

Chapitre 3

Des usages militaires à l'ère digitale

1. Introduction

Ce chapitre explore l'évolution fascinante des ordinateurs, depuis leurs débuts dédiés aux applications militaires et scientifiques jusqu'à leur transformation en un outil omniprésent, accessible à tous et au cœur de notre quotidien. L'informatique, initialement réservée aux besoins de calcul intensif pour des projets de recherche ou des applications militaires, s'est progressivement démocratisée. Elle est passée par l'ère des mainframes, des micro-ordinateurs et des ordinateurs personnels, jusqu'à devenir une technologie essentielle aussi bien pour les individus que pour les entreprises.

2. Des premiers ordinateurs aux machines de Turing

L'histoire des premières machines que l'on peut appeler « ordinateurs » est une fascinante progression de découvertes et d'innovations, chaque étape construisant sur la précédente pour nous amener progressivement vers l'informatique moderne. Pour les découvrir, partons de l'origine, des premières machines électromécaniques, jusqu'à l'apparition de l'ordinateur à transistor.

2.1 Les premiers calculateurs électromécaniques

Tout commence dans les années 1930 et 1940, à une époque où les scientifiques et les ingénieurs cherchent à automatiser les calculs. Le premier jalon de cette aventure est posé par Konrad Zuse, un ingénieur allemand, qui crée en 1941 le **Z3** : la toute première machine que l'on peut qualifier d'ordinateur électromécanique programmable. Le Z3 utilisait des relais électromécaniques pour effectuer des opérations arithmétiques. Bien que rudimentaire et relativement lent, il marquait un grand pas en avant : pour la première fois, une machine pouvait exécuter des instructions automatiquement, sans intervention humaine directe à chaque étape.



Figure 4-1 - Une reconstruction de 2010 de l'ordinateur Z3 par Horst Zuse
Auteur : Dksen sur German Wikipedia (image dans le domaine public)

Presque au même moment, aux États-Unis, une autre machine révolutionnaire voit le jour : le **Harvard Mark I**, construit en collaboration entre Howard Aiken et IBM en 1944. Cette machine électromécanique gigantesque, de plus de 15 mètres de long, était capable d'effectuer des calculs complexes, principalement pour des applications militaires pendant la Seconde Guerre mondiale. Bien qu'il fût encore basé sur des relais, le Mark I pouvait traiter des séries d'instructions de manière automatique et était capable de travailler pendant des heures sans intervention.

2.2 Alan Turing et ses bombes

Pendant la guerre, la cryptanalyse joua un rôle crucial, et l'une des figures clés de cette bataille était Alan Turing, mathématicien britannique dont les travaux ont été déterminants dans le décryptage des messages codés par la célèbre machine *Enigma* utilisée par les Allemands. À Bletchley Park, Turing a conçu une machine électromécanique appelée la **Bombe**. Ce dispositif permettait de tester rapidement des milliers de configurations possibles de la machine Enigma, accélérant ainsi considérablement le processus de décryptage. Grâce à l'ingéniosité de Turing et de ses collègues, les Alliés ont pu décoder des messages critiques, leur donnant un avantage stratégique.

2.3 L'arrivée des ordinateurs électroniques

Pendant la guerre, alors que Turing et ses Bombes jouaient un rôle déterminant dans le décryptage d'Enigma, une autre innovation majeure se préparait dans le domaine des ordinateurs. Les calculateurs électromécaniques, comme le Z3 et le Mark I, étaient lents en raison de la mécanique des relais. L'idée d'utiliser l'électronique pour accélérer les calculs se répandait également. Le besoin de vitesse, notamment pour des applications militaires comme la cryptanalyse, a conduit à l'invention du premier véritable ordinateur électronique, **Colossus**, développé en 1943 par une équipe britannique dirigée par Tommy Flowers. Le Colossus était utilisé pour déchiffrer les messages issus de la « machine de Lorenz », un système de cryptographie complexe utilisé par le haut commandement allemand.

Bien que gardé secret pendant de nombreuses années, il est désormais reconnu comme le premier ordinateur électronique programmable.

