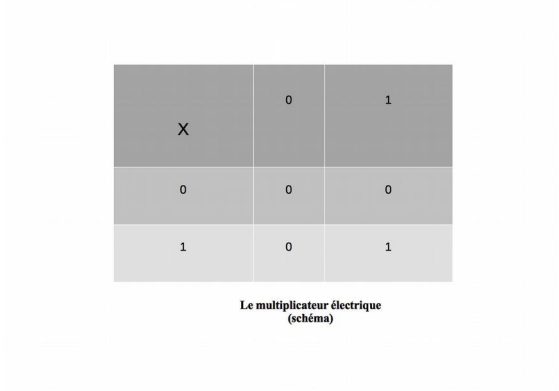
2.1. L'épisode américain de Princeton

Turing fait part de sa découverte au professeur Newmann. De manière concomitante, un autre mathématicien américain, Church démontre qu'il existe bel et bien des problèmes insolubles. Alan décide alors de se rendre à l'université de Princeton, aux États-Unis pour travailler avec Church. Grâce à Newmann, il obtient une bourse et part aux USA en septembre 1936. Princeton est alors le point de convergence des plus grands mathématiciens et physiciens. Il croise Albert Einstein, assiste au cours de Von Neumann. Il rencontre Church avec lequel il entame une fructueuse collaboration.

A Princeton, Church lui demande de faire une conférence sur sa machine. Il publie un article la détaillant. L'article rencontre peu d'échos dans la communauté scientifique. En fait, Alan bien qu'il soit conscient de l'aspect révolutionnaire de son raisonnement, n'intègre pas les codes sociaux de l'université de Princeton. Il faut savoir se vendre, entretenir une cour, pour que ses idées soient connues. Alan est aux antipodes d'un tel comportement.

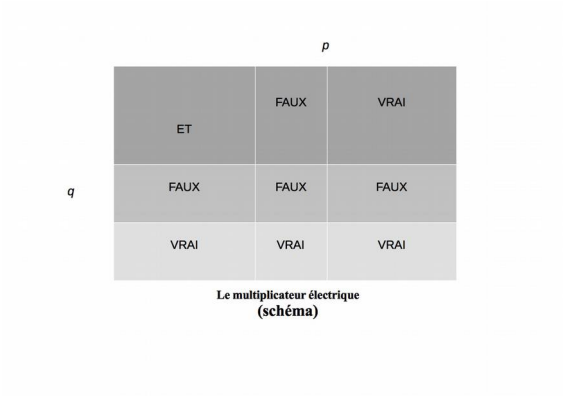
A l'automne 1937, Alan Turing prend sans doute conscience que la guerre se rapproche de l'Angleterre. Il continue à concevoir des codes.
Il fabrique un multiplicateur électrique. Mais pour éviter d'entrer trop de chiffres dans son multiplicateur, il décide de coder tous les chiffres par des suites de 0 et de 1. Il se sert du courant électrique. Un 1 correspond à une impulsion électrique du circuit, un 0 à l'absence d'impulsions.Un premier circuit électrique codait les chiffres en 0 et 1, un second circuit, relié par un commutateur à relais donnait le chiffre pour que l'opération se fasse. La multiplication était également réalisée

grâce aux impulsions d'un autre circuit. En fait, Alan Turing met en application sa machine de Turing. Tous les nombres se codaient à partir de ce système binaire. Il suffisait ensuite d'opérer une multiplication.
Il étend ce multiplicateur à la logique en remplaçant la multiplication par la conjonction de coordination **et ,** le zéro par faux et le 1 par vrai. Il obtient ainsi des combinaisons sur la vérité ou le mensonge d'une phrase, réduite elle-même à un code (par exemple : je mens = p ou je dis la vérité = q). Ce procédé était déjà utilisé, mais Turing mécanise l'idée.



X	0	1
0	0	0
1	0	1

Le multiplicateur électrique (schéma)



p

ET	FAUX	VRAI
FAUX	FAUX	FAUX
VRAI	VRAI	VRAI

q

Le multiplicateur électrique (schéma)

Malgré son absence de stratégie de réussite, le petit milieu de Princeton s'intéresse à ces travaux. Von Neumann lui propose de devenir son assistant dans le laboratoire qu'il vient de créer, laboratoire qui travaille sur la mécanique quantique.

Alan Turing refuse. Il présente sa thèse en juin 1938, sur les affirmations vraies mais impossibles à démontrer, une assertion de Kurt Gödel. Il rentre en Angleterre le 18 juillet 1938, pressé, car la guerre est proche, et Turing craint une invasion allemande de l'Angleterre.

