499BCE  Histaieius of Miletus shaves the head of a
messenger to write his message to Aristagoras
concerning a revolt against the Persians {5}

480BCE  Demaratus warns the Spartans of Xerxes’
imminent attack by a stenographic message
(on wood covered with wax); leads to Persian
naval defeat at Salamis {4}

???  Hebrew atbash cipher (see Jer 51:1, 41) {26}

???  Chinese silk writing transmitted in balls of
wax ingested by a courier {5}

5th c BCE  Spartan transposition cipher based on
wrapping a strip about a scytale {8}

4th c BCE  Kamasutras advocate that a courtesan should
study the art of secret writing (mlecchita-
vikalpa) {9}

1st c  Pliny the Elder uses the milk of the
thithymallus as invisible ink {6}

2nd c  Suetonius’ Gallic Wars: Julius Caesar’s affine
cipher {10}

9th c  ibn Qutayba’s Kitab adab al-katib (Secretaries’
Manual) includes sections on cryptography {15}
9th c  al-Kindi’s *Manuscript on Deciphering Cryptographic Messages* describes frequency analysis {17}

13th c  Roger Bacon’s *Epistle on the Secret Works of Art and the Nullity of Magic* describes seven cryptographic methods {26}

1391  Geoffrey Chaucer’s *Treatise on the Astrolabe* includes a substitution cipher {27}

13th c  Leon Battisti Alberti’s *De compendenis cipheris* (*On ciphering methods*) suggests the use of two simultaneous ciphers, invents a cipher disk {45, 124}

1506  Giovanni Soro appointed as cipher secretary in Venice {28}

1550  Girolamo Cardano devises a grille for creating steganograms {39}

1563  Giambattista (Giovanni) della Porta’s *De furtivis literarum notis* (*On secret characters in writing*) discusses writing with a special ink that penetrates an eggshell and is displayed on the hardboiled interior; also suggests a polyalphabetic substitution cipher {5, 46}

1570s  Philip van Marnix is cryptanalyst to William of Nassau, the Dutch Prince of Orange {39}
16th c. Philibert Babou de la Bourdaisière is cipher secretary to Francis I of France; later, François Viète embarrasses the Spanish cryptographers \{28\}

1585 Blaise de Vigenère’s *Traicté des Chiffres* (*Treatise on ciphers*) \{51\}

1586 Thomas Phelippes, hired by Sir Francis Walshingham, uncovers the Babington plot, sending Mary, Queen of Scots, to the executioner’s block \{40\}

1626 Auguste Rossignol breaks a Huguenot cipher for Henri II; later, he and his brother Bonaventure run the *Cabinet noir* and develop the Great Cipher for Louis XIV \{55\}

1700s The pigpen cipher, or Freemason’s cipher, is made popular \{375\}

1760s The Geheime Kabinets-Kanzlei, the Viennese Black Chamber, is directed by Ignaz de Koch \{59\}

1814 Thomas Young deciphers the “Ptolemaios” cartouche on the Rosetta stone \{207\}

1834 Jean-François Champollion’s *Précis du système hiéroglyphique* deciphers Egyptian hieroglyphs \{211\}
1844  Morse devises a cipher, Morse code, for use with the telegraph {61}

1854  Baron Lyon Playfair popularizes a cipher devised by Sir Charles Wheatstone {79}

1863  Friederich Wilhelm Kasiski shows how to crack the Vigenère cipher in *Die Geheimschriften und die Dechiffrierkunst (Secret writing and the art of deciphering)* {78}

1800s  Pinprick encryption is made popular in newspapers {80}

19th c.  Cryptographic literature: {80}
  Edgar Allan Poe’s *The Gold Bug* (1843)
  Jules Verne’s *Journey to the Center of the Earth* (1864)
  Arthur Conan Doyle’s *Adventure of the Dancing Man* (1903)

1883  Auguste Kerchoffs von Nieuwenhof’s *Cryptologie militaire* {104}

1885  The Beale Papers are published {86}

1917  Arthur Zimmerman, German Foreign minister, sends a telegraph to Mexico signalling unrestricted submarine warfare in the Atlantic, which is decrypted by British codebreakers of Room 40 {110}
1918 Georges Painvin breaks the German WWI ADFGVX cipher {103}

1918 Maj. Joseph Mauborgne of the U.S. Army Signal Corps and and Gilbert Vernam of Bell Labs employ a one-time pad cipher {120}

1918 Scherbius & Ritter manufacture Enigma machines {127}

1929 Lester Hill uses matrix arithmetic to develop a block cipher

1931 Hans-Thilo Schmidt sells wiring plans for Enigma to a French agent {144}

1932 Univ. of Poznan mathematician Marian Rejewski at the Buro Szyfrów in Poland successfully begins to crack Enigma {149}

1940 Alan Turing’s bombes find Enigma keys {174}

1940 William Friedman and others at the U.S. Army Signals Intelligence Service break the Japanese Purple cipher machine {191}

1940s American Typex and British SIGABA machines remain secure during WWII {192}

1940s Alic Kober discovers the bridging syllables in Linear B {225}
1942  Philip Johnston suggests use of Navajo codetalkers \{193\}

1953  Michael Ventris and John Chadwick decipher Linear B \{239\}

1975  Whitfield Diffie and Martin Hellman develop public key cryptography (Clifford Cox had this idea at GCHQ in Cheltenham) \{268\}

1976  The Data Encryption Standard adopted in the U.S. \{250\}

1977  Ron Rivest, Adi Shamir & Leonard Adelman at MIT design RSA \{272\}

1982  Charles Bennett & Gilles Brassard develop quantum cryptography \{339\}

1991  Phil Zimmerman releases PGP into the public domain, is later investigated by the FBI \{295\}

1994  The American Escrowed Encryption Standard is adopted \{310\}

2001  The Advanced Encryption Standard (Rijndael) is adopted