The Codebreakers

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 9 juin 1997

https://www.bortzmeyer.org/codebreakers.html

Auteur(s) : David Kahn
ISBN n°0-684-83130-9
Éditeur : Scribner
Publié en 1967

Le chef d'œuvre sur l'histoire de la cryptographie, paru en 1967, était épuisé depuis longtemps. Il a été réédité il y a peu. Le contenu n'a pratiquement pas changé, malgré le bandeau de couverture qui parle désormais de l'Internet :-(

Non seulement les derniers développements manquent mais des évènements anciens, mais couverts par le secret à l'époque de la première édition, comme l'histoire de Bletchley Park, ne sont pas traités. (Ce centre de décryptage de l'armée britannique de la Seconde Guerre mondiale est resté secret jusqu'à très récemment. Voir le livre presque homonyme "*Code breakers*".) Seul un mince dernier chapitre essaie de mettre le livre à jour.

Mais en revanche, ce livre reste une présentation inégalée de tous les aspects de la cryptographie, depuis l'Antiquité jusqu'à la Seconde Guerre mondiale. Relativement peu technique, lisible sans génie mathématique, ce livre très épais (1100 pages) détaille de nombreux exploits cryptographiques et cryptanalytiques. Une telle somme ne s'écrit pas en un jour et on attend le livre équivalent pour la cryptographie à l'ère de l'informatique, relisant les récits des temps où des militaires à moustache alignaient des chiffres sur du papier, où des professeurs d'université allemands tentaient de déchiffrer le persan antique, où les princes florentins embauchaient des abbés érudits pour communiquer secrètement. Franchement, est-ce que utiliser PGP ou SSH provoque le même frisson ? :-)