DOCID: 3075766

(U) CRYPTOLOGIC ALMANAC

(U) THE PRE-PRE-MODERN ERA

(U) Many historians date the modern era in cryptology from the sixteenth century, when the first book was published in Europe on the subject -- *Polygraphiæ*, by the German monk Trithemius, in 1518. This important book, as we might imagine, was preceded by considerable experimentation and much unpublished writing in Europe.

(U) The need to protect messages goes as far back as messages themselves and, indeed, transcends cultures. Although ancient communicators lacked the tools born from the mathematical and linguistic knowledge that increasingly accumulated during the Renaissance, they did have available a variety of methods to protect their messages.

(U) Many gaps exist in our knowledge of ancient cryptology, but much is available. This article will discuss briefly the development of cryptology before Trithemius.

(U) Cryptography is the art or science of protecting one's own messages by scrambling or substituting components of the text, i.e., letters, syllables, words, or phrases. In some early periods and in locations, before general literacy, any writing system served to keep messages secure -- even plain language was unintelligible to the illiterate. Cryptography, however, presupposes a literate person or group able to pry into a neighbor's communications; it requires measures beyond simple plaintext.

(U) What today's communicators might call TRANSEC, transmission security, i.e., hiding messages, was a principal practice. A loyal soldier would repeat a verbal message, presumably only to the intended recipient, or hide a written message about his person. Stories abound from the Greeks about hiding messages in the sole of a sandal, rolled onto women's earrings, or stuck in the belly of a hare served to King Cyrus of Persia.

(U) The oddest story of concealment is the tale that the order for a Greek island to revolt against the Persians in 500 B.C.E. was tattooed on the shaved head of a slave. Once his hair had regrown, he was dispatched with the message. If true, this obviously was not a time-sensitive revolt. (Lambros Callimahos, NSA's great teacher of cryptology, also suggested a refinement of this method: behead the messenger upon arrival, making him a "one-time slave!")

(U) The ancient Greeks and Romans used light to send messages, usually torches at night or smoke signals by day. There are some reports of Greeks sending flashes using burnished shields in the sun, but it is unclear whether this was a fully developed communications method. Apparently, the communicants used a kind of open code, that is, light or smoke combinations with pre-arranged

Approved for Release by NSA on 12-26-2006 pursuant to E.O. 12958, as amended MDR 51971

meanings, secure but restricted to a limited number of messages. This kind of signaling, of course, was dependent on the cooperation of natural phenomena.

(U) David Kahn, in *The Codebreakers*, notes that cryptographic systems -- or proto-cryptographic systems -- were developed in many places in the ancient world, including Egypt and Persia. However, many of them really were "shorthand" writing methods, and none seemed to have survived the original time and place of usage.

(U) Some ancient Greeks developed a system for using dots to substitute for consonants in messages, and may even have used a cipher disk. One ancient writer referred to a system of converting letters to numbers by use of a 5x5 matrix, a system that would have been recognized by 20th century cryptologists.

(U) The first cipher machine was in all likelihood the "scytale," a wooden staff used by Spartan generals, possibly as early as 900 B.C.E. This machine required two pieces of wood of equal length and thickness. A cloth was wound around the stick, starting at a peg on the top, leaving no space exposed on the wood. The general, or his scribe, would write the message on the cloth horizontally down the stick. When the cloth was unwound, the words and letters were no longer connected, but looked like random jottings. In theory, with this transposition cipher, the message could not be read until the cloth was rewound on the original scytale or its twin. (Some historians, by the way, believe the scytale was the ancestor of the modern officers' swagger stick.)

(U) From his own writings, we know Julius Caesar used both TRANSEC and alternate writing systems. On occasion he would send messages to and from Gaul written in Greek characters, presuming that Gallic tribes couldn't read that language. On at least one occasion, he had a message tied to a lance and thrown into a camp under siege, letting his compatriots know that help was coming.

(U) In addition, a simple alphabetic substitution cipher bears Julius Caesar's name. It is not clear whether the first Caesar actually used this eponymous system, but it is known that his nephew, the first Emperor, Augustus, sent messages in substitution systems.

(U) The range of cryptographic options and cryptanalytic techniques available in the ancient Mediterranean world remains unknown, however. No individual encrypted messages have come down to us, and there were no books on theory written (or, at least, preserved).

(U) Some early figures in pre-modern Europe, including Charlemagne and Alfred the Great, used alternate alphabets to disguise their writing. Cipher systems as we now know them began to emerge in the 14th century. The Italian city-states and the Vatican were pioneers in developing new systems -- and how to solve them! This coincided with the birth of the modern European diplomatic system, which heightened the need to protect communications.

(U) But it is important to remember that cryptology was not limited to Western culture. In fact,

the apogee of cryptologic development occurred in the House of Islam.

(U) The government of the Caliph in the ninth and tenth centuries (Western reckoning used here for consistency) employed both cryptography and cryptanalysis for administrative communications and for protection of some records. Some Islamic sects that might have been considered heretical by the mainstream apparently also developed cryptography for their own protection.

(U) Conversant with ancient writings on mathematics, such as the books of Euclid, and their own research, Arab scholars came to a deep understanding of mathematics, including mathematical cryptography. In that same period, in addition to the writings of ancient Greece, Arab scholars drew on other eastern Mediterranean countries and the states of India for knowledge of many other subjects, including philosophy, several branches of science, and medicine. In reconstructing texts or encountering unknown languages, scholars also developed a linguistic approach to cryptology.

(U) Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn 'omran ibn Ismail al-Kindi is considered by many the greatest mathematical cryptologist of his time. His book *A Manuscript on Deciphering Cryptographic Messages* is the oldest extant text on the subject in the world, written in the late ninth century. Al-Kindi served several caliphs successfully, but ran afoul of one near the end of his life and was beaten, then dismissed from service. He died in Baghdad in 873 C.E.

(U) Many mathematical concepts that are now integral parts of Western learning, including the decimal system of numerals, algebra, and statistics, were preserved in the House of Islam; this knowledge was transferred from the Caliphate to European scholars in the early modern period.

(U) Among the useful concepts in this early technical transfer was the concept of "zero." Or, as it is in Arabic, "empty," or sifr.

Yes, the concept and word "cipher" itself entered English from Arabic.

NOTE: (U) The National Cryptologic Museum has a first edition of the Trithemius work on cryptology in its display of rare books. The first edition is on loan from historian David Kahn.

SOURCES: *The Friedman Legacy* (Center for Cryptologic History, 1992).

Ibraham A. Al-Kadi, "Origins of Cryptology: the Arab Contributions," *CRYPTOLOGIA*, April 1992.

David Kahn, *The Codebreakers*.

Albert C. Leighton, "Secret Communication among the Greeks and Romans," *Technology and Culture*, Vol. 10, 1969.

[(U//~~FOUO~~) David A. Hatch, Center for Cryptologic History, 972-2893s, dahatch@nsa]

UNCLASSIFIED//FOR OFFICIAL USE ONLY