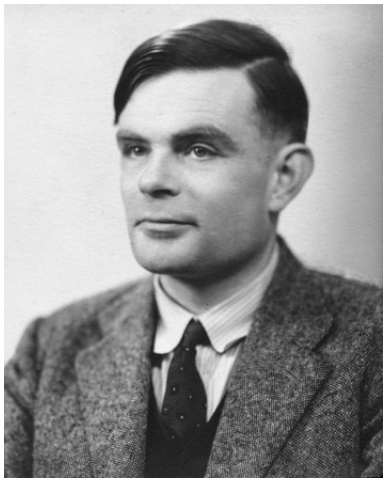
https://www.amessi.org/alan-turing-un-genie-des-maths-au-service-du-dechiffrement

Alan Turing, un génie des maths au service du déchiffrement

- CHERCHEURS-SAVANTS-DECOUVERTES
- Alan TURING
-



Date de mise en ligne : mercredi 8 janvier 2014

Alors qu'une brillante carrière attendait Alan Turing à Princeton, aux Etats-Unis, aux côtés d'un autre pionnier de l'informatique, John von Neumann, il préfère rentrer en 1938 à Cambridge, où il est recruté par les services du renseignement. Avec près de 200 autres « grosses têtes » du pays, il va s'attaquer au déchiffrement des messages échangés par l'armée allemande. Celle-ci dispose en effet d'une machine de chiffrement très efficace réputée inviolable, Enigma.

Sommaire

Une manière simple de coder un message est de substituer les lettres de l'alphabet en les décalant : A devient C, B devient D, C devient E... Pour être encore plus efficace, il est possible de changer la règle de décalage à chaque lettre. C'est à peu près l'idée d'Enigma, qui mécanise et simplifie la procédure à l'écriture et à la lecture. Elle se présente comme une machine à écrire avec deux claviers, l'un sur lequel on tape le message en clair et l'autre dont les lettres s'allument, indiquant leur traduction codée. Dans l'esprit, les techniques de chiffrement dites symétriques, encore utilisées aujourd'hui pour, par exemple, crypter un document, appartiennent à cette famille de codes.

En réalité, ce sont les Polonais qui cassent les premiers les secrets de cette technique, juste avant l'invasion de leur pays en 1939. Mais les messages sont trop nombreux et les Allemands raffinent leur technique. Turing invente donc une autre méthode pour venir à bout des messages codés. Il bénéficie aussi de moyens supplémentaires appelés « bombes » pour tester très rapidement des milliers de combinaisons.

NOUVELLE MÉTHODE

L'équipe polonaise recourait aux premières lettres des messages pour trouver les clés de décryptage. Turing préfère utiliser des notions de probabilités afin de repérer dans la totalité des textes des occurrences plus probables (comme les mots désignant la météo ou des positions) afin de réduire les possibilités.

Son rôle ne sera dévoilé que bien après la guerre, pour des raisons de sécurité. Malgré son succès, on ne peut faire de Turing un pionnier du chiffrement comme il l'est en informatique ou en intelligence artificielle, car cette activité était déjà florissante avant lui : César a laissé son nom à une de ces techniques. En revanche, il illustre ce qui fait le sel de ce métier : analyse des messages, recherche de failles ou de régularités, mise en oeuvre de stratégies opérationnelles.

Ses travaux laissent aussi des traces dans deux autres branches du chiffrement. Les méthodes dites asymétriques, utilisées par exemple pour garantir les transactions électroniques, ont une sécurité qui repose sur des processus mathématiques calculables, mais en des temps très longs et en pratique rédhibitoires. Analyser la complexité de ces méthodes est donc toujours d'actualité afin que la robustesse de ces techniques ne s'effondre pas sous le coup de nouveaux algorithmes.

Dans la même veine, les cryptologues élaborent des preuves de sécurité, c'est-à-dire des démonstrations mathématiques permettant de garantir la fiabilité d'une procédure. C'est alors le modèle de calcul de la machine de Turing qui sert de fondement théorique à l'élaboration de ces preuves.

David Larousserie - LeMonde.fr
Voir aussi : http://en.wikipedia.org/wiki/Alan_Turing