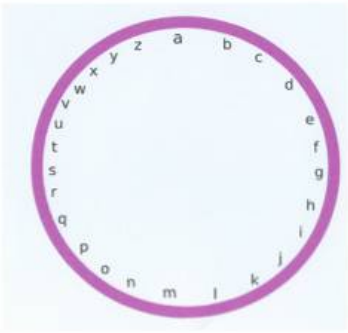
2.2. Les machines Enigma

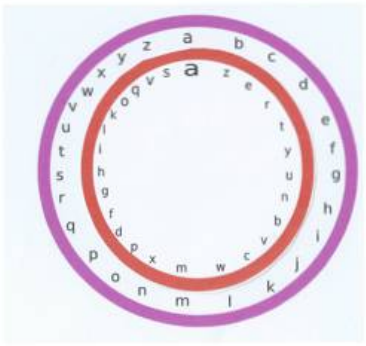
2.2.1. L'équipe polonaise

En 1938, la guerre contre l'Allemagne est donc imminente. Le gouvernement anglais s'est engagé auprès du gouvernement polonais. Les français sont également partenaires de ces deux pays, en tout cas en matière de renseignements. Depuis quelque temps déjà, les services secrets ont réussi à voler des machines Enigma aux allemands. Cette machine, vendue dans le commerce dans les années 1920, est perfectionnée par l'armée allemande pour coder ses messages.
Elle fonctionne sur le principe de la substitution. Le cadran d'Alberti, qui date du 15ème siècle, est la base de fonctionnement de la machine Enigma.

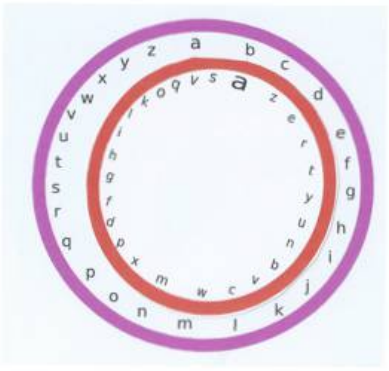
LE CADRAN D'ALBERTI, 15ÈME SIÈCLE

Dans un premier cercle fixe, les lettres sont placées dans l'ordre alphabétique.

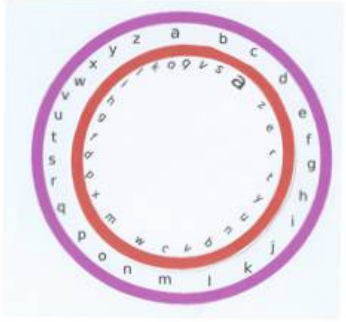




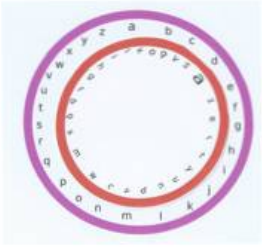
Un second cercle amovible contient des lettres dans un ordre que seul le récepteur connaît. Ici, il s'agit de la position initiale du deuxième cercle de lettres. Le a est sur le a, le b sur le z et le c sur le e.



Une fois que les cercles sont placés, le codage commence. Le cercle du dessous tourne à chaque fois qu'une lettre est codée. Si le a donne un a au premier tour, au second il est sur un b.



Puis le a devient un c, tandis que toutes les autres lettres changent en même temps.



Et ainsi de suite. Il existe 26 possibilités différentes de coder le a.

La machine Enigma fonctionne sur ce principe, mais avec 5 roues (les rotors). Ce qui multiplie d'autant les possibilités.

La machine Enigma est plus complexe. Elle utilise plusieurs rotors et un cablage particulier. Les lettres se transforment par substitution. On tape une lettre, il en sort une autre, qui s'éclaire sur une ampoule électrique

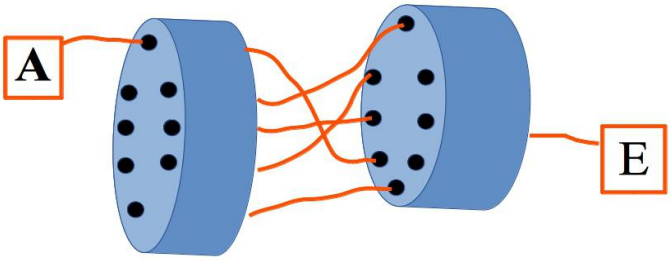
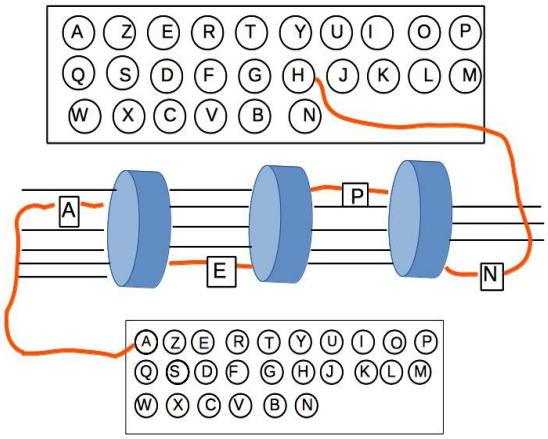


