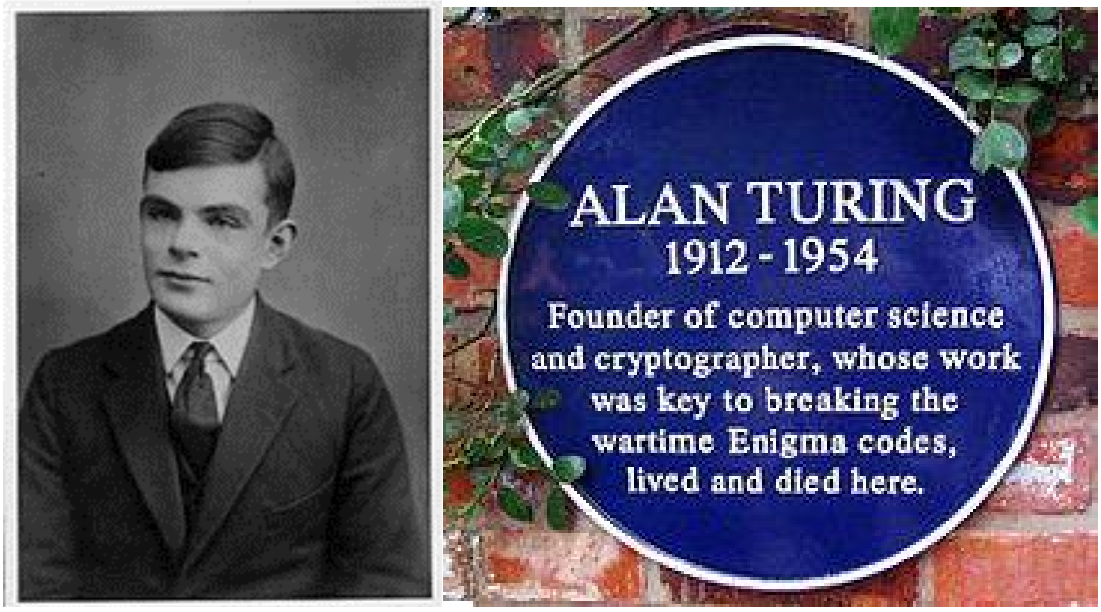
Alan Turing (23 juin **1912** - 7 juin **1954**)

biologiste, mathématicien, cryptologue et informaticien britannique



Il est l'auteur en 1936 d'un article de logique mathématique qui est devenu un **texte fondateur de la science informatique**. Pour résoudre le problème fondamental de la décidabilité en arithmétique, il y présente une expérience de pensée que l'on nommera ensuite **machine de Turing** et des concepts de programmation et de programme, qui prendront tout leur sens avec la diffusion des ordinateurs, dans la seconde moitié du XXe siècle. Avec d'autres logiciens (Church, Kleene, etc.), **Turing est ainsi à l'origine de la formalisation des concepts d'algorithme et de calculabilité**, qui fonderont cette discipline. Son modèle a contribué à établir définitivement la **thèse Church-Turing**, qui donne une définition mathématique au concept intuitif de fonction calculable.

Durant la Seconde Guerre mondiale, il joue un rôle majeur dans les recherches sur les cryptographies générées par la machine **Enigma**, utilisée par les nazis. **Ses découvertes permirent, selon plusieurs historiens, de raccourcir la capacité de résistance du régime nazi de deux ans**. Après la guerre, il travaille sur un des tout premiers ordinateurs, puis contribue de manière provocatrice au débat déjà houleux à cette période sur la capacité des machines à penser, en établissant le **test de Turingnote**. Vers la fin de sa vie, il s'intéresse à des modèles de morphogenèse du vivant conduisant aux « **structures de Turing** ».

Enfance et jeunesse. Alan Turing à l'âge de 16 ans.
Alan Turing est né à Paddington. Très tôt, il montre les signes de son génie. Il est relaté qu'il apprit seul à lire en trois semaines. Il révèle une affinité précoce pour les chiffres et les énigmes. À 6 ans, il est inscrit à l'école St. Michael's. La directrice reconnaît rapidement son talent. À 13 ans, il fréquente la Sherborne School. En 1926, durant une grève générale, Turing s'était rendu tout seul à bicyclette à son école distante de près de 90 km, s'arrêtant pour la nuit dans un hôtel.

