Chapter G

Some cryptographers

Publishing results is a major goal of active researchers in most sciences. Not so in cryptography: some of the top work remains secret, at least for a while. We now describe some of the contributors to cryptography BDH (before Diffie & Hellman). Others have played a role in this text before, among them Caesar, Augustus, Vigenère, Alberti, Porta, Vernam, Shannon, Kasiski, Babbage, Friedman, Viète, Bacon, and Cardano, in order of appearance.

G.1. Arab cryptology

The Arab civilization was the first to produce systematic approaches to cryptology and codify them in books. Around the time that the long drawn-out demise of the Roman empire came to an end—with a whimper, not a bang—there arose from the Arab peninsula a new world power. محمد (Mohammed, 570–632) was a businessman from Mecca. Starting in 610, he put together the Holy Qurān and the monotheistic religion of Islam, borrowing heavily from the Judaic and Christian writings. Muslim doctrine views this holy book as the words of God. He was forced to flee from Mecca to Medina in 622, the Hijrah, and enthusiastically welcomed in his new hometown. In spite of substantial initial resistance, mainly in Mecca, the new religion fired up enormous energies, and within a century its followers had conquered half of the “known”
world: the Arab peninsula, Palestine, Egypt, North Africa, Spain, and Mesopotamia. One of his successors, Caliph al-mamūn (reigned 813–833), built his capital Baghdad into a magnificent city. Besides the military and architectural successes, he also created an intellectual center, the Bait al-Hikmah (House of Wisdom). It housed the world’s leading scientists. One of their important tasks was the acquisition, translation, and study of the Greek and Roman scientific texts. Without these successful efforts, the mathematical works of Pythagoras, Diophant, Euclid, and many others might well have gotten lost in the ensuing Dark Ages of Europe, where religious fundamentalism discouraged free thinking and independent research.

From the start, Arabic as the language of the Qurān was studied, and grammars and secretarial handbooks were produced. And we own the first systematic writings about cryptography to this period. Al-Kindī (al-Kindī, 801–873), wrote the oldest surviving treatise on cryptography, including cryptanalytic techniques and the necessary statistical methods.

Al-Kindī was versed in many fields, including philosophy, medicine,