ILLUSTRATION DU CABLAGE ÉLECTRIQUE D'UN ROTOR D'UNE ENIGMA DE BASE (d'après « comment les maths ont vaincu Hitler »)

Comme dans le cadran d'Alberti, il y a bien deux roues comportant chacune un alphabet dans un ordre différent. Mais la transformation de la lettre se fait par le biais de câbles électriques. Il faut donc connaître le câblage pour savoir comment la machine code. Il est donc nécessaire de voler des machines Enigma aux allemands.



LE CIRCUIT D'UNE LETTRE DANS LA MACHINE ENIGMA DE BASE

La lettre passe ensuite dans plusieurs roues, qui codent à chaque fois de manière différente. A la fin, la lettre refait un tour complet. Il existe donc, initialement, deux systèmes de brouillage : celui des roues et celui de la révolution de la lettre dans la machine. Ici, il s'agit du schéma d'une des première machines Enigma, elle ne comporte que trois roues.

Ces lettres font donc un circuit. On peut le décoder à condition de connaître l'état initial des roues dentées du circuit, avant que l'opérateur commence à taper son texte. Il existe 26 positions différentes pour chaque roue, elles sont au nombre de 3. Cela fait donc qu'il existe 26 x 26 x 26 positions différentes, soit 17 576 états possibles des roues. La machine Enigma n'a rien de novateur, hormis l'ampoule électrique. Tour d'abord, le chiffreur envoie en morse un message codé. Le destinataire le reçoit. Grâce à ce message, il positionne les roues, pour créer un état initial de la machine similaire à celui utilisé par l'émetteur pour coder le texte. Puis, il entre le texte chiffré dans la machine. Texte codé qu'il a également reçu en morse. Enigma donne alors le texte en clair. Ce système est très simple à utiliser pour l'armée allemande.
L'armée allemande est persuadée que sa machine est infaillible. Pourtant en 1938, cela fait déjà 6 ans que les services du chiffre polonais décryptent tous les messages émis par Enigma.

Au départ, il s'agit d'une équipe de mathématicien polonais qui se contente de déductions logiques. En effet, la première machine Enigma comportait 3 rotors, trois roues dentées. Lorsque Berlin voulait coder un texte, les services du chiffre nazi envoyaient 3 lettres à l'ensemble de leurs forces armées : soit à 500 sous-marins environ, 200 bases terrestres, plus tout le commandement. Ils envoyaient le même message radio à environ 1000 destinataires. Il suffisait aux polonais ou aux anglais d'intercepter ce premier message par onde radio en morse. Après, l'équipe polonaise écoutait les réponses envoyées par les récepteurs. Si deux récepteurs pour un état initial des rotors sur RTS répondent WHJ, les polonais qui savaient déjà que la machine avait un état de départ RTS savent désormais qu'elle a un état final WHJ. Ils peuvent alors décoder les messages avec une machine Enigma, volé aux allemands. De plus, les mathématiciens polonais remarquent que la machine Enigma produit toujours les mêmes cycles et toujours les mêmes combinaisons de couples de lettres.
Ils fabriquent donc une table de correspondances de lettres.

Une deuxième version d'Enigma les oblige à revoir les indicateurs de départ en avril 1937, mais le principe de codage centralisé avec un émetteur et un millier de destinataire ne change pas.

La 3ème version d'Enigma date du 15 septembre 1938, avant la conférence de Munich. Cette fois-ci, les allemands suppriment la règle d'un émetteur pour 1000 destinataires. Chaque opérateur choisit donne son propre état initial de la machine. Il règle ces rotors sur 3 lettres, par exemple AGH. Il envoie un message radio à un destinataire lui signifiant de faire ce réglage. En fait, le destinataire sait simplement que ce signal s'adresse à lui et pas à un autre. C'est un indicateur. Le destinataire règle donc sa machine Enigma sur AGH et commence à coder. Il envoie le code à l'émetteur, comme une confirmation que les deux sont bien sur la même longueur d'onde. L'émetteur envoie alors à son tour un deuxième message par onde radio. Cette fois-ci, le message de 3 lettres donnent la position des rotors. Par exemple, cela pourrait être TUI. Il répète deux fois la position du rotor. Il envoie donc TUITUI que la machine code, par exemple, en RYNFYP. Le récepteur sait que le message lui est adressé. Le codage commence. En fait, chaque opérateur crée sa clef de cryptage pour son récepteur. L'équipe polonaise est affolée. En une nuit, tout le système devient incompréhensible. Le nombre de possibilités se démultiplient tout comme le nombre de message radio. C'est une inflation généralisée de messages et de codes. L'équipe polonaise s'aperçoit néanmoins qu'il existe de nombreuses répétitions de lettres dans les différents clefs de cryptage. Ils notent ces lettres qui se répètent toujours de la même façon dans un même message. Ils nomment ces répétitions des femelles. Ils s'aperçoivent que 40 % des clefs de cryptage ont des doublons, des « femelles ». Ils font une table des clefs de cryptage avec les doublons des lettres. Ainsi, ils savent que si les premières lettres reçues sont TUITUI, leur codage final sera comportera une répétition des lettres finales en deuxième et cinquième position, par exemple Y et Y. Puis, ils perforent les doublons sur une carte . Par exemple, ils font un trou sur la deuxième position et la cinquième. Lorsqu'ils reçoivent une clef de cryptage des allemands sous la forme de 6 lettres, ils posent les cartes perforées dessus pour vérifier si les lettres se répètent vraiment comme sur leur

