Les dates clés
2500 ans de secrets bien (ou mal) gardés

La cryptologie remonte aussi loin que des sociétés organisées ont eu besoin de conserver secrètes un certain nombre d'informations. L'histoire est riche d'inventions toutes aussi originales les unes que les autres. Jusqu'à l'arrivée de l'informatique qui a tout changé.

V^e siècle av JC
Scytale lacédémonienne : ruban de papyrus qui nécessitait d'être enroulé autour d'une baguette de bois de diamètre connu pour être lue.

Rome (I^er siècle av JC)
Code de César : système cryptographique pour coder les messages militaires par décalage alphabétique de chaque lettre.

IX^e siècle
al Kindi, savant et philosophe arabe. Il rédige le premier manuscrit connu sur la cryptologie.

XV^e siècle
Cadran d'Alberti : système à base de disques concentriques.

XVI^e siècle
Grille de Cardan : système à base de quadrillages.

1863
Friedrich Kasiski, officier prussien, étudie dans son ouvrage *Les Chiffres et l'art du décryptement* la statistique des fréquences des caractères d'un texte dans une langue particulière. Il définit et introduit un invariant, appelé « indice de coïncidence », qui facilite les attaques.

1883
Auguste Kerckhoffs, linguiste et cryptologue flamand**,** énonce, dans son essai *La cryptographie militaire*, un certain nombre de principes fondamentaux pour le chiffrement, avec notamment le fait que le mécanisme de chiffrement doit *« pouvoir tomber sans inconvénient entre les mains de l'ennemi ».*

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

1919
Deux brevets sont déposés pour les premières machines « chiffrantes » : **Enigma** qui équipera l'armée allemande, puis **Hagelin** adoptée par les alliés.

1930
Kurt Gödel et Alan Turing, travaux sur les limites de la pensée mathématique, menant à « l'impossibilité concrète », c'est-à-dire à l'existence d'énoncés qui ne peuvent être ni prouvés, ni réfutés.

1938
Entrée d'Alan Turing, mathématicien britannique, au GE&CS (Government Code and Cypher School).

1940
Turing « casse » les codes de l'armée allemande.

1945
Premiers ordinateurs.

1976
Naissance de la cryptologie asymétrique. Whitfield Diffie et Martin Hellman, dans un article intitulé *New Directions in Cryptography*, rendent le processus de chiffrement entièrement public, y compris la clé spécifique au destinataire alors appelée clé publique. Seule la clé de déchiffrement doit rester secrète. Le concept de cryptographie à clé publique était inventé.

1978
RSA : Premier mécanisme de chiffrement asymétrique par Ronald Rivest, Adi Shamir et Leonard Adleman.

1981
Première conférence académique de cryptologie « Crypto » qui se tient depuis, chaque année, à Santa Barbara en Californie.