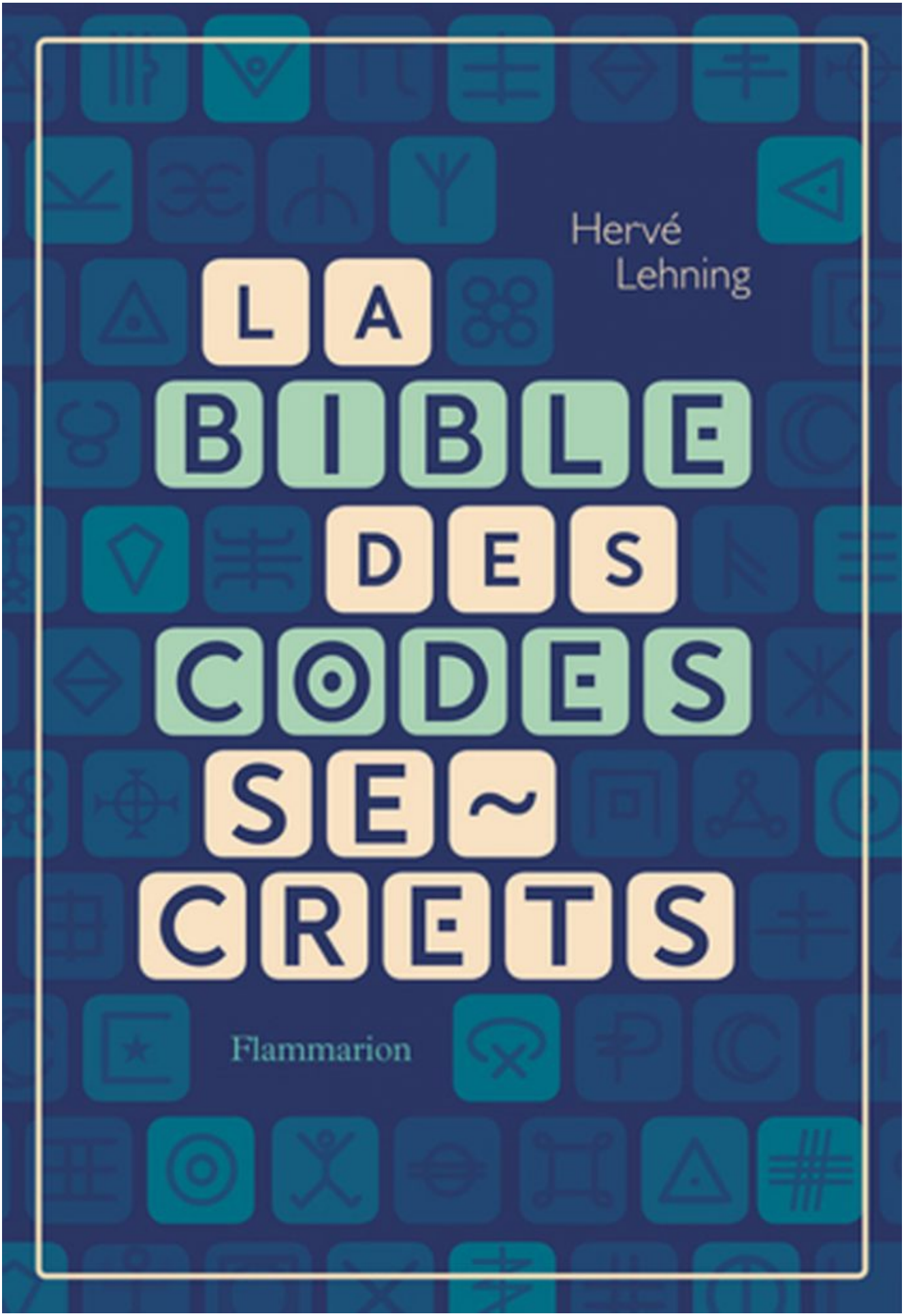
Hervé
Lehning
LA
BIBLE
DES
CODES
SE~
CRETS
Flammarion

La Bible des codes secrets

L’art de coder des messages, diplomatiques, militaires ou commerciaux, repose sur une clef (mot, phrase ou nombre), à changer périodiquement, et non sur le secret des méthodes ou des algorithmes.