table. Si les trous laissent apparâitre les bonnes lettres à la bonne position de la table crée, ils ont trouvé la clef de cryptage. Ils peuvent alors positionner les roues de la machine Enigma. Ils commencent à décoder tout le message.
Face à l'inflation des messages, ils multiplient le nombre de cartes perforées. Mais ils sont contraints de ne plus le faire manuellement. Ils inventent une machine pour explorer les trous des cartes perforées. Cette machine est branchée sur une machine Enigma. La machine à décoder utilise les impulsions électriques d'Enigma pour connaître le codage et la lettre. Lorsque les répétitions sont trouvées sur la carte, c'est-à-dire lorsque la machine tombe sur les trous de la carte perforée correspondant aux lettres de la table initiale, la machine s'arrête car elle a trouvé la clef de cryptage. Ces machines sont appelées des « Bombes » car les mécanismes font un bruit de tic-tace comme ceux d'une bombe à retardement.

Malheureusement pour les polonais, en décembre 1938, les allemands modifient de nouveau Enigma pour la quatrième fois. Ils ajoutent deux nouvelles roues dentées. Le nombre de roues dentées passe donc de 3 à 5, ce qui multiplie d'autant les possibilités de coder. Les polonais décident alors de fabriquer 10 fois plus de bombes pour décrypter. En janvier 1939, les opérateurs allemands utilisèrent de surcroît le tableau de connexion de la machine. Ce système de brouillage multipliait encore les difficultés. Cette fois-ci le nombre de possibilités dépasse largement les millions. L'équipe polonaise souhaite fabriquer 60 bombes pour décrypter les messages. Mais ils vont, très prudemment, donner les plans des Bombes aux anglais et aux français pour qu'ils poursuivent le travail. Quelques semaines avant l'invasion de la Pologne, l'équipe anglaise de décodage reçoit les plans des Bombes polonaises et des machines Enigma.

