The following are the most commonly used asymmetric algorithms:

- **Rivest, Shamir, and Adleman (RSA) encryption algorithm,** named after the three men who developed it, is a well-known cryptography system used for encryption and digital signatures. The RSA algorithm is commonly considered the standard for encryption and the core technology that secures most business conducted on the Internet. The RSA key may be of any length. The algorithm works by multiplying two large prime numbers, and through other operations in the algorithm, it derives one set of numbers for the public key and one for the private key.
- **The Diffie-Hellman key exchange** is an early key exchange design where two parties agree upon a secret key known only to them, without prior arrangement. The keys are passed in a way that they are not compromised, using encryption algorithms to verify that the data is reaching its intended recipient.
- **El Gamal encryption algorithm** is an extension of the Diffie-Hellman design. El Gamal is a complete public key encryption algorithm that uses some of the key exchange elements from Diffie-Hellman and incorporates encryption in those keys. The resultant encrypted keys reinforce the security and authenticity of the public key encryption design.
- **Elliptic curve cryptography (ECC)** uses elliptic curves to calculate simple encryption keys that are difficult to break for use in general-purpose encryption. One of the key benefits of ECC encryption algorithms is that it has a compact design because of the advanced mathematics involved.