RSA Algorithm

Perhaps the most famous public-key cryptosystems algorithm is the RSA algorithm. This algorithm makes use of the difficulty to determine the prime factorization of large numbers, the infinite number of primes in existence, Euler's theorem, and the Euclidean Algorithm to encrypt communication. The RSA algorithm is an asymmetric (two keys) cryptographic algorithm, and can also be classified as public-key cryptography, as it involves the general knowledge of one of the keys.

As computer power and shortcuts to factorize large numbers become more efficient as we progress through the 21st century, the rapid increase of the magnitude of the large primes is necessary to keep encryptions secure. Decryption on the receiving end of the encrypted message uses a variety of techniques to decrypt the message efficiently, including the Chinese Remainder Theorem.