Sportif accompli, Alan Turing sera classé, en 1948, 4ème au marathon de l'Association des Athlètes Amateurs, dont les meilleurs coureurs sont traditionnellement qualifiés pour les Jeux olympiques).

Le penchant naturel de Turing pour les sciences ne lui apporte le respect ni de ses professeurs, ni des membres de l'administration de Sherborne, dont la définition de la formation mettait plus en valeur les disciplines classiques (littérature, arts, culture physique) que les sciences.

Malgré cela, Turing continue de faire des prouesses dignes d'intérêt dans les matières qu'il aime, résolvant des problèmes très ardus pour son âge. En 1928, Turing découvre les travaux d'Albert Einstein et comprend, alors qu'il a à peine 16 ans, qu'ils remettent en cause les axiomes d'Euclide et les lois de la mécanique céleste de Galilée et Newton.

À la Sherborne School en 1927, Turing se lie d'amitié avec son camarade Christopher Morcom, passionné comme lui de sciences et de mathématiques. Leur relation est écourtée en février 1930 quand Morcom meurt des complications de la tuberculose bovine contractée après avoir bu du lait de vache infecté.

N'admettant pas la disparition complète d'un esprit aussi brillant et d'un ami aussi cher, Turing, bien que matérialiste et athée, est persuadé que l'esprit de Morcom continue à exister et décide d'incarner le destin scientifique qu'aurait dû avoir son ami.

Études supérieures et travaux sur la calculabilité.
À cause de son manque d'enthousiasme à travailler autant dans les matières classiques que dans les matières scientifiques, Turing échoue plusieurs fois à ses examens et finit par n'être admis que dans l'établissement qu'il avait mentionné par défaut, King's College de l'université de Cambridge, alors qu'il avait demandé Trinity College en premier choix.

Il étudie de 1931 à 1934 sous la direction de Godfrey Harold Hardy, mathématicien titulaire de la chaire de Sadleirian puis responsable du

centre de recherches et d'études en mathématiques. Il suit également les cours d'Arthur Eddington et, la dernière année, de Max Newman qui l'initie à la logique mathématique, notamment aux problèmes fondamentaux posés quelques années plus tôt par l'Allemand David Hilbert. En 1935, Turing est élu « fellow » du King's College, l'équivalent d'une bourse de thèse.

Son remarquable article en 1936 « On Computable Numbers, with an Application to the Entscheidungsproblem » répond à un problème posé par Hilbert dans les théories axiomatiques, le problème de la décision : est-il possible de trouver une méthode « effectivement calculable » pour décider si une proposition est démontrable ou non ?

Pour montrer que ce n'est pas possible, il faut caractériser ce qu'est un procédé calculable. Turing le fait en imaginant, non une machine matérielle, mais un être calculant, qui peut être indifféremment un appareil logique simple ou un humain discipliné appliquant des règles, comme le faisaient les employés des bureaux de calcul à l'époque.

Dans le cours de son raisonnement, il démontre que le problème de l'arrêt d'une machine de Turing ne peut être résolu par algorithme : il n'est pas possible de décider avec un algorithme (c'est-à-dire avec une machine de Turing) si une machine de Turing donnée s'arrêtera.

Bien que sa preuve fût publiée après celle d'Alonzo Church, Turing est plus accessible et intuitif. Il est novateur dans son concept de « machine universelle » dite « de Turing », avec l'idée qu'une telle machine puisse accomplir les tâches de n'importe quelle autre machine. L'article présente aussi la notion de **nombre réel calculable**.

En 1937-1938 il travaille sur divers sujets à l'université de Princeton. Il obtient en mai 1938 son diplôme de l'université. Son manuscrit présente la notion d' « hypercalcul », où les machines de Turing sont complétées par ce qu'il appelle des « oracles », autorisant ainsi l'étude de problèmes qui ne peuvent pas être résolus de manière algorithmique. L'appellation de « **machine de Turing** » vient de Church, son directeur de thèse.