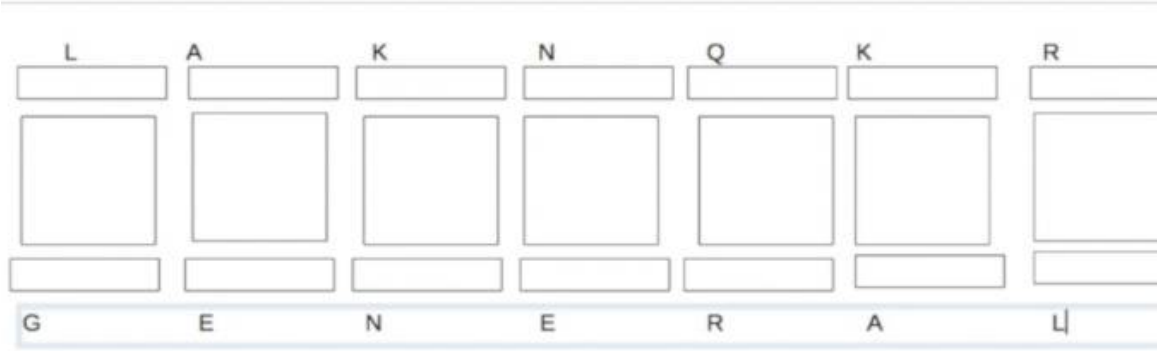
2.2.2. L'arrivée de Turing

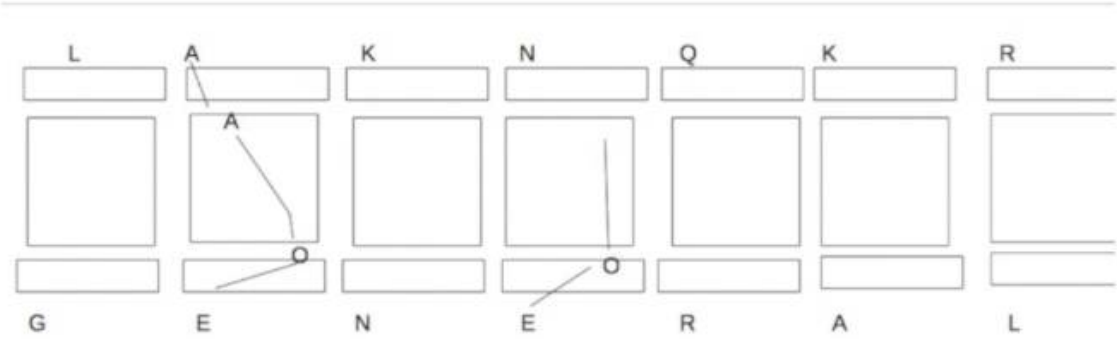
Le gouvernement britannique transmet les plans à une équipe de mathématicien à Bletchley Park, aujourd'hui à la limite du Grand Londres, près de la ville de Milton Keyes. Alan Turing fait partie de la nouvelle équipe, certainement grâce à sa réputation établie dans le milieu universitaire de faiseurs de codes.
L'équipe d'Alan Turing est soumise à ce problème apparemment insoluble car il existe plus de 100 milliards de possibilités différentes de positionner correctement la machine. Les mathématiciens anglais procèdent alors par élimination en relevant les contradictions et en cherchant les failles. Bien qu'ils n'aient pas la Bombe sous les yeux, ils vont raisonner abstraitement à partir des plans. Alan conçoit d'abord une Bombe virtuelle, une nouvelle machine de Turing imaginaire.

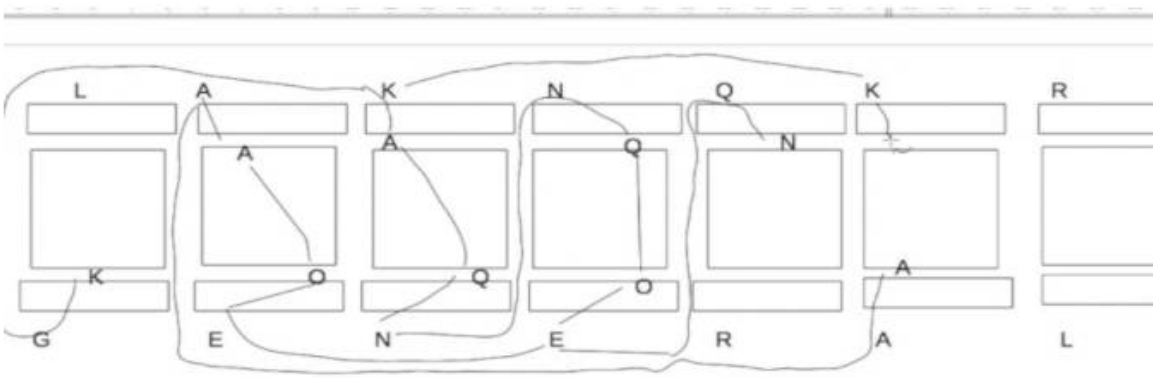
Les machines Enigma, on l'a dit, ont trois systèmes de brouillage : le premier est le tableau de connexion. Une lettre A est appareillée sur un E de manière aléatoire par un opérateur. Ensuite, cette lettre E est de nouveau brouillée par une roue dentée, qui lui donne une autre valeur, un F par exemple. Enfin, les impulsions électriques modifient une dernière fois la lettre A qui apparaît comme un F sur l'ampoule, à la fin du circuit.
Turing part de l'hypothèse que les lettres LAKNQKR code le mot GENERAL. Il dessine la machine Enigma avec deux tableaux de connexions qui sont en fait identiques.
Il réduit Enigma à un circuit électrique fermé. Il propose à ce circuit des hypothèses pour mieux les éliminer ensuite.
Ainsi ,iIl passe le A dans le rotor. Il imagine que le rotor code le A en O. Le tableau connecterait ensuite, par exemple, le O sur un E. Cela induisait la réciprocité car le tableau ne connecte qu'une fois une lettre. Donc pour chaque E connecté, on verra un O. Alan pose cet axiome de départ. Il en pose un deuxième sur le même principe. De ces deux axiomes découlent les autres combinaisons de lettres. Si les résultats concordent, le décodage est opérationnel.

Alan Turing utilise l'idée de la Bombe car il s'agit d'un circuit électrique fermé, comme son multiplicateur électrique. Les lettres sont codées par signal électrique. Une fois que les correspondances de lettres sont trouvées, le système s'arrête. C'est alors qu'une personne note la transcription du message et téléphone à une autre personne pour lui donner la transcription. Cette même personne prévient ensuite les forces armées.