Cependant, Colossus avait une limitation : il était conçu pour une tâche spécifique, et non pour être un ordinateur polyvalent.

Le véritable tournant se produit avec l'**ENIAC** (*Electronic Numerical Integrator and Computer*), développé aux États-Unis en 1945 par John Presper Eckert et John Mauchly. L'ENIAC est souvent considéré comme le premier ordinateur électronique à usage général. Bien qu'il soit énorme et consomme une quantité d'énergie impressionnante, il pouvait exécuter des milliers d'opérations par seconde, une vitesse jamais atteinte à l'époque. Il a été utilisé pour des calculs scientifiques, comme la simulation de trajectoires balistiques et les recherches en énergie atomique. Cependant, programmer l'ENIAC restait compliqué : il fallait connecter manuellement des câbles pour modifier les calculs.

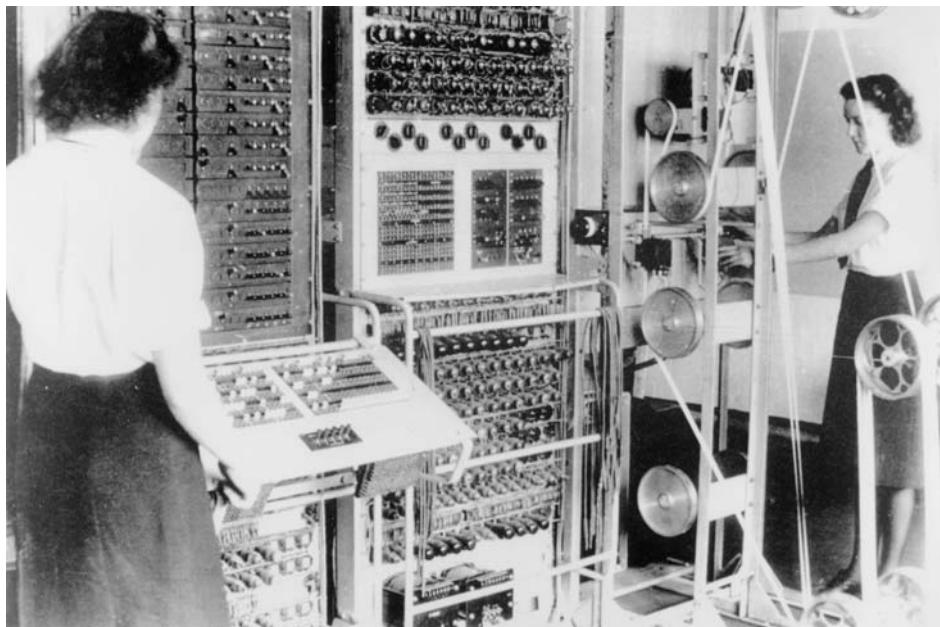


Figure 4-2 - L'ordinateur Colossus Mark II en 1944 (image dans le domaine public)

2.4 L'ère des programmes enregistrés

Les ordinateurs deviennent vraiment polyvalents avec l'introduction du concept de **programme enregistré**, où le programme à exécuter est stocké en mémoire, plutôt que câblé manuellement. C'est une idée théorisée par John von Neumann et mise en pratique avec des machines comme le **Manchester Baby** (ou SSEM - *Small-Scale Experimental Machine*) en 1948 et l'**EDSAC** (*Electronic Delay Storage Automatic Calculator*) en 1949. Ces machines utilisaient des tubes à vide pour stocker les instructions et les données en mémoire. Elles ont permis aux ordinateurs de devenir programmables, sans nécessiter une reconfiguration physique.