En 1939 il participe à des cours de Ludwig Wittgenstein sur les fondements des mathématiques. Tous deux discutent et constatent leur désaccord, Turing défend le formalisme alors que Wittgenstein pense que les mathématiques sont surestimées et qu'elles ne permettent pas de découvrir une quelconque vérité absolue.

La salle informatique du King's College, à Cambridge, porte désormais le nom de Turing.

Cryptanalyse. Réplique de la « Bombe ».
Fin 1938, après les accords de Munich, la Grande-Bretagne comprend enfin que le nazisme est une menace, et commence à se réarmer. Turing fait partie des jeunes cerveaux appelés à suivre des cours de chiffre et de cryptanalyse à la « Government Code and Cypher School » (GC&CS). **Juste avant la déclaration de guerre, il rejoint le centre secret de Bletchley Park**.

Il y est affecté aux équipes chargées du chiffre de la machine **Enigma** utilisée par les forces armées nazies. Ce travail profite initialement des percées effectuées par les services secrets polonais et français. Mais, en mai 1940, les Allemands perfectionnent leur système cryptographique. Turing participe aux recherches qui permettent de pénétrer les réseaux de l'armée de terre et de l'aviation.

Il conçoit des méthodes mathématiques et des versions améliorées de la « Bombe » polonaise, machine électromécanique qui permet d'éliminer rapidement des ensembles de clés potentielles sur des blocs de communication d'Enigma. **Turing dirige l'équipe chargée de trouver les clés bien plus hermétiques des réseaux de l'Enigma navale**. Ces percées décisives redonnent à la Grande-Bretagne un avantage dans les batailles d'Angleterre, de Libye et de l'Atlantique.

Les capacités de décryptage de Bletchley Park et l'opération Ultra furent tenues **secret militaire absolu** jusqu'aux déclassifications au milieu des années 1970. Seuls quelques anciens cryptanalystes français et polonais ont publié auparavant quelques informations sur la lutte contre Enigma, dans leurs pays respectifs. Les techniques de décryptage d'Enigma n'ont pas été déclassées avant 2000.

Codage de la voix.
Turing part en 1943 pour les États-Unis, en mission de liaison avec les cryptanalystes américains. Il y découvre les progrès des technologies électroniques et conçoit une machine à coder la voix. Il contribue à de nombreuses autres recherches mathématiques, comme celles qui aboutiront à casser le code généré par le téléscripteur de Fish (machine construite par Lorenz et Siemens).

Cette nouvelle machine allemande, réservée au cryptage des communications d'états-majors, est très différente du système Enigma et résiste longtemps aux attaques des cryptanalystes alliés. Mais ceux-ci parviennent à percer les codes Fish, grâce à de nouvelles machines (Colossus entre autres). Cette machine, le premier grand calculateur électronique de l'histoire, fut conçue par Max Newman et construite au laboratoire des Postes de Dollis Hill par une équipe de Thomas Flowers en 1943. Turing n'a nullement participé à la conception de

Colossus. Mais il l'a vu fonctionner, ce qui a certainement contribué à l'orienter vers la conception d'un ordinateur après la guerre.

Cryptanalyse d'Enigma et Bletchley Park.

À partir de septembre 1938, Turing travaille à temps partiel pour la Government Code and Cypher School. Avec le concours d'un expert en cassage de codes, Dilly Knox, il se concentre sur la cryptanalyse d'Enigma. Après une rencontre à Varsovie en juillet 1939 où le bureau polonais du chiffre explique aux Français et aux Anglais le câblage détaillé des rotors d'Enigma et la méthode polonaise de décryptage des messages associés, Turing et Knox se mettent au travail sur une approche moins spécifique. La méthode polonaise était fondée sur le décryptage de la clef répétée au début du message, mais cette répétition était susceptible d'être supprimée, car vulnérable, ce qui arriva en mai 1940. Tenus à l'écart, les cryptanalystes polonais réfugiés en Grande-Bretagne seront affectés au décryptage de codes mineurs, tandis que les services secrets français continueront à transmettre clandestinement des informations aux Alliés.