LE SCHÉMA DE LA BOMBE DE TURING







Le défaut de cette méthode est qu'elle demande beaucoup de bombes et de nombreux opérateurs. Tout d'abord, il faut des opérateurs capables de reconnaître intuitivement un mot du message initial. Ensuite, il faut que le message ne contienne pas d'incohérences calculées, de faux messages déroutants à côté d'informations importantes. Au fur et à mesure de l'avancée de la guerre totale, le gouvernement britannique intensifie l'effort. Bletchley Park prend de plus en plus d'importance. En 1943, 10 000 personnes travaillent sur le décodage des messages nazis. Les Bombes de Turing sont la matière d'oeuvre de l'usine à décoder.

2.3. L'industrialisation des « Bombes ». Le deuxième voyage aux USA.

2.3.1. La rencontre avec Shannon et Bell

Le 7 novembre 1942, Alan Turing part aux USA. Le secret pèse encore sur ce voyage. On sait qu'il avait pour mission d'améliorer la collaboration entre services secrets. Les USA se sont d'ailleurs lancés dans la production industrielle de Bombes.

Pendant ce séjour, il visita les laboratoires Bell et s'intéressa au cryptage de la parole. Il rencontre Shannon. Il a de nombreuses discussions sur la théorie de l'information, l'informatique. Les deux hommes parlent de la transmission d'information par réduction de celles-ci en code binaire et évoquent la possibilité de réduire la pensée à une série de chiffres. Lorsqu'il rentre à Betchley, les chercheurs conçoivent un machine électronique de décryptage. Son ancien professeur, Newman, a conçu sa nouvelle machine sur la base des Bombes de Turing mais en utilisant des électrons. Il met ainsi au point un super-décodeur, un des premiers computer, appelé le Colossus. Newman lui propose de participer au projet mais Turing décline, une nouvelle fois.

2.3.2. Théorie de l'information et code : la machine à coder la voix d'Alan Turing

Il souhaite construire une machine pour crypter la voix. Il utilise l'électronique pour capter l'onde de la voix, et par des calculs, parvient à la comprimer pour la reconstituer. Il appelle cette machine Dalila, comme le personnage biblique. Cette machine est opérationnelle à la fin de la guerre. Elle ne trouve pas d'utilité militaire cependant.

2.3.3. Les travaux sur l'Intelligence Artificielle et les sciences naturelles

Après la guerre, Alan Turing s'intéresse au concept des machines parlantes. Il invente un test connu sous le nom de « jeu de l'imitation » ou « test de Turing », anticipant les « chats bots » d'aujourd'hui, ou agents conversationnels, c'est-à-dire ces programmes se faisant passer pour des humains, Turing proposait un dialogue au cours duquel une machine tenterait de tromper un examinateur pour lui faire croire qu'il est humain. La machine recevait des questions sur la poésie ainsi que des questions sur des calculs. En fait, Alan Turing cherche à définir le périmètre de l'intelligence. Il pose la question suivante dans un article de 1950 intitulé « Machine à calcul et intelligence : « les machines peuvent-elles penser ? »

Il étend la question au domaine des organismes vivants : l'organisation interne d'un être vivant est-il conscient? Peut-on rendre compte de cette organisation par un calcul ? Il prend alors une année sabbatique pour étudier le problème. Il tire deux conclusions : la première est que la nature est prédictive, la seconde est qu'elle ne l'est pas. Tout comme pour le calcul des nombres infinis, Turing délimite une frontière entre les deux.

2.3.4. La mort d'Alan Turing

En 1954, Alan Turing se donne la mort. Il est contraint depuis près de 2 ans de subir un traitement hormonal que l'État lui impose. Il a été jugé coupable d'outrages aux bonnes mœurs après que la police a mené une enquête sur un cambriolage dont il a été victime. Le voleur était une connaissance d'un amant d'Alan. Il passe alors de l'état de victime à celui de coupable. La justice lui propose cette peine horrible en toute bonne conscience. Il est en fait puni pour son homosexualité. Lorsqu'Alan Turing est retrouvé mort, il y a une pomme croquée, auprès de lui. La pomme n'a pas été analysée. Le suicide est prononcé, l'affaire est classée, sans enquête.