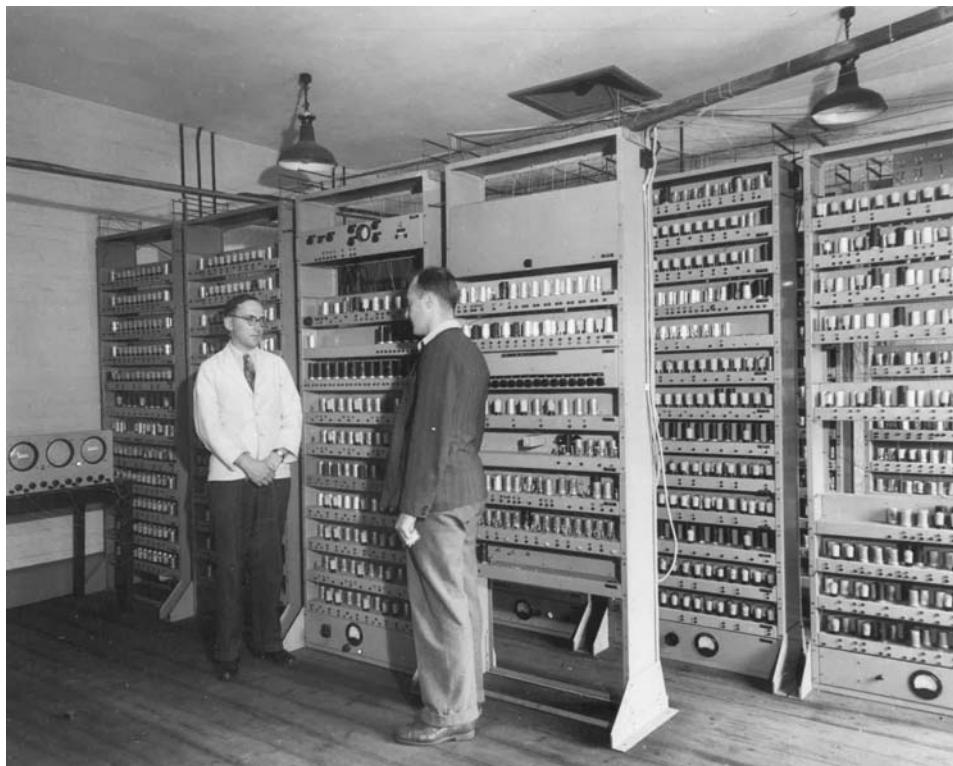


Figure 4-3 - L'ordinateur EDSAC en 1949. ©Computer Laboratory, University of Cambridge. / Wikimedia <https://creativecommons.org/licenses/by/2.0/deed.fr>

Le *Manchester Baby*, conçu par Freddie Williams et Tom Kilburn à l'université de Manchester, est considéré comme le premier ordinateur à programme enregistré au monde. Sa capacité à stocker des instructions en mémoire est une évolution qui a défini l'informatique moderne. Peu de temps après, l'EDSAC, développé par Maurice Wilkes à l'université de Cambridge, a suivi la même approche. Ces machines ont marqué le début de l'informatique telle que nous la connaissons aujourd'hui, où l'ordinateur peut exécuter n'importe quel programme à partir de la mémoire.

2.5 Le premier ordinateur commercial

La prochaine grande étape est franchie avec l'**UNIVAC I** (*Universal Automatic Computer*), conçu en 1951 par les mêmes inventeurs que l'ENIAC, Eckert et Mauchly. L'UNIVAC I est le premier ordinateur commercialisé aux entreprises et aux agences gouvernementales. C'est lui qui a prédit avec précision le résultat de l'élection présidentielle américaine de 1952, démontrant ainsi la puissance des ordinateurs pour des applications pratiques dans la société civile en traitant des données à grande échelle.



Figure 4-4 - L'ordinateur UNIVAC I en 1951

Auteur : U.S. Census Bureau employees (image dans le domaine public)

2.6 L'invention des transistors et la révolution informatique

Les ordinateurs à tubes à vide, bien que puissants, étaient énormes, consommaient beaucoup d'énergie et étaient sujets à des pannes fréquentes. Le transistor, beaucoup plus petit, plus rapide et plus fiable, a permis de créer des ordinateurs beaucoup plus compacts et plus performants.

Le premier ordinateur à utiliser des transistors fut le **TX-0**, conçu au MIT dans les années 1950. Ce prototype montrait qu'il était possible de remplacer les tubes à vide par des transistors pour construire des machines plus efficaces. Le TX-0 a ouvert la voie à une nouvelle génération d'ordinateurs beaucoup plus petits et plus rapides. Et ainsi commença l'ère moderne de l'informatique.