Turing transforme la cryptanalyse, de technique élaborée qu'elle était depuis longtemps, en une branche des mathématiques.

Il ne s'agit plus de deviner un réglage **parmi 159 milliards de milliards de réglages disponibles**, mais de mettre en œuvre une logique fondée sur la connaissance du fonctionnement interne de la machine Enigma et d'exploiter les imprudences des chiffreurs allemands, afin de déduire le réglage de toutes les machines Enigma d'un réseau particulier pour la journée : disposition initiale des rotors (parmi 80 dispositions disponibles), réglage initial des rotors (parmi 336 réglages disponibles), permutations des fiches du tableau de connexions (parmi 17.500 enfichages disponibles), etc. **Turing rédige alors la première spécification fonctionnelle d'une nouvelle bombe, machine électromécanique capable d'abattre quotidiennement le travail de 10.000 personnes.**

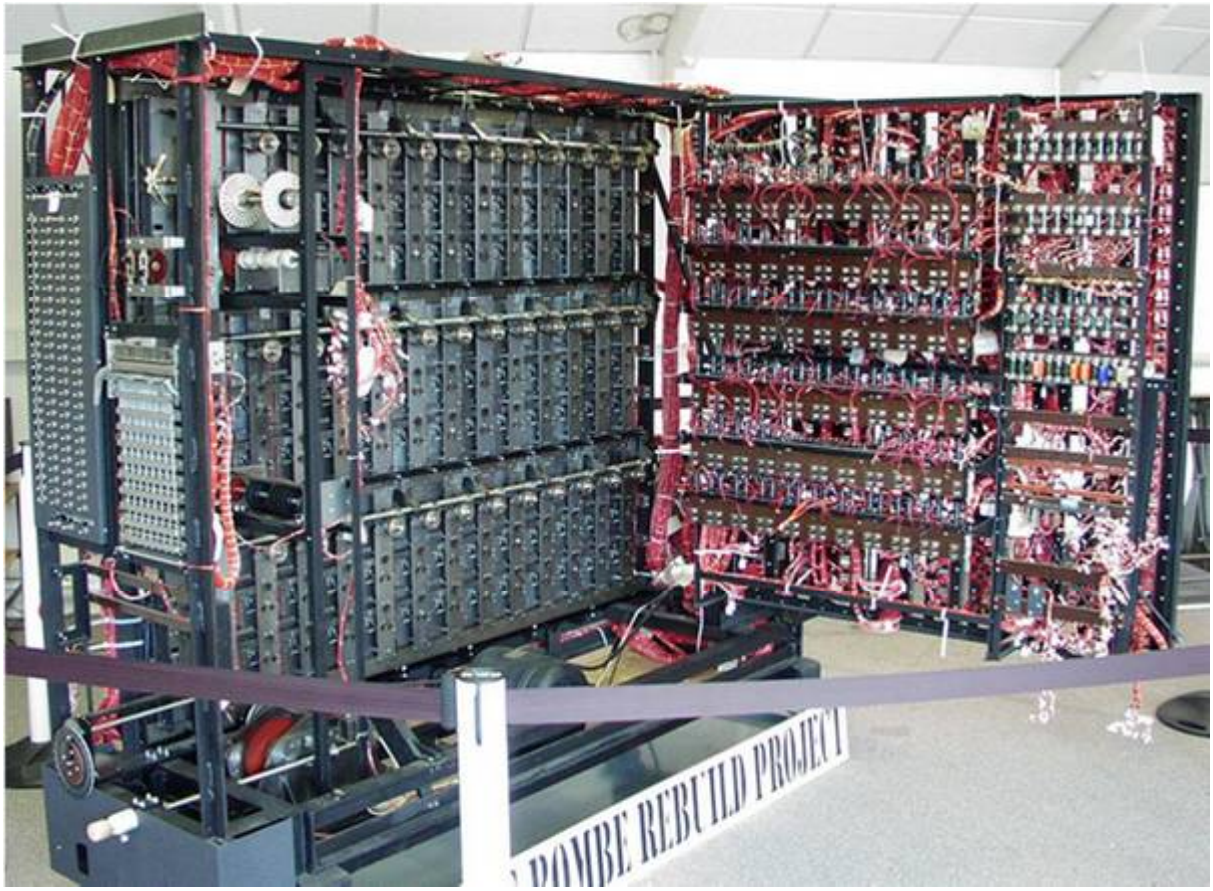
La spécification de cette bombe est le premier des cinq progrès majeurs dus à Turing pendant la durée de la guerre. Les autres sont :