Alan Turing s'est-il suicidé ? Voici ce qu'en pense Andrew Hodges, son biographe : « Ne disposant

que peu de messages de l'esprit invisible d'Alan sur lesquels travailler, nous n'avons pu percer son code intérieur. Et d'après son propre principe d'imitation, il est tout à fait dépourvu de sens de spéculer sur des pensées non formulées. Ce qu'on ne peut pas dire, il faut le taire. Face à la vie, Alan Turing ne disposait pas ce détachement philosophique. Comme aurait pu le dire un ordinateur, l'inexprimable le laissait sans voix. »

3. Le legs d'Alan Turing : étudier le code

3.1. Le point sur l'Intelligence Artificielle aujourd'hui

Le legs d'Alan Turing aujourd'hui est sans limite. Le test de Turing a fasciné des écrivains de science-fiction et des cinéastes. Elle a inspiré les chercheurs en informatique. Aujourd'hui, les publications sur le sujet montrent néanmoins que depuis Alan Turing, les machines ont finalement peu progressé. Ainsi, une équipe internationale menée par Gary Marcus, professeur de psychologie et de neurosciences à l'université de New York, a pu montrer qu'il était impossible à un robot de dépasser le niveau de logique d'un élève de 4ème ; aucun robot n'est capable de lire par lui-même une vidéo pour en faire un récit ; aucun robot n'arrive à répondre lorsqu'il existe une ambiguïté. Par exemple, l'application Siri d'Apple ne comprend pas les pronoms et ne peut pas lever les ambiguïtés. L'assistant personnel à la mode orwellienne n'est pas né.

Vous pouvez d'ailleurs demander à un élève de créer des problèmes insolubles pour Siri mais qui sont de toute évidence pour eux. Par exemple, si vous dites à l'application : « les élèves et les professeurs se sont disputés. Ils ont dû être renvoyés et que vous demandez ensuite à Siri « qui est renvoyé ? ». Siri répond « ce n'est pas gentil ». Siri ne connaît pas le contexte de l'école, il obéit à la logique du calcul binaire, celui-ci ne souffre pas l'ambiguïté. Alors, qui est intelligent ? Est-ce que cela existe l'Intelligence Artificielle ? Ces questions sont utiles aujourd'hui pour enseigner les valeurs de l'humanisme en cours d'Enseignement Moral et Civique. Alan Turing a d'ailleurs établi qu'une machine n'était valable qu'à condition qu' un être humain puisse la contrôler.

3.2. Programmation, code et langage : les héritages d'Alan

En fait, Alan Turing est remonté à l'étymologie du mot calcul. Et c'est sans doute ce qui est faisable avec des élèves. En latin « calculus » désigne le petit caillou. Celui-ci avait deux fonctions à l'époque antique. La première est de statuer sur le sort d'un accusé. Un caillou blanc innocentait, un caillou noir condamnait. L'autre fonction est celle de dénombrer lors de la collecte les cailloux et donc le nombre de voix pour ou contre la sanction.
Le caillou est la métaphore de la décision ou bien la transcription concrète de la pensée de celui qui manipule le caillou.
Le caillou est également un ordre de grandeur. En changeant l'ordre de grandeur, on change la décision. Il s'agit d'équivalences entre l'abstraction crée par l'esprit humain à propos de questions sur la culpabilité et de compte-rendus dans la réalité. Comment faire passer le monde des idées dans la réalité physique ? Le caillou est une réponse, car il permet de représenter des chiffres et des idées.

Aujourd'hui, un ordinateur fonctionne lorsque vous lui donnez ces petits cailloux, des zéros et des un, que vous lui fournissez une tâche pour répondre à une question. Un langage informatique ne se compose cependant pas de zéro et de 1. La machine utilise les zéro et les un pour travailler. Mais l'opérateur entre des phrases dans un certain ordre. Il respecte une syntaxe et une sémantique. Dans ce cadre, une série de chiffres représente des valeurs, qui vont faire varier des réponses. Par exemple, dans le langage informatique Python, si vous voulez faire faire des additions, vous écrirez le programme :

```
mon_age = 45
mon_age =
45
```

Puis vous écrirez mon_age =mon_age+2
et la machine écrira :

mon_age
47

etc...Le legs de Turing est le système binaire qui avec des zéros et des un interprètent les phrases que j'ai écrites. L'autre héritage est le programme que je crée. Ce programme est une notice, une façon de noter et de transcrire.
Lorsque l'ordinateur a fini son calcul, il s'arrête. Sauf si on introduit dans les phrases un ordre pour qu'ils ne s'arrêtent jamais. C'est toujours l'être humain qui contrôle. Le codage est cette substitution que nous fabriquons pour faire faire des opérations à la machine. Le codage est donc une notion très extensible.

Les élèves sont initiés au codage, notamment en utilisant une application graphique du langage informatique, l'application Scratch. Ils apprennent à créer un programme pour faire déplacer un chat. Ils déplacent des blocs d'instruction, qui forment un algorithme puis ils modifient les valeurs. Le chat prend alors des positions différentes dans un petit espace.

