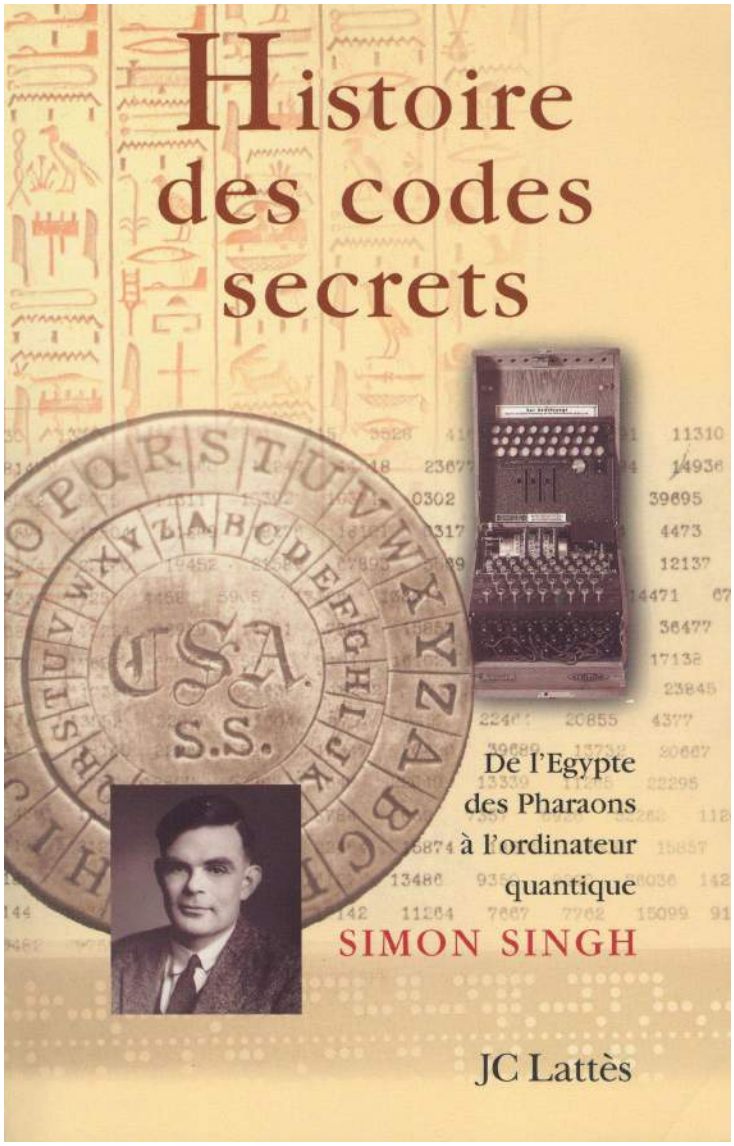
Histoire des codes secrets

Auteur : Simon Singh.
Editions Jean-Claude Lattès
Copyright 1990
430 pages.
Voici la bible de l'historien en cryptologie, illustrée de nombreux dessins, exemples et photos.
A la fin du livre est organisé un concours de décryptement avec des exercices progressifs.



Histoire des codes secrets

De tous temps, les codes secrets ont décidé du sort des hommes, des peuples et des nations. Grâce à eux, les militaires ont pu mener leurs guerres dans l'ombre, les puissants et les bandits protéger leurs trésors, les amants camoufler leur passion. Les codes sauvèrent ainsi les Grecs des Perses, accompagnèrent César dans ses conquêtes, firent arrêter et décapiter Marie Stuart, scellèrent l'énigme du Masque de fer, décidèrent Wilson à rejoindre les alliés, et permirent d'épargner des milliers de vies pendant la Seconde Guerre mondiale.

Simon Singh, avec la clarté et le sens du récit historique qui ont fait le succès du *Dernier Théorème de Fermat*, retrace la lutte permanente, au cours des âges, entre ceux qui élaborent les codes et ceux qui cherchent à les briser. Une histoire qui court des origines à aujourd'hui, des stratagèmes de la communication pendant l'Antiquité à la confidentialité sur Internet au XXIe siècle. Une histoire qui met en scène des personnages et des scientifiques souvent inconnus – secret oblige –, mathématiciens, physiciens, linguistes mais aussi joueurs d'échecs, de bridge, ou encore cruciverbistes, tous hors du commun.

A la croisée du jeu et de la guerre, de l'histoire et de la science, de l'espionnage et de l'informatique, une fantastique page de l'esprit humain, enfin révélée.

Simon Singh est docteur en physique nucléaire. Il a travaillé au laboratoire du CERN à Genève et est l'auteur du Dernier Théorème de Fermat.

En fin d'ouvrage, un jeu concours : Simon Singh offre 10 000 livres sterling (environ 100 000 FF) au lecteur qui réussira à briser une série de codes secrets.

9 782709 620482

00339 → 22 €72
149,00 FF

149,00 F TTC
99.10.45.2985.5
ISBN : 2-7096-2048-0
Documents droits réservés
Maquette : Didier Thimonier

Sommaire

Introduction 11
1 Le chiffre de Marie, reine d'Écosse 17
2 Le chiffre indéchiffrable 61
3 La mécanisation du codage 115
4 À l'attaque d'Enigma 159
5 La barrière de la langue 209
6 Alice et Bernard s'affichent en public 265
7 Pretty Good Privacy 319
8 Saut quantique dans le futur 345

Concours 379
Annexes 396
Glossaire 411
Remerciements 415
Éléments de bibliographie 418
Crédits photographiques 423
Index 424

ARCSI - Association des Réservistes du Chiffre et de la Sécurité de l'Information
Association régie par la loi de 1901 - N° SIRET : 511 069 569 00016
Tous droits de propriété intellectuelle réservés à l'ARCSI, association loi 1901, selon les règles du droit français