- la procédure d'identification par déduction de la clef quotidienne des différents réseaux de la Kriegsmarine
- le développement d'une procédure statistique d'amélioration de l'efficacité des bombes
- le développement d'une procédure (« Turingerie ») de déduction des réglages des roues de la machine Lorenz SZ 40/42
- enfin, vers la fin de la guerre, le développement d'un brouilleur de radiophonie.

En utilisant certaines techniques statistiques en vue d'optimiser l'essai des différentes possibilités du processus de décryptage, Turing apporte une contribution innovatrice. Deux documents qu'il rédige alors (Rapport sur les applications de la probabilité à la cryptographie et Document sur la statistique des répétitions) ne seront déclassés et remis aux National Archives du Royaume-Uni qu'en avril 2012.

La « bombe de Turing ».

Quelques semaines à peine après son arrivée à Bletchley Park, Turing rédige les spécifications d'une machine électromécanique plus efficace que la bomba polonaise. La capacité de la bombe de Turing est doublée, grâce à un autre mathématicien de Cambridge, Gordon Welchman. Encore améliorée par un espoir de Cambridge, Richard Pendered, la bombe, une fois fabriquée par les ingénieurs de la British Tabulating Company, est l'outil fondamental le plus automatisé de l'attaque des messages chiffrés par Enigma.



réplique de la « bombe de Turing »

Au moyen d'un fragment probable de texte en clair, la bombe recherche les réglages corrects possibles utilisés pour 24 heures par chaque réseau allemand (ordre des rotors, réglages des rotors et enfichage du tableau de connexions). Pour chaque réglage possible des rotors, la bombe effectue électriquement une chaîne de déductions logiques fondées sur les mots probables.

À chaque occurrence d'une contradiction, la bombe écarte ce réglage et passe au suivant. La plupart des réglages essayés provoquent des contradictions, ils sont alors rejetés et ceux qui restent sont alors examinés de près.

Pendant presque toute la guerre, ce procédé permet de déchiffrer une grande partie des messages Enigma de la Luftwaffe dont les chiffreurs multiplient les négligences. Comme l'aviation coopère étroitement avec les deux autres armées (mer et terre), la GC&CS obtient des renseignements sur l'ensemble des activités de la Wehrmacht.
Mais l'interprétation des messages une fois déchiffrés pose souvent de tels problèmes à l'état-major qu'ils ne peuvent être qu'en partie exploités. Ce sera le cas du plan d'invasion de la Crète13.

La Hut 8 et l'Enigma navale.
Affecté à la Hut 8 (bâtiment préfabriqué N°8), Turing décide de traiter un problème autrement difficile, la cryptanalyse de l'Enigma navale : « parce que personne d'autre ne s'en occupait et que je pouvais l'avoir pour moi tout seul ». La même nuit, il conçoit le Banburismus, technique statistique séquentielle (plus tard appelée analyse séquentielle par Abraham Wald), dans l'espoir de percer l'Enigma navale : « Pourtant je n'étais pas sûr que cela marcherait en pratique. »

Dans cette idée, il invente une mesure de poids de la preuve qu'il baptise le Ban. Les Banburismes peuvent écarter certaines séquences des rotors Enigma, gain de temps important. Cependant, les chiffreurs de la Kriegsmarine, en particulier les sous-mariniers, appliquent sans faille toutes les consignes de sécurité. Les messages de l'Enigma navale ne sont décryptés que pendant les périodes couvertes par les manuels ou grâce aux feuilles de bigrammes capturés par les Alliés.