3.3. Le codage informatique et la musique : les travaux de l'Université de Cambridge pour apprendre le code

A Cambridge, le docteur du laboratoire de calcul de l'Université Sam Aaron a mis au point une application pour coder la musique, en se basant sur les fonctions de Scratch. Sonic pi, c'est son nom est exploitable sur mac ou windows. Il a cependant été crée pour l'ordinateur de poche « framboise », le rapsberry. Cet ordinateur à très bas coût est produit à l'origine en Angleterre. Sam Aaron l'utilise pour faire travailler des groupes de jeunes élèves sur des notions de codage.

Pour travailler le codage informatique, dans l'esprit de Turing, Sam Aaron propose tout d'abord de faire écrire un programme :

```
play 70
sleep 1
play 75
sleep 0.5
play 82
```

Puis il fait fonctionner la machine.
Cela correspond à un objectif du cycle 4 en mathématique en France. La machine joue jusqu'à épuisement le morceau. Elle a donc son programme. Maintenant, en gardant le programme, on demande à un élève de modifier les chiffres, appelées variables par les mathématiciens et cela donne :

```
play 50
sleep 0.5
play 75
sleep 1
play 50
```

A ce moment, l'être humain agit sur le programme et crée son algorithme..
Sam Aaron propose une séquence sur 11 semaines pour travailler la musique et la créativité. Il associe dans ce cours des enseignants de collège à des artistes.

Il commence par faire écouter le début de *Get Lucky* de Daft Punk ***3***, puis engage une discussion sur la musique électronique.
En cours d'histoire ou de musique , il est pertinent de re-contextualiser alors la musique électronique dans le cadre d'une étude sur les rythmes. Depuis le chant de travail des afro-américains et son rythme ternaire, son tempo lent, jusqu' au rock'n roll au rythme binaire et au tempo plus rapide, l'histoire des rythmes et de la technologie épousent l'époque.

Puis, en revenant au logiciel, on propose alors aux élèves de modifier les variables pour qu'ils obtiennent leur propre sonnerie de téléphone, par exemple. On modifie ainsi le programme. On ouvre Get Lucky . Puis on décompose le morceau Puis on fait les modifications On mélange les deux modifications et on ajoute une itération. Le morceau doit être joué 3 fois : 3.times do et end. On exporte ensuite la nouvelle musique crée en format wav. Pour ce faire, il faut lancer la musique avec RUN puis cliquer au début du morceau « Rec » puis de nouveau « Rec ». Celle-ci peut ensuite être retravaillée avec Audacity afin de mêler d'autres sons.

Une étude d'impact a été réalisée par les chercheurs de Cambridge. Ils ont conclu que cette approche développait la créativité des élèves et les motivaient.

Les applications sont multiples. A nous de nous en inspirer dans la réalité dans nos établissements, à nous de faire comme Turing, de mêler l'abstraction à la réalité, l'histoire aux mathématiques, à la musique et à l'anglais, bien sûr.

Conclusion
L'informatique est très certainement la fille de la guerre. Alan Turing a pu travailler et collaborer avec Shannon parce que la guerre contre le nazisme était totale. Les Etats ont eu un rôle central dans le développement de la collaboration entre scientifiques. Cela dit, l'informatique et l'ordinateur étaient aussi au point en Allemagne Nazie. Personne n'y a pourtant vu d'intérêt. Le dogmatisme national-socialiste ne laissait pas de place au doute, encore moins au débat et à la remise en cause. Les nazis ont cru jusqu'au bout qu' Enigma était infaillible. Ils pensaient que des traîtres ou des espions livraient les secrets des codes aux anglais. Alan Turing n'aurait pu s'épanouir dans un régime totalitaire. Il fallait une démocratie, une université, une tradition intellectuelle de libre-débat pour qu'un individu aussi singulier qu'Alan Turing rêve dans un pré de la forme de l'ordinateur. Cela n'a cependant pas empêché l'État anglais de pousser cet homme au suicide.

Je dirai donc que la découverte de l'informatique et de son code est la fille de la guerre certainement mais dans un pays démocratique et libre.

Aujourd'hui, la Russie fête Kim Philby, l'espion anglais, qui, étudiant à Cambridge espionna tout au long de sa vie pour l'Union Soviétique. Dans une exposition actuellement ouverte à Moscou, le régime de Poutine célèbre celui qui sut si bien, à les en croire, livrer les plans des allemands lors de la bataille de chars de Koursk. Or, le décodage des machines Enigma joua un grand rôle également. La mémoire de Turing est encore à défendre et la recherche historique doit suivre son cours.
Pour rester dans l'esprit de Turing, je pense qu'il faut regarder de l'autre côté de la Manche, à Cambridge, pour suivre l'exemple proposé par Sam Aaron. Turing a tout imaginé, les mathématiques lui ont permis de démultiplier sa créativité. Le logiciel Sonic Pi fera peut-être naître chez nos élèves une nouvelle motivation et leur ouvrira des horizons inconnus.