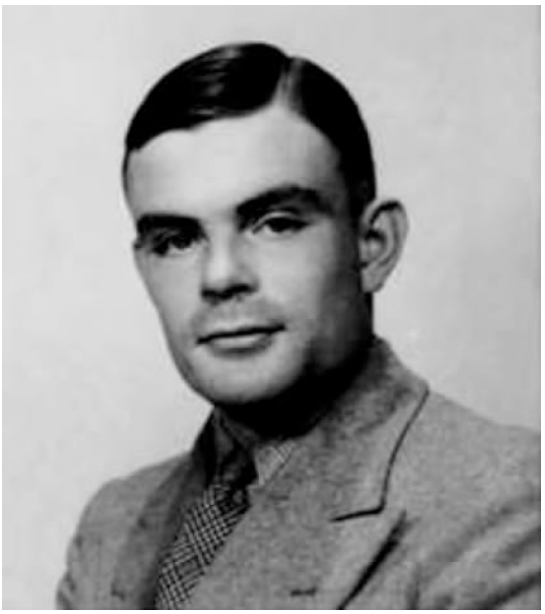
Dossier "Cryptologie : l'art des codes secrets"
par Philippe GUILLOT

9. Cryptologie et informatique

La cryptologie et l'informatique ont connu un développement à partir du second conflit mondial. La théorie de l'information crée par Claude Shannon, qui a conduit à la numérisation de pans technologiques entiers, est née de la question de savoir ce que pouvait apprendre un adversaire qui observe une communication chiffrée.

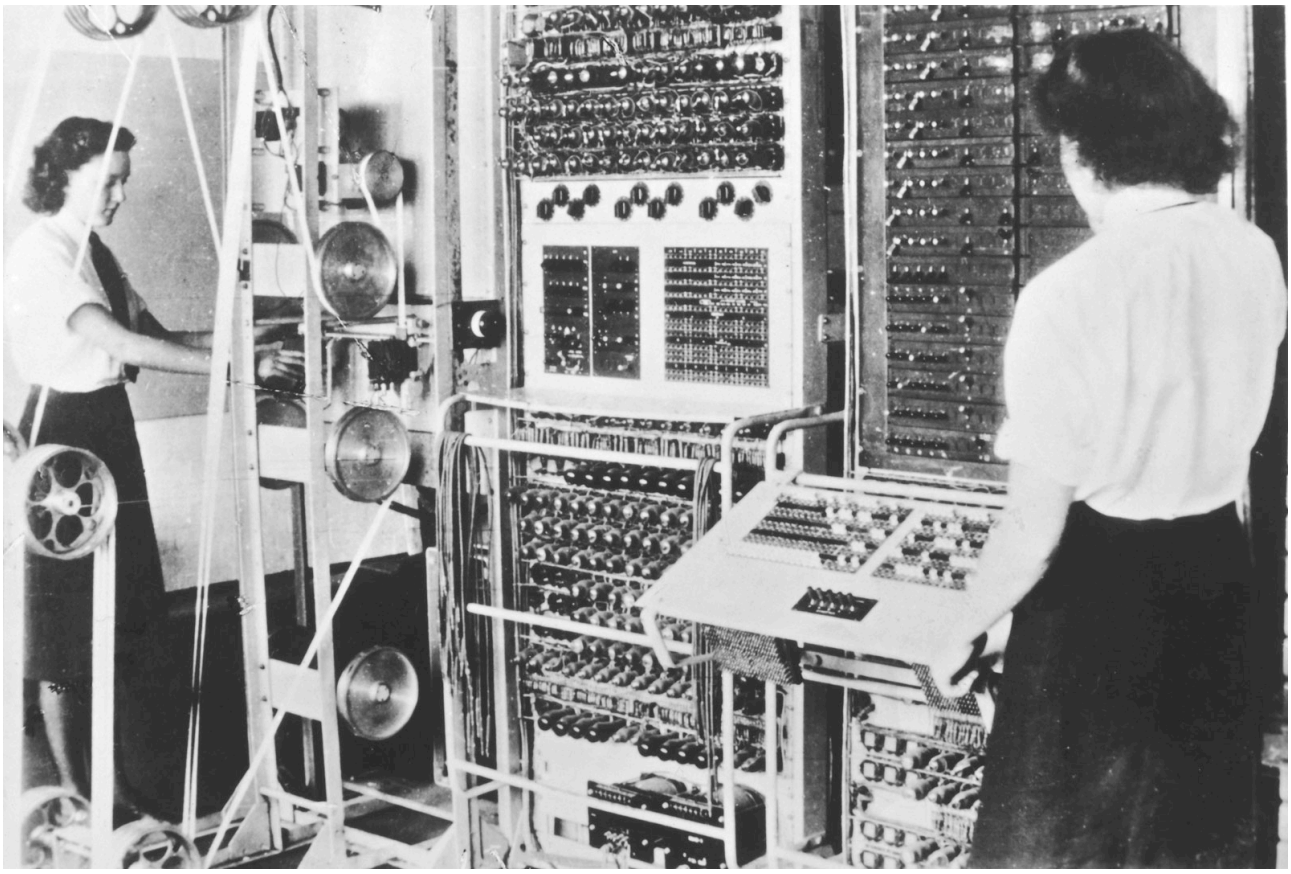
Le mathématicien Alan Turing, connu pour avoir modélisé la notion de calculabilité avec la machine qui porte son nom, a eu un rôle crucial au sein de l'équipe de Bletcheley Park, chargée du décryptement des messages allemand.