En novembre 1942, Turing se rend aux États-Unis pour travailler avec l'U.S. Navy sur l'Enigma navale et à la conception de bombes. Les bombes « à l'américaine » n'éveillent pas son enthousiasme. Pourtant, c'est l'extraordinaire puissance de travail combinée des centaines de bombes construites grâce aux moyens de l'industrie américaine qui, finalement, permet de percer à nouveau les secrets d'Enigma.

A partir de fin 1943, les sous-marins allemands auront été pour l'essentiel soit détruits, soit chassés de l'Atlantique-Nord par la puissance des marines de guerre alliées. En mars 1943, Turing revient à Bletchley Park. En son absence, son adjoint Hugh Alexander avait pris la fonction de directeur de la Hut 8. C'est Alexander qui avait de fait toujours dirigé le service. Turing devient consultant en cryptanalyse pour l'ensemble de la GC&CS.

À propos du rôle de Turing, Alexander dit : « On ne peut pas douter que les travaux de Turing déterminèrent notre succès. Au départ, il fut le seul cryptographe à penser que le problème valait d'être abordé et non seulement lui revient le mérite de l'essentiel du travail de la Hut 8, mais encore il partage avec Welchman et Keen le mérite de l'invention de la bombe. Il est difficile de dire que tel ou tel est absolument indispensable, mais si quelqu'un fut indispensable à la Hut 8, ce fut Turing. Le travail de pionnier tend toujours à être oublié quand après tout paraît plus facile, sous l'effet de l'expérience et de la routine ».

Travail sur les premiers ordinateurs.
En 1945, pendant son séjour à Ebermannstadt, les deux bombes atomiques américaines sont larguées sur le Japon et il n'en est pas surpris : il connaissait, depuis son voyage secret aux États-Unis de 1942-1943, l'existence du projet à Los Alamos.

De 1945 à 1947, il travaille au National Physical Laboratory, situé à Teddington au Royaume-Uni. Fin 1945, après avoir lu le rapport Von Neumann qui décrit la structure générale d'un ordinateur et discute des méthodes de programmation, **Turing rédige ce qui est sans doute le premier projet détaillé d'un ordinateur** : l'ACE (Automatic Computing Engine). Toutefois, il ne parvient pas à s'entendre avec les ingénieurs électroniciens du NPL chargés de construire cette machine, qui soulèvent des objections techniques et préfèrent commencer par un prototype plus modeste. Le projet rencontre d'ailleurs des obstacles bureaucratiques et budgétaires.

Turing, trop individualiste pour être un organisateur ou un grand négociateur, préfère partir en 1947 suivre des cours de biologie à Cambridge.

À la rentrée 1948 il est appelé par Max Newman, son ancien professeur de logique à Cambridge et collègue à Blechtley Park, à l'université de Manchester où Newman, inspiré lui aussi par le rapport Von Neumann, dirige le développement de l'un des tout premiers véritables ordinateurs : le **Manchester Mark I**, industrialisé ensuite par la firme Ferranti. Turing devient directeur adjoint du laboratoire de calcul de l'université de Manchester (titre sans grande signification) et travaille à la programmation de l'ordinateur.

Lors de la conférence marquant l'inauguration de l'ordinateur EDSAC, à Cambridge, il présente une méthode de preuve de correction de programmes fondée sur des assertions, qui préfigure la méthode connue sous le nom de « méthode de Floyd-Hoare ».

Vers l'intelligence artificielle : le test de Turing.

Turing continue parallèlement ses réflexions fondamentales réunissant la science et la philosophie. Dans l'article « Computing Machinery and Intelligence » (Mind, octobre 1950), Turing explore le problème de l'intelligence artificielle et propose une expérience maintenant connue sous le nom de test de Turing, où il tente de définir un standard permettant de qualifier une machine de « consciente ». Turing fait le pari « que d'ici cinquante ans, il n'y aura plus moyen de distinguer les réponses données par un homme ou un ordinateur, et ce sur n'importe quel sujet ».