Ce livre, rédigé par un mathématicien, expose en détail une centaine de codes ou « chiffres » dans leur contexte historique. Le codage et son décryptage sont allés de pair avec le renseignement. Jusqu’à la première guerre mondiale, des générations de généraux ont cru leurs codes inviolables, en raison de leur complexité toujours accrue. Or l’espionnage, les interceptions ou les hasards de la guerre peuvent révéler l’algorithme utilisé. Comme la science, le décryptement progresse de façon inductive, à savoir du particulier au général, la méthode déductive ne servant qu’à contrôler le sens du message final. Ainsi en 1822, le Français Jean-François Champollion (1790-1832) parvient à décrypter les hiéroglyphes égyptiens grâce à la pierre de Rosette, où figuraient des versions en grec et égyptien démotique. Suite à la création du service des postes en France au XVème siècle, le « Cabinet noir » décachète les lettres, pour vérifier qu’elles ne contiennent rien d’outrageant envers le roi, les déchiffre éventuellement et les recachète. Son fondateur, le mathématicien Antoine Rossignol (1600-1682), inspire le « Grand Chiffre » de Louis XIV, qui résistera trois siècles aux assauts des décrypteurs. La dissolution du Cabinet noir par la Révolution contribue à la perte de l’expertise française en cryptographie. Les armées révolutionnaires puis impériales en subissent les conséquences. Les Britanniques emploient des éclaireurs francophones et hispanophones, chargés de guider l’armée, de porter les messages, d’intercepter ceux de l’ennemi et de les décrypter. De leur côté, les services de renseignement russes interceptent et décryptent l’essentiel des dépêches de Napoléon. La bataille la plus meurtrière de la guerre de Sécession se déroule à Shiloh en 1862 avec une offensive surprise des troupes sudistes, qui avaient chiffré leur plan d’attaque…avec le code de Jules César lors de la conquête de la Gaule (58-51 avant JC). En 1914, le croiseur allemand *Magdeburg*, chargé de poser des mines en mer Baltique, s’échoue sur l’île d’Oldensholm. Il est pris à partie par deux croiseurs russes, qui récupèrent les livres de codes de la Marine allemande et les transmettent à l‘Amirauté britannique, qui les décrypte. Les Allemands ne changent leur code qu’en 1916 après la bataille du Jutland. En 1917, les Britanniques interceptent un télégramme chiffré entre l’ambassadeur

d’Allemagne aux Etats-Unis et l’ambassade d’Allemagne au Mexique, via la société internationale de télécommunications Western Union. Cette dépêche, dite « Zimmermann » du nom du ministre allemand des Affaires étrangères et dont le code avait été « cassé » par les Britanniques, annonce une guerre sous-marine totale. Elle propose aussi au Mexique une alliance avec l’Allemagne pour recouvrer le Texas, le Nouveau-Mexique et l’Arizona, annexés par les Etats-Unis en 1845. Ce télégramme va contribuer à l’entrée des Etats-Unis dans la première guerre mondiale. Lors de la seconde, le déchiffrement de la machine de cryptage automatique « Enigma » des forces armées allemandes sera réalisé par les services britanniques (10.000 personnes !), l’espionnage français et trois mathématiciens polonais…grâce à la trahison d’un chiffreur allemand !

Loïc Salmon

« La bible des codes secrets », Hervé Lehning. Editions Flammarion, 464 pages, 25 €.

Les écoutes de la victoire

Renseignement : opérations alliées et ennemies pendant la première guerre mondiale

DRM : des moyens de haute technologie pour le recueil de renseignements