Aalan Turing. http://www.criticalgamer.co.uk/2009/09/19/thank-you-alan-turing/

La recherche des clés devenait une tâche trop complexe pour être réalisée à la main, et il a fallu construire des machines de plus en plus puissantes pour tester les innombrables combinaisons de clés possibles. Les techniques mises en œuvre pour réaliser ces calculs ont contribué de manière cruciale au développement des premiers ordinateurs. L'ingénieur en téléphone Tommy H. Flowers a eu l'idée d'employer des tubes à vide, récemment utilisés pour la commutation téléphonique, pour construire un immense calculateur, le Colossus, destiné au décryptement du téléscripteur chiffrant allemand.

Tommy Flowers. http://www.kpbs.org/photos/2012/nov/19/20422/



Le calculateur COLOSSUS

http://www.thehistoryblog.com/wp-content/uploads/2012/11/Codebreaking-machine-Colossus-at-Bletchley-Park.jpg

Les progrès réalisés par les moyens de calcul suivent une loi empirique, appelée *Loi de Moore*, du nom du directeur de recherche de l'entreprise américaine de circuits intégrés *Fairchild* qui l'a énoncé la première fois en 1965. Cette loi énonce que la puissance des calculateurs électroniques double tous les dix-huit mois. Elle a été étonnamment vérifiée jusqu'à aujourd'hui.

Alors qu'il a fallu plus de 70 heures à l'ordinateur ENIAC pour calculer deux mille décimales du nombre π en 1949, le moindre calculateur embarqué dans un téléphone portable réalise aujourd'hui ce calcul en une fraction de seconde. En 1977, la revue *Scientific American* a présenté le RSA sous le titre *Un nouveau système qu'on mettrait des millions d'années à casser*. Pourtant, la clé publique qu'il contenant a été factorisée en 1994, bien avant les millions d'années annoncés.

Cet incroyable et constant progrès rend envisageable l'application de la force brutale pour chercher la clé d'un procédé dans des ensembles de plus en plus grands. Pourtant, c'est au chiffreur, et non au décrypteur que bénéficie les progrès des moyens de calcul.

Supposons qu'à un moment donné, on utilise des nombres de 200 chiffres comme module RSA. Si la puissance de calcul double, la taille du module pourra être portée à 250 chiffres sans que l'utilisateur ne constate le moindre changement dans la rapidité du calcul. Mais le travail de l'adversaire pour factoriser ce nouveau module suit une loi donnée par la formule $c(n) = \exp(k (\ln n)^{1/3} (\ln \ln n)^{2/3})$ pour un nombre de n chiffres. Ce travail devra donc être multiplié par 36. Avec sa puissance de calcul qui n'aura que doublé, il aura perdu un facteur 18 dans l'affaire.

Plus les machines sont puissantes, et plus la dissymétrie entre le chiffrement et l'attaque donne un avantage au chiffrement.