En mai 1952, Turing écrit un programme de jeu d'échecs. Ne disposant pas d'un ordinateur assez puissant pour l'exécuter, il simule les calculs de la machine, mettant environ une demi-heure pour effectuer chaque coup. Une partie est enregistrée, où le programme perd contre un collègue de Turing.

Le programme « ELIZA » de Weizenbaum, écrit en 1966, qui ne prend que trois pages de langage SNOBOL, sera le premier à donner l'illusion pendant quelques minutes de satisfaire au test de Turing.

En 1952, Turing s'est intéressé à une autre branche des mathématiques, l'analyse, et à partir de l'équation de réaction-diffusion, a élaboré un modèle biomathématique de la morphogenèse, tant chez l'animal que chez le végétal. Il fait paraître un article où il propose trois modèles de formes (Turing patterns). Dans les années 1990, des expériences de chimie viendront confirmer expérimentalement les modèles théoriques de Turing.

Condamnation pour homosexualité.

Turing ne faisait aucun mystère de son orientation sexuelle. Au début des années 1950, après que l'Union soviétique a déclenché la guerre froide et mis au point sa bombe atomique, les services de contre-espionnage britanniques et américains sont traumatisés par plusieurs affaires de trahison dramatiques, où sont impliqués des intellectuels anglais homosexuels, souvent liés à Cambridge.

De leur point de vue, le « profil » de Turing le range parmi les personnes peu sûres. Le procès est médiatisé. Turing doit choisir entre incarcération ou castration chimique.

Il choisit le traitement. Alors qu'il avait été consacré, en 1951, en devenant membre de la Royal Society, à partir de 1952 il sera écarté des plus grands projets scientifiques.

Décès.
Suicide ou accident, en 1954, Turing meurt d'un empoisonnement au cyanure. L'enquête conclut au suicide.

Réhabilitation d'Alan Turing.
En 2009, une pétition, à l'initiative de l'informaticien John Graham-Cumming, est envoyée au Premier ministre Gordon Brown : « nous soussignés demandons au Premier ministre de s'excuser pour les poursuites engagées contre Turing qui ont abouti à sa mort prématurée ». En septembre 2009, celui-ci a présenté des regrets au nom du gouvernement britannique.

Cependant, le ministre de la justice Tom McNally exprime en février 2012 son refus de revenir sur la condamnation. Celle-ci, bien que paraissant aujourd'hui « cruelle et absurde », a été rendue en fonction des lois de son temps (« une grâce posthume n'a pas été jugée appropriée car Alan Turing a été justement reconnu coupable de ce qui était, à l'époque, une infraction pénale »).

En décembre 2012, un groupe de onze scientifiques britanniques, dont le physicien Stephen Hawking, appelle le gouvernement britannique à annuler sa condamnation, à titre posthume. Le 24 décembre 2013, la reine Élisabeth II, **sur proposition du secrétaire d'État à la Justice, Chris Grayling**, le grâcie en signant une prérogative royale de clémence. C'est la 4ème fois que le pardon royal est accordé depuis 1945. **Grayling** déclare que sa condamnation serait considérée aujourd'hui « comme injuste et discriminatoire » et **salue** « **son génie qui a contribué à sauver des milliers de vies** ».

Depuis 1966, le prix Turing (« Turing Award ») est annuellement décerné par l' »Association for Computing Machinery » à des personnes ayant apporté une contribution scientifique significative à la science de l'informatique. Cette récompense est souvent considérée comme l'équivalent du prix Nobel d'informatique.

En février 2011, au terme d'une vente aux enchères, des documents rédigés par Turing durant la Seconde Guerre mondiale sont acquis par le musée de Bletchley Park avec l'aide du « National Heritage Memorial Fund » afin d'éviter leur départ à l'étranger.

Sources Wikipédia
notes condensées et remises en forme par Gaby F5PSI
pour l'activité de TM60AT, en décembre 2014