2.7 Reparlons un peu d'Alan Turing

Alan Turing est probablement la figure la plus emblématique de l'histoire de l'informatique, non pas pour ses bombes, bien qu'elles soient d'une grande importance historique, mais bel et bien parce qu'il est le père des **sciences informatiques**. Dans les années 1930, alors que les scientifiques cherchaient à comprendre les fondements du calcul et à répondre à des questions comme celle de savoir si tout problème mathématique pouvait être résolu par une méthode systématique, Turing apporta une réponse révolutionnaire. En 1936, il présenta dans un article son concept de **machine de Turing**, une idée simple mais visionnaire qui allait poser les fondements de l'informatique moderne.



Figure 4-5 - Alan Turing en 1948 - Mathématicien et cryptologue britannique (image dans le domaine public)

La machine de Turing est un modèle théorique, conçu pour décrire le fonctionnement abstrait d'un ordinateur capable de résoudre n'importe quel problème algorithmique. Elle fonctionne en lisant et en écrivant des symboles sur un ruban infini, en suivant une série d'instructions précises. Bien qu'il s'agisse d'une machine purement théorique, Turing montra qu'elle pouvait simuler n'importe quelle opération de calcul, jetant ainsi les bases théoriques de l'ordinateur moderne. L'importance de ce modèle pour les « sciences informatiques » est immense. En introduisant la conceptualisation d'une machine universelle capable d'exécuter n'importe quel programme, Turing posa les bases théoriques permettant de modéliser les capacités de l'ordinateur programmable. Sa théorie donna naissance à l'idée qu'une machine unique pouvait simuler n'importe quel calcul, une avancée fondamentale pour la compréhension des futurs ordinateurs. Cette vision théorique est devenue la colonne vertébrale de l'informatique moderne, influençant aussi bien les conceptions matérielles que les réflexions sur la complexité des algorithmes.

Ce modèle démontre également que certains problèmes, comme **le problème de l'arrêt**, ne pouvaient pas être résolus par un algorithme, ouvrant la voie à la définition et la compréhension de la notion essentielle de **calculabilité**. La notion de **calculabilité** désigne la capacité à résoudre un problème par un algorithme, c'est-à-dire une suite finie d'instructions. Un problème est dit « calculable » si une machine de Turing peut, en un nombre fini d'étapes, trouver une solution pour toute entrée donnée.

Cette notion permet de délimiter ce qui est possible ou non en termes de calcul automatique et s'avère donc capitale pour l'algorithmique. Avant Turing, il n'existait pas de cadre théorique pour déterminer quels problèmes pouvaient être résolus par des machines. Grâce à son modèle, Turing a donc démontré que certains problèmes ne peuvent pas être résolus par un algorithme, peu importe la machine ou le temps disponible. Cela a posé les bases de la théorie de la complexité et de l'étude des algorithmes, en fournissant des critères pour évaluer non seulement si un problème est solvable, mais aussi à quel coût en temps ou en espace, deux éléments centraux dans la théorie algorithmique moderne.

Le « problème de l'arrêt » pose la question suivante : peut-on concevoir un algorithme (ou une machine) qui, étant donné un programme informatique et une entrée quelconque, détermine de manière systématique si ce programme s'arrêtera un jour (c'est-à-dire s'il finira par donner un résultat) ou au contraire s'il continuera à tourner indéfiniment ? Turing a démontré que ce problème est **indécidable**, c'est-à-dire qu'il n'existe pas d'algorithme général capable de résoudre ce problème pour tous les programmes et toutes les entrées possibles. Pour arriver à cette conclusion, il a utilisé un raisonnement par l'absurde. Il a montré que si un tel algorithme d'arrêt existait, il conduirait à une contradiction logique en l'appliquant à lui-même. La démonstration de l'indécidabilité du problème de l'arrêt a des conséquences profondes en informatique théorique. Elle marque une **limite fondamentale** de ce que les ordinateurs peuvent faire : il existe des problèmes pour lesquels aucun algorithme ne peut fournir de solution, même avec un temps et des ressources illimités. Cela a ouvert la voie aux recherches sur d'autres problèmes indécidables sur la théorie de la complexité.