Circa 300 BC
Euclid composes *The Elements*. Three of its thirteen books are devoted to number theory, introducing such fundamental concepts as divisibility, prime numbers, and composite numbers.

58-51 BC
Julius Caesar conquers Gaul. His book on the Gallic Wars contains the first documented use of encrypted messages.

1586
Blaise de Vigenère, a French diplomat, develops the first polyalphabetic cipher, in which letters may be encoded differently depending on their position in the document.

1640
French mathematician Pierre de Fermat discovers "Fermat's little theorem," which is still used to test large numbers for primality, even though it is not infallible.

1801
German mathematician Carl Friedrich Gauss publishes *Disquisitiones Arithmeticae,* the founding document of modern number theory. He is the first to appreciate the power of modular arithmetic, which greatly clarifies the somewhat mysterious results of Fermat.

1940
Relying on earlier work by Polish mathematicians and cryptographers, British mathematician Alan Turing cracks the Enigma cipher. The ability of Western commanders to decipher secret German messages hastened the Allied victory in World War II.

1976
Whitfield Diffie, Martin Hellman and Ralph Merkle propose a new approach to cryptography in which the encryption and decryption keys are different. This launches the era of public-key cryptography. They were unaware that James Ellis of British intelligence had already come up with the same idea but had to keep it secret.

1977
Ronald Rivest, Adi Shamir, and Leonard Adleman invent the RSA encryption algorithm, a public-key system whose security depends on the difficulty of factoring large numbers. They publicly challenge anybody to decode a message encoded with a 129-digit number.

1981
Carl Pomerance develops the "quadratic sieve" method, which allows large factorization problems to be parceled out to many computers working in parallel.

1988
The "number field sieve" method is invented by John Pollard.

1994
Rivest, Shamir, and Adleman's 1977 message is decoded by a team of hundreds of computers using the quadratic sieve method.

1994
Peter Shor of AT&T Research develops a "quick" (i.e. polynomial- time) factoring algorithm that would work on a quantum computer. However, it remains uncertain whether such a computer can ever be built.

1999
A 155 digit RSA challenge number is factorized by a group of researchers using the general number field sieve method.

2002
Manindra Agrawal, Neeraj Kayal, and Nitin Saxena develop a polynomial-time testing algorithm for prime numbers that works on ordinary computers. It relies on an ingenious modification of Fermat's little theorem.